MCSA/MCSE:
Windows XP Professional
Fast Pass

MCSA/MCSE:
Windows® XP Professional
Fast Pass

Lisa Donald

San Francisco • London

SYBEX®

Associate Publisher: Neil Edde
Acquisitions and Developmental Editor: Maureen Adams
Production Editor: Elizabeth Campbell
Technical Editor: Craig Vazquez
Copyeditor: Rebecca Rider
Compositor: Craig Woods, Happenstance Type-o-Rama
CD Coordinator: Dan Mummert
CD Technician: Kevin Ly
Proofreaders: Laurie O'Connell, Nancy Riddiough
Indexer: Nancy Guenther
Book Designer: Judy Fung
Cover Design and Illustration: Richard Miller, Calyx Design

Library of Congress Card Number: 2004109307

ISBN: 0-7821-4362-8

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Software License Agreement: Terms and Conditions

The media and/or any online materials accompanying this book that are available now or in the future contain programs and/or text files (the "Software") to be used in connection with the book. SYBEX hereby grants to you a license to use the Software, subject to the terms that follow. Your purchase, acceptance, or use of the Software will constitute your acceptance of such terms.
The Software compilation is the property of SYBEX unless otherwise indicated and is protected by copyright to SYBEX or other copyright owner(s) as indicated in the media files (the "Owner(s)"). You are hereby granted a single-user license to use the Software for your personal, noncommercial use only. You may not reproduce, sell, distribute, publish, circulate, or commercially exploit the Software, or any portion thereof, without the written consent of SYBEX and the specific copyright owner(s) of any component software included on this media.
In the event that the Software or components include specific license requirements or end-user agreements, statements of condition, disclaimers, limitations or warranties ("End-User License"), those End-User Licenses supersede the terms and conditions herein as to that particular Software component. Your purchase, acceptance, or use of the Software will constitute your acceptance of such End-User Licenses.
By purchase, use or acceptance of the Software you further agree to comply with all export laws and regulations of the United States as such laws and regulations may exist from time to time.

Software Support

Components of the supplemental Software and any offers associated with them may be supported by the specific Owner(s) of that material, but they are not supported by SYBEX. Information regarding any available support may be obtained from the Owner(s) using the information provided in the appropriate read.me files or listed elsewhere on the media.
Should the manufacturer(s) or other Owner(s) cease to offer support or decline to honor any offer, SYBEX bears no responsibility. This notice concerning support for the Software is provided for your information only. SYBEX is not the agent or principal of the Owner(s), and SYBEX is in no way responsible for providing any support for the Software, nor is it liable or responsible for any support provided, or not provided, by the Owner(s).

Warranty

SYBEX warrants the enclosed media to be free of physical defects for a period of ninety (90) days after purchase. The Software is not available from SYBEX in any other form or media than that enclosed herein or posted to www.sybex.com. If you discover a defect in the media during this warranty period, you may obtain a replacement of identical format at no charge by sending the defective media, postage prepaid, with proof of purchase to:

SYBEX Inc.
Product Support Department
1151 Marina Village Parkway
Alameda, CA 94501
Web: http://www.sybex.com

After the 90-day period, you can obtain replacement media of identical format by sending us the defective disk, proof of purchase, and a check or money order for $10, payable to SYBEX.

Disclaimer

SYBEX makes no warranty or representation, either expressed or implied, with respect to the Software or its contents, quality, performance, merchantability, or fitness for a particular purpose. In no event will SYBEX, its distributors, or dealers be liable to you or any other party for direct, indirect, special, incidental, consequential, or other damages arising out of the use of or inability to use the Software or its contents even if advised of the possibility of such damage. In the event that the Software includes an online update feature, SYBEX further disclaims any obligation to provide this feature for any specific duration other than the initial posting.
The exclusion of implied warranties is not permitted by some states. Therefore, the above exclusion may not apply to you. This warranty provides you with specific legal rights; there may be other rights that you may have that vary from state to state. The pricing of the book with the Software by SYBEX reflects the allocation of risk and limitations on liability contained in this agreement of Terms and Conditions.

Shareware Distribution

This Software may contain various programs that are distributed as shareware. Copyright laws apply to both shareware and ordinary commercial software, and the copyright Owner(s) retains all rights. If you try a shareware program and continue using it, you are expected to register it. Individual programs differ on details of trial periods, registration, and payment. Please observe the requirements stated in appropriate files.

Copy Protection

The Software in whole or in part may or may not be copy-protected or encrypted. However, in all cases, reselling or redistributing these files without authorization is expressly forbidden except as specifically provided for by the Owner(s) therein.

For my Pop. Love you always.

Acknowledgments

Writing a book is a team effort. The following people made it possible.

Huge thanks go out to Rebecca Rider, who worked as the editor for this book; she put in countless hours, was highly detail oriented, and did a tremendous job. Elizabeth Campbell, the production editor, somehow managed to keep this project on track, which was not always an easy task, while at the same time always being wonderful to work with. Craig Vazquez worked as the technical editor. He did a great job of keeping me honest and minimizing any errors within the book.

Thanks to James Chellis for allowing me to work on the MCSE series. Neil Edde, the associate publisher for this series, has nurtured the MCSE series since the early days. Maureen Adams, the acquisitions and developmental editor, helped get the book going in the early stages.

Any errors missed by the editor and technical editors were caught by the book's proofreaders: Laurie O'Connell and Nancy Riddiough. Without the great work of the team, this book would not have been possible.

On the local front, I'd like to thank my family and friends for their support. As always, a big hug to Kevin and Katie for just being themselves. Thanks to my mom and dad for their emotional support. And finally to Dietrich, who is always an adventure to be around.

Contents at a Glance

Contents

Introduction

Microsoft's Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) tracks for Windows 2000 and Windows Server 2003 are the premier certifications for computer industry professionals. Covering the core technologies around which Microsoft's future will be built, these programs are powerful credentials for career advancement.

This book is organized according to Microsoft's official objectives for the *Installing, Configuring, and Administering Microsoft Windows XP Professional* (Exam 70-270) exam. The chapters correspond to the seven broad objective categories:

- Installing Windows XP Professional
- Implementing and Conducting Administration of Resources
- Implementing, Managing, Monitoring, and Troubleshooting Hardware Devices and Drivers
- Monitoring and Optimizing System Performance and Reliability
- Configuring and Troubleshooting the Desktop Environment
- Implementing, Managing, and Troubleshooting Network Protocols and Services
- Configuring, Managing, and Troubleshooting Security

Within each chapter, the individual exam objectives are addressed. Each section of a chapter covers one exam objective. For each objective, I first present the critical information and then follow it with several Exam Essentials. Additionally, each chapter ends with a section of Review Questions. Here is a closer look at each of those components:

Critical Information Each individual exam objective section begins with a Critical Information section that presents detailed information that is relevant to the exam. This is the place to start if you're unfamiliar with or uncertain of the technical issues related to the objective.

Exam Essentials Here I give you a short list of topics that you should explore fully before you take the test. These Exam Essentials sum up the key information you should take out of the exam objective section.

Review Questions This section comes at the end of every chapter. It provides 10 questions that should help you gauge your mastery of the chapter.

The Microsoft Certified Professional Program

Since the inception of its certification program, Microsoft has certified over 1.5 million people. As the computer network industry increases in both size and complexity, this number is sure to grow—and the need for *proven* ability will also increase. Companies rely on certifications to verify the skills of prospective employees and contractors.

Microsoft has developed its Microsoft Certified Professional (MCP) program to give you credentials that verify your ability to work with Microsoft products effectively and professionally. Obtaining your MCP certification requires that you pass any one Microsoft certification exam.

Several levels of certification are available based on specific suites of exams. Depending on your areas of interest or experience, you can obtain any of the following MCP credentials:

Microsoft Certified System Administrator (MCSA) on Windows 2000 or Windows Server 2003 This certification targets system and network administrators with roughly 6 to 12 months of desktop and network administration experience. The MCSA can be considered the entry-level certification. You must take and pass a total of four exams to obtain your MCSA. Or, if you are an MCSA on Windows 2000, you can take one Upgrade exam to obtain your MCSA on Windows Server 2003.

Microsoft Certified System Engineer (MCSE) on Windows 2000 or Windows Server 2003 This certification track is designed for network and systems administrators, network and systems analysts, and technical consultants who work with Microsoft Windows 2000 Professional and Server and/or Windows XP and Server 2003 software. You must take and pass seven exams to obtain your MCSE. Or, if you are an MCSE on Windows 2000, you can take two Upgrade exams to obtain your MCSE on Windows Server 2003.

Microsoft Certified Desktop Support Technician (MCDST) This certification track is the newest from Microsoft. This program is aimed at professionals who support end users in Windows 2000/2003 and XP. You must take two exams to earn your MCDST.

Microsoft Certified Application Developer (MCAD) This track is designed for application developers and technical consultants who primarily use Microsoft development tools. Currently, you can take exams on Visual Basic .NET or Visual C# .NET. You must take and pass three exams to obtain your MCSD.

Microsoft Certified Solution Developer (MCSD) This track is designed for software engineers and developers and technical consultants who primarily use Microsoft development tools. Currently, you can take exams on Visual Basic .NET and Visual C# .NET. You must take and pass five exams to obtain your MCSD.

Microsoft Certified Database Administrator (MCDBA) This track is designed for database administrators, developers, and analysts who work with Microsoft SQL Server. As of this printing, you can take exams on either SQL Server 7 or SQL Server 2000. You must take and pass four exams to achieve MCDBA status.

Microsoft Certified Trainer (MCT) The MCT track is designed for any IT professional who develops and teaches Microsoft-approved courses. To become an MCT, you must first obtain your MCSE, MCSD, or MCDBA, then you must take a class at one of the Certified Technical Training Centers. You will also be required to prove your instructional ability. You can do this in various ways: by taking a skills-building or train-the-trainer class, by achieving certification as a trainer from any of several vendors, or by becoming a Certified Technical Trainer through CompTIA. Last of all, you will need to complete an MCT application.

The Installing, Configuring, and Administering Microsoft Windows XP Professional Exam

The Windows XP Professional exam covers concepts and skills related to installing, configuring, and managing Windows XP Professional computers. It emphasizes the following elements of Windows XP Professional support:

- Installing Windows XP Professional
- Implementing and administering resources
- Implementing, managing, and troubleshooting hardware devices and drivers
- Monitoring and optimizing system performance and reliability
- Configuring and troubleshooting the desktop environment
- Implementing, managing, and troubleshooting network protocols and services
- Implementing, monitoring, and troubleshooting security

This exam is quite specific regarding Windows XP Professional requirements and operational settings, and it can be particular about how administrative tasks are performed within the operating system. It also focuses on fundamental concepts of Windows XP Professional's operation. Careful study of this book, along with hands-on experience, will help you prepare for this exam.

Microsoft provides exam objectives to give you a general overview of possible areas of coverage on the Microsoft exams. Keep in mind, however, that exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit Microsoft's Training and Certification website (`www.microsoft.com/traincert`) for the most current listing of exam objectives.

Tips for Taking the Windows XP Professional Exam

Here are some general tips for achieving success on your certification exam:

- Arrive early at the exam center so that you can relax and review your study materials. During this final review, you can look over tables and lists of exam-related information.
- Read the questions carefully. Don't be tempted to jump to an early conclusion. Make sure you know *exactly* what the question is asking.
- Answer all questions. Remember that the adaptive format does *not* allow you to return to a question. Be very careful before entering your answer. Because your exam may be shortened by correct answers (and lengthened by incorrect answers), there is no advantage to rushing through questions.
- On simulations, do not change settings that are not directly related to the question. Also, assume default settings if the question does not specify or imply which settings are used.
- For questions you're not sure about, use a process of elimination to get rid of the obviously incorrect answers first. This improves your odds of selecting the correct answer when you need to make an educated guess.

Exam Registration

You may take the Microsoft exams at any of more than 1,000 Authorized Prometric Testing Centers (APTCs) and VUE Testing Centers around the world. For the location of a testing center near you, call Prometric at 800-755-EXAM (755-3926), or call VUE at 888-837-8616. Outside the United States and Canada, contact your local Prometric or VUE registration center.

Find out the number of the exam you want to take, and then register with the Prometric or VUE registration center nearest to you. At this point, you will be asked for advance payment for the exam. The exams are $125 each and you must take them within one year of payment. You can schedule exams up to six weeks in advance or as late as one working day prior to the date of the exam. You can cancel or reschedule your exam if you contact the center at least two working days prior to the exam. Same-day registration is available in some locations, subject to space availability. Where same-day registration is available, you must register a minimum of two hours before test time.

You may also register for your exams online at `www.prometric.com` or `www.vue.com`.

When you schedule the exam, you will be provided with instructions regarding appointment and cancellation procedures, ID requirements, and information about the testing center location. In addition, you will receive a registration and payment confirmation letter from Prometric or VUE.

Microsoft requires certification candidates to accept the terms of a Non-Disclosure Agreement before taking certification exams.

What's on the CD?

The enclosed CD offers bonus exams and flashcards to help you study for the exam. The CD's resources are described here:

Glossary of terms Included is a Glossary of terms used throughout this book in PDF format. We've also included Adobe Acrobat Reader, which provides the interface for the PDF contents as well as the search capabilities.

The Sybex MCSE Test Engine This is a collection of multiple-choice questions that will help you prepare for your exam. There are two bonus exams designed to simulate the actual live exam.

Sybex MCSE Flashcards for PCs and Handheld Devices The "flashcard" style of question offers an effective way to quickly and efficiently test your understanding of the fundamental concepts covered in the exam. The Sybex MCSE Flashcards set consists of more than 150 questions presented in a special engine developed specifically for this book. Here's what the Sybex MCSE Flashcards interface looks like:

Because of the high demand for a product that will run on handheld devices, we have also developed a version of the flashcard questions that you can take with you on your Palm OS PDA (including the PalmPilot and Handspring's Visor).

Contacts and Resources

To find out more about Microsoft Education and Certification materials and programs, to register with Prometric or VUE, or to obtain other useful certification information and additional study resources, check the following resources:

Microsoft Training and Certification Home Page

`www.microsoft.com/traincert`

This website provides information about the MCP program and exams. You can also order the latest Microsoft Roadmap to Education and Certification.

Microsoft TechNet Technical Information Network

`www.microsoft.com/technet`

800-344-2121

Use this website or phone number to contact support professionals and system administrators. Outside the United States and Canada, contact your local Microsoft subsidiary for information.

Prometric

`www.prometric.com`

800-755-3936

Contact Prometric to register to take an MCP exam at any of more than 800 Prometric Testing Centers around the world.

Virtual University Enterprises (VUE)

`www.vue.com`

888-837-8616

Contact the VUE registration center to register to take an MCP exam at one of the VUE Testing Centers.

Cramsession on Brainbuzz.com

`cramsession.brainbuzz.com`

Cramsession is an online community focusing on all IT certification programs. In addition to discussion boards and job locators, you can download one of several free cram sessions, which are nice supplements to any study approach you take.

Chapter 1

Installing Windows XP Professional

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Perform and troubleshoot an attended installation of Windows XP Professional.**
- ✓ **Perform and troubleshoot an unattended installation of Windows XP Professional.**
  - Install Windows XP Professional by using Remote Installation Services (RIS).
  - Install Windows XP Professional by using the System Preparation Tool.
  - Create unattended answer files by using Setup Manager to automate the installation of Windows XP Professional.
- ✓ **Upgrade from a previous version of Windows to Windows XP Professional.**
  - Prepare a computer to meet upgrade requirements.
  - Migrate existing user environments to a new installation.
- ✓ **Perform post-installation updates and product activation.**
- ✓ **Troubleshoot failed installations.**

The first step in using Windows XP Professional is to install it. You can install Windows XP through attended installations or through unattended installations. A large part of this exam focuses on using unattended installations. You also need to know how to troubleshoot installation problems. If you have an existing operating system, you need to know how to upgrade to Windows XP Professional. Once you have Windows XP Professional installed, you need to know how to perform the post-installation updates and product activation.

Perform and Troubleshoot an Attended Installation of Windows XP Professional

Windows XP Professional is easy to install. But this doesn't mean you don't need to prepare for the installation process. Before you begin the installation, you should know what is required for a successful installation and have all of the pieces of information you'll need to supply during the installation process. In preparing for the installation, you should make sure you have the following information:

- The hardware requirements for Windows XP Professional
- How to use the Hardware Compatibility List (HCL) to determine whether your hardware is supported by Windows XP Professional
- Verification that your computer's Basic Input/Output System (BIOS) is compatible with Windows XP Professional
- Whether the devices in your computer have Windows XP drivers
- The installation options suitable for your system, including which disk-partitioning scheme and file system you should select for Windows XP Professional to use

Critical Information

You can run the installation from the CD or over a network. There are four main steps in the Windows XP Professional installation process:

- Collecting information
- Preparing installation
- Installing Windows
- Finalizing installation

The Windows XP installation process is designed to be as simple as possible. The chances for installation errors are greatly minimized through the use of wizards and the step-by-step process. However, it is possible that errors may occur.

Table 1.1 lists some possible installation errors you might encounter.

TABLE 1.1 Common Installation Problems

Problem	Description
Media errors	Media errors are caused by defective or damaged CDs. To check the CD, put it into another computer and see if you can read it. Also check your CD for scratches or dirt—it may just need to be cleaned.
Insufficient disk space	Windows XP needs at least 2GB of free space for the installation program to run properly. If the Setup program cannot verify that this space exists, the program will not let you continue.
Not enough memory	Make sure that your computer has the minimum amount of memory required by Windows XP Professional (64MB). Having insufficient memory may cause the installation to fail or blue-screen errors to occur after installation.
Not enough processing power	Make sure that your computer has the minimum processing power required by Windows XP Professional (Pentium 233MHz). Having insufficient processing power may cause the installation to fail or blue-screen errors to occur after installation.
Hardware that is not on the HCL	If your hardware is not on the HCL, Windows XP may not recognize the hardware, or the device may not work properly.
Hardware with no driver support	Windows XP will not recognize hardware without driver support.
Hardware that is not configured properly	If your hardware is Plug and Play–compatible, Windows should configure it automatically. If your hardware is not Plug and Play–compatible, you will need to manually configure the hardware per the manufacturer's instructions.
Incorrect CD key	Without a valid CD key, the installation will not go past the Product Key dialog box. Make sure that you have not typed in an incorrect key (check your Windows XP installation folder for this key).

TABLE 1.1 Common Installation Problems *(continued)*

Problem	Description
Failure to access Transmission Control Protocol/Internet Protocol (TCP/IP) network resources	If you install Windows XP with typical settings, the computer is configured as a Dynamic Host Configuration Protocol (DHCP) client. If there is no DHCP server to provide IP configuration information, the client will still generate an auto-configured IP address, but be unable to access network resources through TCP/IP if the other network clients are using DHCP addresses.
Failure to connect to a domain controller when joining a domain	Make sure that you have specified the correct domain name. If your domain name is correct, verify that your network settings have been set properly and that a domain controller and Domain Name System (DNS) server are available. If you still can't join a domain, install the computer in a workgroup, then join the domain after installation.

Exam Essentials

Know how to install and troubleshoot a Windows XP installation. Be able to install third party disk drives. List the common installation problems and how they can be corrected.

Perform and Troubleshoot an Unattended Installation of Windows XP Professional

You can automate the installation of Windows XP Professional by using Remote Installation Services (RIS) to remotely deploy unattended installations (which require a Windows 2000 Server or Windows Server 2003) or by using the System Preparation Tool for disk imaging. To help customize both options for automating remote installations, you can also use answer files. Answer files are used with automated installations to provide answers to the questions that are normally asked during the installation process.

Critical Information

Remote Installation Services (RIS) was introduced in Windows 2000 Server and is also supported by Windows Server 2003. It allows you to remotely install Windows XP Professional.

A RIS server installs Windows XP Professional on RIS clients, as illustrated in Figure 1.1. The RIS server must have the RIS server software installed and configured. RIS clients are computers that have a Pre-boot eXecution Environment (PXE) network adapter or use a RIS boot disk. PXE is a technology that is used to boot to the network when no operating system or network configuration has been installed and configured on a client computer. The RIS boot disk

is a PXE ROM emulator for network adapters that don't have a PXE boot ROM or for a PC that doesn't support booting from the network. In order to use a RIS boot disk, the network adapter must be PCI compliant. The RIS boot disk is generated with the Remote Boot Floppy Generator (`rbfg.exe`) utility.

The RIS clients access RIS servers through DHCP to remotely install the operating system from the RIS server. The network must have a DHCP server, a DNS server, and Active Directory to connect to the RIS server. No other client software is required to connect to the RIS server. Remote installation is a good choice for automatic deployment when you need to deploy to large numbers of computers and your clients are PXE compliant.

The RIS server can be configured with either of two types of images:

- A CD-based image that contains only the Windows XP Professional operating system. You can create answer files for CD-based images to respond to the Setup program's configuration prompts.
- A Remote Installation Preparation (RIPrep) image that can contain the Windows XP operating system and applications. This type of image is based on a preconfigured computer.

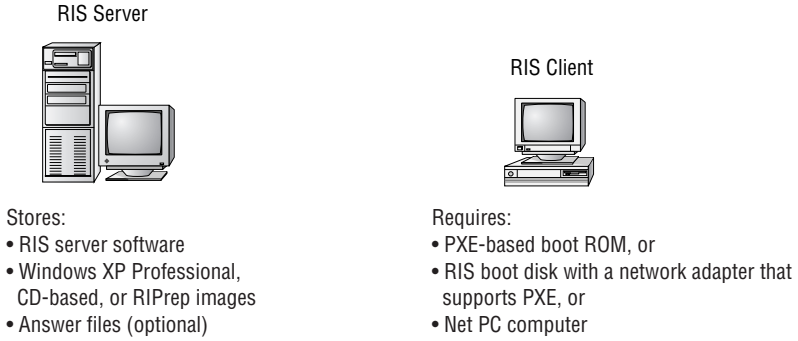
Using Remote Installation Services (RIS)

A variety of installation options are available through the Windows XP Client Installation Wizard (CIW). For RIS installation, you need a RIS server that stores the Windows XP Professional operating system files in a shared image folder, and clients that can access the RIS server. Depending on the type of image you will distribute, you may also want to configure answer files so that users need not respond to any Windows XP Professional installation prompts.

Following are some of the advantages of using RIS for automated installation:

- You can remotely install Windows XP Professional.
- The procedure simplifies management of the server image by allowing you to access Windows XP distribution files and use Plug and Play hardware detection during the installation process.
- You can quickly recover the operating system in the event of a computer failure.

FIGURE 1.1 RIS uses a RIS server and RIS clients.



Windows XP security is retained when you restart the destination computer. Here are the basic steps of the RIS process:

1. The RIS client initiates a special boot process through the PXE network adapter (and the computer's BIOS configured for a network boot) or through a special RIS boot disk. On a PXE client, the client presses F12 to start the PXE boot process and to indicate that they want to perform a RIS installation.
2. The client computer sends out a DHCP discovery packet that requests an IP address for the client and the IP address of a RIS server (running Windows 2000 Server or Windows Server 2003). Within the discovery packet, the client also sends its Globally Unique Identifier (GUID). The GUID is a unique 32-bit address that is used to identify the computer account as an object within the Active Directory.
3. If the DHCP server and the RIS server are on the same computer, the information requested in the discovery packet is returned. If the DHCP server and the RIS server are on separate networks, the DHCP server will return the client information for IP configuration. Then the client will send out another broadcast to contact the RIS server.
4. The client contacts the RIS server using the Boot Information Negotiation Layer (BINL) protocol. The RIS server contacts Active Directory to see if the client is a "known client" and whether it has already been authorized (also called pre-staged) through Active Directory.
5. If the client is authorized to access the RIS server, BINL provides to the client the location of the RIS server and the name of the bootstrap image (enough software to get the client to the correct RIS server).
6. The RIS client accesses the bootstrap image via the Trivial File Transfer Protocol (TFTP), and the Windows XP CIW is started.
7. The RIS client is prompted for a username and password that can be used to log on to the Windows 2000 or Windows 2003 domain that contains the RIS server.
8. Depending on the user or group credentials, the user sees a menu offering the operating systems (images) that can be installed. The user sees only the options for the installs determined by the parameters defined on the RIS server.

The following sections describe how to set up the RIS server and the RIS clients, and how to install Windows XP Professional through RIS.

RIS Client Options

RIS offers several client installation options. This allows administrators to customize remote installations based on organizational needs. When the client accesses the Windows XP CIW, they see the installation options that have been defined by the administrator. Remote installation options include the following:

Automatically setting up the computer When you automatically set up the computer, the user sees a screen indicating which operating system will be installed but is not prompted for any configuration settings. If only one operating system is offered, the user does not even have to make any selections and the entire installation process is automatic.

Customizing the setup of the computer If you configure RIS to support customizing the setup of the computer, then administrators who install computers within the enterprise can override the RIS settings to specify the name and location of the computer being installed within Active Directory.

Restarting a previous setup attempt The option to restart a previous setup attempt is used when a remote installation fails prior to completion. The operating system installation will restart when this option is selected from the CIW.

Performing maintenance or troubleshooting The maintenance and troubleshooting option provides access to third-party troubleshooting and maintenance tools. Examples of tasks that can be completed through this option include updating flash BIOS and using PC diagnostic tools.

Preparing the RIS Server

The RIS server is used to manage and distribute the Windows XP Professional operating system to RIS client computers. RIS servers can distribute CD-based images (created with the `Risetup.exe` utility) or images created from a reference Windows XP computer, called RIPrep images (created with the `RIPrep.exe` utility). A CD-based image contains the operating system installation files taken directly from the Windows XP Professional CD and can be customized for specific computers through the use of answer files. RIPrep images are based on a preconfigured computer and can contain applications as well as the operating system. `RIPrep.exe` is used to create the image of the target computers on the RIS server.

The RIS server is configured to specify how client computers will be installed and configured. The administrator can configure the following options for client computers:

- Define the operating system installation options that will be presented to the user. Based on access permissions from Access Control Lists (ACLs), administrators can define several installation options, and then allow specific users to select an option based on their specific permissions.
- Define an automatic client-computer naming format, which bases the computer name on a custom naming format. For example, the computer names might be a combination of location and username.
- Specify the default Active Directory location for client computers that are installed through remote installation.
- Pre-stage client computers through Active Directory so that only authorized computers can access the RIS server. This option requires a specified computer name, a default Active Directory location, and identification of RIS servers and the RIS clients the RIS Servers will service.
- Authorize RIS servers so that unauthorized RIS servers can't offer RIS services to clients.
- Create and modify the RIS answer file.

The following steps for preparing the RIS server are discussed in the upcoming sections:

1. Make sure that the server meets the requirements for running RIS (Windows 2000 Server or Windows Server 2003, TCP/IP, DHCP, DNS, Active Directory).
2. Install the RIS Server.

3. Configure and start RIS, using either a CD-based image or a RIPrep image.
4. Authorize the RIS server through DHCP Manager.
5. Grant users who will perform RIS installations the user right to create computer accounts.
6. Grant users who will perform the RIS installation the Log On as a Batch Job user right.
7. Configure the RIS server to respond to client computers (if this was not configured when RIS was installed).
8. Configure RIS template files (if you wish to customize installation options for different computers or groups).

Preparing the RIS Client

The RIS client is the computer on which Windows XP Professional will be installed. RIS clients rely on PXE, which allows the client computer to remotely boot and connect to a RIS server.

To act as a RIS client, the computer must meet all the hardware requirements for Windows XP Professional and have a network adapter installed. In addition, the RIS client must support one of the following configurations:

- Use a PXE-based boot ROM (a boot ROM is a special chip that uses read-only memory) with a BIOS that supports starting the computer with the PXE-based boot ROM (as opposed to booting from the hard disk).
- Follow the Net PC/PC 98 standard for PCs, which uses industry-standard components for the computer. This includes processor, memory, hard disk, video, audio, and an integrated network adapter and modem, in a locked case with limited expansion capabilities. The primary advantages of Net PCs are that they are less expensive to purchase and to manage.
- Have a network adapter that supports PXE and that can be used with a RIS boot disk. The only network adapters that can be used with RIS boot disks are the network adapters that are displayed when running the `RBFG.exe` utility. If your network adapter is not on the list, ensure that you have the most current `RBFG.exe` utility, since Microsoft makes updates and adds drivers to this utility periodically. You can obtain updates through Windows Update or Service Packs.

If the client computer does not have a network adapter that contains a PXE-based boot ROM, then you can use a RIS boot disk to simulate the PXE startup process. The PXE-based boot disk is used to provide network connectivity to the RIS server. In order to use a RIS boot disk, the client computer must use a PCI-compliant network adapter.

If your client uses PCMCIA or ISA network adapters, there is no support to use RIS boot disks.

To create a RIS boot disk, take the following steps:

1. On a Windows XP Professional computer that is connected to the same network as the RIS server, select Start ➢ Run. In the Run dialog box, type the following command and click the OK button:

   ```
   \\RIS_Server\Reminst\Admin\I386\Rbfg.exe
   ```

2. The Windows XP Remote File Generator dialog box appears. Insert a blank floppy disk in your computer, select the appropriate destination drive, select the installed network card from the Adapter List, and click the Create Disk button. The network adapter must be on the list of those shown when running the `RBFG.exe` utility. When the disk is made, it will support any and all of these network adapters.
3. You see a message verifying that the boot floppy was created and asking whether you want to create another disk. You can click Yes and repeat the procedure to create another boot disk, or click No. After you are finished creating RIS boot disks, click the Close button.

Installing Windows XP Professional through RIS

After the RIS server has been installed and configured, you can install Windows XP Professional on a RIS client that uses either a PXE-compliant network card or a RIS boot disk with a network card that supports PXE.

To install Windows XP Professional on the RIS client, take the following steps:

1. Start the computer. When prompted, press F12 for a network service boot.
2. The Client Installation Wizard starts. Press Enter to continue.
3. The Windows XP Logon dialog box appears. Specify the domain to which you will log on, and enter a valid domain username and password.
4. A menu appears with the options Automatic Setup, Custom Setup, Restart a Previous Setup Attempt, and Maintenance and Troubleshooting. Select Automatic Setup.

If you have only one RIS image, it will automatically be installed. If you have multiple RIS images, the user will see a menu of RIS images. After you select a RIS image, the remote installation process will start. What happens next depends on the image type and whether you have configured answer files.

System Preparation Tool

The *System Preparation Tool* (`Sysprep.exe`) is used to prepare a computer for *disk imaging*, which can be done with third-party image software or with disk-duplicator hardware. Disk imaging (also sometimes called disk cloning or disk duplication) is the process of creating a reference computer for the automated deployment. The reference, or source, computer has Windows XP Professional installed and is configured with the settings and applications that should be installed on the target computers. An image is then created that can be transferred to other computers, thus installing the operating system, settings, and applications that were defined on the reference computer.

Using the System Preparation Tool and disk imaging is a good choice for automatic deployment when you have the hardware that supports disk imaging and you have a large number of computers with similar configuration requirements. For example, education centers that reinstall the same software every week might use this technology.

To perform an unattended install, the System Preparation Tool prepares the reference computer by stripping away the security identifier (SID), which is used to uniquely identify each computer on the network. The System Preparation Tool also detects any Plug and Play devices that are installed and can adjust dynamically for any computers that have different hardware installed.

If you are using disk-duplicator hardware, you create a reference computer, and then use the System Preparation Tool to create the image. You would then remove the drive that has the disk image and insert it into a special piece of hardware, called a disk duplicator, to copy the image. The copied disks are inserted into the target computers. After you add the hard drive that contains the disk image to the target computers, you can complete the installation from those computers. Figure 1.2 illustrates the disk-imaging process. You can also copy disk images by using special third-party software.

When the client computer starts an installation using a disk image, a Mini-Setup Wizard will execute. You can customize what is displayed on the Windows Welcome screen and the options that are displayed through the Mini-Setup Wizard process, which query for information such as username or time zone selection. You can also create fully automated deployments with disk imaging through the use of answer files.

Using the System Preparation Tool to Create Disk Images

To create a disk image, you install Windows XP Professional on the source computer with the configuration that you want to copy. The source computer's configuration should also include any applications that should be installed.

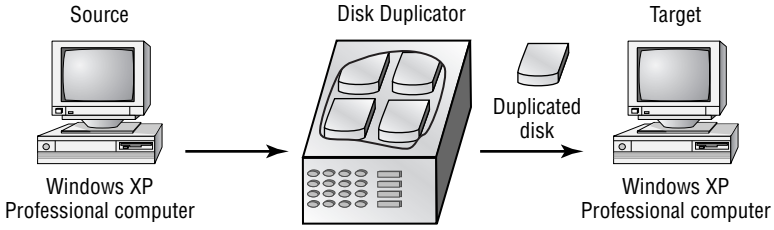
Once you have your source computer configured, you use the System Preparation Tool (`Sysprep.exe`) to prepare the disk image for disk duplication. After you've created the disk image, you can copy the image to destination computers through third-party software or through hardware disk duplication.

PREPARING FOR DISK DUPLICATION

To use a disk image, the source and target computers must meet the following requirements:

- Both the source and destination computers must be able to use the same hard-drive controller driver.
- Both the source and destination computers must have the same Hardware Abstraction Layer (HAL). For example, both use an Advanced Configuration and Power Interface (ACPI) HAL. If the source computer is ACPI-compatible and the target computer is non-ACPI-compatible, Windows XP Professional will not load properly.

FIGURE 1.2 Disk imaging with disk-duplicator hardware



- The size of the installation partition must be as large as the smallest space the image program will install the image to.
- Plug and Play devices on the source and destination computers do not need to match, as long as the drivers for the Plug and Play devices are available.

USING THE SYSTEM PREPARATION TOOL

The System Preparation Tool (`Sysprep.exe`) is included on the Windows XP Professional CD in the `\Support\Tools` folder, in the `Deploy.cab` file. When you run this utility on the source computer, it strips out information from the master copy that must be unique for each computer, such as the security ID (SID).

After you install the copied image on the target computer, a Mini-Setup Wizard runs. This wizard automatically creates a unique computer SID and then prompts the user for computer-specific information, such as the product ID, regional settings, and network configuration. The required information can also be supplied through an automated installation script.

Table 1.2 defines the command switches that you can use to customize the System Preparation Tool's (`Sysprep.exe`) operation.

TABLE 1.2 System Preparation Command-Line Switches

Switch	Description
`-quiet`	Runs the installation with no user interaction.
`-pnp`	Forces Setup to run Plug and Play detection of hardware.
`-reboot`	Restarts the target computer after the System Preparation Tool completes.
`-noreboot`	Specifies that the computer should be shut down without a reboot.
`-clean`	Specifies that critical devices should be cleaned out.
`-nosidgen`	Doesn't create a SID on the destination computer (used with disk cloning).
`-activated`	Prevents Windows Product Activation from resetting.
`-factory`	Allows you to add additional drivers and applications to the image after the computer has restarted.
`-reseal`	Reseals an image and prepares the computer for delivery after modifications have been made to an image using the factory mode.
`-bmsd`	Used to build a list of all available mass storage devices in `sysprep.inf`.

TABLE 1.2 System Preparation Command-Line Switches *(continued)*

Switch	Description
`-forceshutdown`	If you have used the `-reseal` switch, this switch prepares the operating system as specified, then immediately shuts down the computer without any user intervention.
`-mini`	Specifies that you want to run the Mini-Setup Wizard on the next restart of the computer.

After you run the System Preparation Tool on a computer, you need to run the Mini-Setup Wizard. Then run the Setup Manager to create an answer file that will answer the Mini-Setup Wizard's questions when the computer (the imaged computer or the original computer that has had the System Preparation Tool run on it) is restarted.

In the following sections, you will learn how to create a disk image and how to copy and install from a disk image.

CREATING A DISK IMAGE

To run the System Preparation Tool and create a disk image, take the following steps:

1. Install Windows XP Professional on a source computer. The computer should have a similar hardware configuration to the destination computer(s). You should not join a domain, and the administrator password should be left blank.
2. Log on to the source computer as administrator and, if desired, install and configure any applications, files (such as newer versions of Plug and Play drivers), or custom settings (for example, a custom desktop) that will be applied to the target computer(s).
3. Verify that your image meets the specified configuration criteria and that all applications are properly installed and working. Extract the `Deploy.cab` file from the Windows XP Professional CD.
4. Select Start ➢ Run and click the Browse button in the Run dialog box. Select Local Drive (C:), then Deployment Tools; double-click `Sysprep` and click the OK button.
5. The Windows System Preparation Tool dialog box appears. This dialog box warns you that the execution of this program will modify some of the computer's security parameters. Click the OK button.
6. You will be prompted to turn off your computer.
7. You may now boot up with third-party imaging software and create an image of the computer to deploy to other computers.

COPYING AND INSTALLING FROM A DISK IMAGE

After you've run the System Preparation Tool on the source computer, you can copy the image and then install it on the target computer.

If you are using special hardware (a disk duplicator) to duplicate the disk image, shut down the source computer and remove the disk. Copy the disk and install the copied disk into the target computer. If you are using special software, copy the disk image per the software vendor's instructions.

After the image is copied, turn on the destination computer. The Mini-Setup Wizard runs and prompts you as follows (if you have not configured an answer file):

- Accept the End User License Agreement.
- Specify regional settings.
- Enter a name and organization.
- Specify your product key.
- Specify the computer name and administrator password.
- Specify dialing information (if a modem is detected).
- Specify date and time settings.
- Specify which networking protocols and services should be installed.
- Join a workgroup or a domain.

If you have created an answer file for use with disk images, you should save the images on the reference computer prior to using the Sysprep utility. Answer files are described in the next section of this chapter. Answer files allow the installation to run without requiring any user input.

Unattended Answer Files

Answer files are automated installation scripts used to answer the questions that appear during a normal Windows XP Professional installation. You can use answer files with Windows XP unattended installations, the System Preparation Tool (disk images), or RIS installations. Setting up answer files allows you to easily deploy Windows XP Professional to computers that may not be configured in the same manner, with little or no user intervention.

You create answer files through the Setup Manager (`Setupmgr`) utility. There are several advantages to using Setup Manager to create answer files:

- You can easily create answer files through a graphical interface, which reduces syntax errors.
- It simplifies the addition of user-specific or computer-specific configuration information.
- You can include application setup scripts within the answer file.
- The utility creates the distribution folder and allows you to populate the distribution folder by adding files, programs, and applications that will be used along with the installation files.

In the following sections, you will learn about options that can be configured through Setup Manager, how to create answer files with Setup Manager, answer file format, and how to manually edit answer files.

Options That Can Be Configured through Setup Manager

The Setup Manager can be used to configure a wide variety of installation options. The following list defines what can be configured through Setup Manager and gives a short description of each parameter:

Set user interaction. Sets the level of user interaction that will be used during the setup process. This can be fully automated, or the user can supply configuration information for the items you specify.

Set default username. Specifies the username and organization that will be defined for the computer.

Define computer names. Configures multiple usernames during the setup process. In this case, Setup Manager will generate a Uniqueness Database File (UDF), which maps unique names and settings to specific computers.

Set an administrator password. Encrypts the administrator password that has been defined within the answer file, or allows you to prompt the user on the first logon to specify an administrator password.

Display settings. Configures the display for color depth, screen area, and the refresh frequency display settings that should be applied.

Configure network settings. Specifies any custom network settings you want to be applied. You can also configure the computer to be added to a domain or workgroup, and if you join a domain, automatically create an account within the domain for the computer.

Set time zone and regional options. Specifies the appropriate time zone to be configured for the target computer. Regional options include language settings such as how time and date are displayed.

Set Internet Explorer settings. Configures the basic settings that will be applied to Internet connections.

Set telephony settings. Configures telephony properties—for example, area codes and dialing rules.

Add `cmdlines.txt` file. Adds applications during the GUI-mode phase of Windows XP Professional installation.

Create an installation folder. Uses the default installation folder (`\Windows`) to generate or set a custom folder during the setup process.

Install printers. Sets up and configures printers as a part of the automated deployment process.

Add command to the Run Once. Installs whatever command or applications you specify the first time a user logs on to the computer.

Run command at the end of setup. Runs a command at the end of the setup process, but before a user logs on to the computer the first time.

Copy additional files. Copies additional files to the user desktop.

Create a distribution folder. Creates a Windows distribution folder on a network share that contains the Windows XP Professional source files or any additional files (such as device drivers) you want to add.

Creating Answer Files with Setup Manager

After you have extracted the Windows XP Deployment Tools from the Windows XP Professional CD, you can run the Setup Manager utility to create a new answer file, create an answer file that duplicates the current computer's configuration, or edit existing answer files.

The following steps describe how to create a new installation script. In this example, the instructions are for creating an answer file for a RIS installation. This answer file provides default answers, uses the default display configuration, configures typical network settings, and does not edit any additional options.

1. Select Start ➢ Run and click the Browse button in the Run dialog box. Double-click the Deployment Tools folder, double-click the `Setupmgr` program, and then click the OK button.
2. The Windows Setup Manager Wizard starts. Click the Next button.
3. The New or Existing Answer File dialog box appears. This dialog box provides choices for creating a new answer file or modifying an existing answer file. Select the option Create a New Answer File and click the Next button.
4. The Product to Install dialog box appears. You can choose Windows Unattended Installation, Sysprep Install, or Remote Installation Services. Select Remote Installation Services and click the Next button.
5. The User Interaction Level dialog box appears. This dialog box offers the following options:
   - Provide Defaults allows you to configure default answers that will be displayed. The user is prompted to review the default answer and can change the answer if desired.
   - Fully Automated uses all the answers in the answer file and will not prompt the user for any interaction.
   - Hide Pages lets you hide the wizard page from the user if you have supplied all of the answers on the Windows Setup Wizard page.
   - Read Only allows the user to see the Setup Wizard display page but not to make any changes to it (this option is used if the Setup Wizard display page is shown to the user).
   - GUI Attended allows only the text-mode portion of the Windows Setup program to be automated.

   Select the Provide Defaults option and click the Next button to continue.
6. Next, from the Display Settings dialog box, you can configure the following settings:
   - For the Colors option, set the display color to the Windows default, 16 colors, 256 colors, high color (16 bit), high color (24 bit), or high color (32 bit).
   - The Screen Area option allows you to set the screen area to the Windows default, or to one of the following: 640×480, 800×600, 1024×768, 1280×1024, or 1600×1200.

- The Refresh Frequency option (the number of times the screen is updated) allows you to set the refresh frequency to the Windows default or to 60Hz, 70Hz, 72Hz, 75Hz, or 85Hz.
- The Custom button displays a dialog box in which you can further customize display settings for the color, screen area, and refresh frequency.

For this example, click Next to accept the default configuration and continue.

7. The Time Zone dialog box appears. Select your computer's time zone from the drop-down list and click the Next button.
8. The Providing the Product Key dialog box appears. Type in the product key for the computer that will be installed. Each computer will need its own license key. When you are done, click the Next button.
9. The Computer Name dialog box will appear. You can let a computer name be automatically generated or you can choose to specify the destination computer name.
10. Next is the Administrator Password dialog box. You can choose to prompt the user for a password, or you can specify the administrator password. You can also specify that when the computer starts, the administrator will automatically be logged on. Enter and confirm an administrator password. Then click the Next button.
11. In the Network Settings dialog box, you can choose from Typical Settings, which installs TCP/IP, enables DHCP, and installs Client for Microsoft Networks; or Custom Settings, which allows you to customize the computer's network settings. Select the Typical Settings option and click the Next button.
12. The Advanced Settings dialog box options appear. These additional settings allow you to configure the following options:
    - Telephony settings
    - Regional settings
    - Languages
    - Browser and shell settings
    - Installation folder
    - Install printers
    - A command that will run once the first time a user logs on
    - Additional commands that should be run at the end of unattended setup
13. The Setup Information File Text dialog box appears. This dialog box allows you to give the answer file a descriptive name and help text. Enter the name in the Description String text box and the help text in the Help String text box. Click Finish to continue.
14. The Setup Manager dialog box appears. Specify the path and file name you want to use to save your answer file, then click the OK button.
15. When you see the Completing Setup Manager dialog box, click the Finish button.

An answer file can be used to provide automated answers for a CD-based installation. Simply create a new answer file named `winnt.sif` and copy it to a floppy. Insert the Windows XP Professional CD and set the BIOS to boot from CD. As the installation begins, Windows XP will look for `winnt.sif` and use it as the answer file.

Manually Editing Unattended Answer Files

In addition to creating answer files through Setup Manager, you can edit or create your answer files through a text editor program. Answer files consist of section headers, parameters, and values for the parameters. You do not have to specify every option through your answer file if the option is not required by the installation. Following is a sample answer file, `Unattended.txt`.

```
;SetupMgrTag
[Data]
    AutoPartition=1
    MsDosInitiated="0"
    UnattendedInstall="Yes"

[Unattended]
    UnattendMode=ProvideDefault
    OemPreinstall=Yes
    TargetPath=\Windows

[GuiUnattended]
    AdminPassword=abc
    OEMSkipRegional=1
    TimeZone=4

[UserData]
    FullName="Test User"
    OrgName="ABC Corp"
    ComputerName=SJ-UserTest

[TapiLocation]
    CountryCode=1
    AreaCode=408

[SetupMgr]
    DistFolder=C:\winXPdist
```

```
    DistShare=winXPdist

[Identification]
    JoinDomain=SJ-CORP
    DomainAdmin=administrator
    DomainAdminPassword=test

[Networking]
    InstallDefaultComponents=Yes
```

The Setup Manager utility allows you to configure answer files through a GUI interface. However, it has limitations on what can be configured, and many additional options can be configured by manually editing the answer files in a text editor (such as Notepad). In the following sections, you will learn how to configure settings for the following options:

- Mass storage devices
- Plug and Play devices
- HALs
- Passwords
- Language, regional, and time zone settings
- Display settings
- NTFS conversion
- Application installation
- Windows product activation
- Dynamic updates
- Driver signing

MASS STORAGE DEVICES

If you have a mass storage device on the remote computer and it is recognized and supported by Windows XP, you need not specify anything in the answer file for mass storage devices. However, if the device has a driver that is not shipped with the Windows XP Professional CD, possibly because the device is brand new, you can configure the device under the `[MassStorageDrivers]` section of the answer file.

Here are the steps to configure mass storage devices:

1. The distribution folder that contains the remote image files (all the files that will be used by the remote installation) must have a folder that was manually created called `\$OEM$`. Within the `\$OEM$` folder, create a folder called `Textmode` and copy into it the Windows XP mass storage device driver that was provided by the device manufacturer. The driver files should include files with extensions of `*.sys`, `*.dll`, `*.inf`, and `*.cat`, and the `Txtsetup.oem` file. If you specified additional Plug and Play drivers in the `[PnPdrvrs]` section heading, you would also copy the Plug and Play driver files to the `\$OEM$` folder.

2. Within your answer file, create a [MassStorageDrivers] section. The parameters and values to be set within the Txtsetup.oem file should be provided by the manufacturer of the mass storage device.
3. Within your answer file, create a section named [OEMBootFiles] that includes a list of all of the driver files that are in the \OEM\Textmode folder. For example, a device named driver might be configured as follows:

```
[OEMBootFiles]
   driver.sys
   driver.dll
   driver.inf
   Txtsetup.oem
```

4. In the [Unattended] section, include OemPreinstall=Yes.

PLUG AND PLAY DEVICES

If you have a Plug and Play device that does not have a driver included on the Windows XP Professional CD, you can add the driver to the unattended installation as follows:

1. Within the \$OEM$\$1 subfolder, create a folder that will be used to store the Plug and Play drivers—for example, \$OEM$\$1\PnPdrivers. You may even want to create subdirectories for specific devices, such as \$OEM$\$1\PnPdrivers\Modems.
2. In the answer file, edit the [Unattended] section heading to reflect the location of your Plug and Play drivers. For example, if you installed your Plug and Play modem in \$OEM$\$1\PnPdrivers\Modems and your sound card in \$OEM$\$1\PnPdrivers\SoundCards, your answer file would have the following line:

```
[Unattended]
   OEMPnPDriversPath=PnPdrivers\Modems;
   PnPdrivers\SoundCards
```

If the drivers you are installing are not digitally signed, you will have to configure the driver-signing policy within the [Unattended] section of the answer file as DriverSigningPolicy=Ignore. Use unsigned drivers with caution, as they have not been tested by Microsoft and could cause operating system instability.

HALS

If you want to use alternate HALs, follow these steps:

1. Create a folder called \OEM\Textmode (or verify that one exists).
2. Copy any files that are provided by the HAL vendor into the Textmode folder.
3. Edit the [Unattended] section of the answer file based on the instructions from the HAL manufacturer.

PASSWORDS

If you are upgrading a Windows 98 or Windows Millennium Edition (Me) computer to Windows XP Professional, you can customize the answer file to set passwords for the user accounts. You can also opt to force users to change their passwords during the first logon.

Table 1.3 explains the options that can be configured for passwords.

TABLE 1.3 Password Options for Answer Files

Answer File Section	Key	Usage	Example
`[Win9xUpg]`	`DefaultPassword`	Sets a password to whatever you specify, for all computers that are upgraded from Windows 98 or Windows Me to Windows XP Professional	`DefaultPassword=`*`password`*
`[Win9xUpg]`	`ForcePassword`	Forces all users who have upgraded from Windows 98 or Windows Me to change their password the first time they log on	`ForcePasswordChange=Yes`
`[Win9xUpg]`	`UserPassword`	Forces specific users to change their passwords on their local accounts when they log on to Windows XP Professional for the first time after upgrading from Windows 98 or Windows Me	`UserPassword=`*`user,password,user,password`*
`[GuiUnattended]`	`AdminPassword`	Sets the local administrator password	`AdminPassword=`*`password`*

LANGUAGE, REGIONAL, AND TIME ZONE SETTINGS

The `[RegionalSettings]` section heading is used to set language and regional settings. Time zone settings are in the `[GUIUnattended]` section under the `TimeZone` option.

To set regional settings for answer files, you must copy the appropriate language files to the computer's hard disk. This can be accomplished by using the `/copysource:`*`lang`* switch with `Winnt32`, or the `/rx:`*`lang`* switch with `Winnt`. Table 1.4 lists the options that can be set for the `[RegionalSettings]` section.

TABLE 1.4 Regional Setting Options for Answer Files

Option	Description
`InputLocale`	Specifies the input locale and the keyboard layout for the computer
`Language`	Specifies the language and locale that will be used by the computer
`LanguageGroup`	Specifies default settings for the `SystemLocale`, `InputLocale`, and `UserLocale` keys
`SystemLocale`	Allows localized applications to run and to display menus and dialog boxes in the language selected
`UserLocale`	Controls settings for numbers, time, and currency

To set the time zone, you edit the `[GuiUnattended]` section of the answer file as follows:

```
[GuiUnattended]
    TimeZone=TimeZone
```

DISPLAY SETTINGS

The `[Display]` section of the answer file is normally used to customize the display settings for portable computers. You should verify that you know what the proper settings are before you set this option. Table 1.5 lists the options that can be set in this section of the answer file.

TABLE 1.5 Display Setting Options for Answer Files

Option	Description
`BitsPerPel`	Specifies the number of valid bits per pixel for the graphics device
`Vrefresh`	Sets the refresh rate for the graphics device that will be used
`Xresolution`	Specifies the horizontal resolution for the graphics device that will be used
`Yresolution`	Specifies the vertical resolution for the graphics device that will be used

NTFS CONVERSION

You can configure the answer file to automatically convert FAT16 or FAT32 partitions during the installation. To convert the drives, you add the following entry:

```
[Unattended]
    FileSystem=ConvertNTFS
```

APPLICATION INSTALLATION

You can install applications through unattended installations in a variety of ways. Following are some of the options you can choose:

- Use the `Cmdlines.txt` file to add applications during the GUI portion of setup.
- Within the answer file, configure the `[GuiRunOnce]` section to install an application the first time a user logs on.
- Create a batch file.
- Use the Windows Installer.
- Use the `Sysdiff` tool to install applications that do not have automated installation routines. To use the Sysdiff method, install Windows XP Professional on a reference computer and take a snapshot of the base configuration. Then add your applications and take another snapshot of the reference computer with the differences. The difference file (difference between first snapshot and second snapshot) can then be applied to computers that are being installed through unattended installations.

WINDOWS PRODUCT ACTIVATION

Windows XP Professional includes a new feature called Windows Product Activation, which is used to prevent software piracy. You can create an entry within the answer file that supplies a unique product key for each computer that will be deployed within a mass deployment. To set Windows Product Activation, you must create a separate answer file for each computer, and use the value `ProductKey` under the `[UserData]` section of each specific user file. Under the `[Unattended]` section of the answer file, the `Autoactivate=Yes` parameter can be used to automate product activation.

DYNAMIC UPDATES

Dynamic updates are used to provide reliability and compatibility improvements to Windows XP Professional after the operating system CD has been released. You can apply dynamic updates to automated installations through Dynamic Update Packages. Dynamic Update Packages can be downloaded from the Microsoft website. You apply dynamic updates through the `[Unattended]` section of the answer file under `Dushare=`*`path to update share`* key and value.

DRIVER SIGNING

When drivers are applied to Windows XP Professional, they are checked to see if the driver has been digitally verified and signed. Drivers that are signed by Microsoft have passed extensive testing and are verified to be non-harmful to your system. Driver signing options can be set to Ignore, Warn, or Block. To set driver signing within an answer file, you use the `[Unattended]` section and the `DriverSigningPolicy` key.

Exam Essentials

Understand the features and uses of RIS. Know when it is appropriate to use RIS to manage unattended installations. Be able to list the requirements for setting up RIS servers and RIS clients. Be able to complete an unattended installation using RIS.

Be able to use disk images for unattended installations. Know how to perform unattended installations of Windows XP Professional using the System Preparation Tool and disk images.

Know how to use Setup Manager to create answer files. Understand how to access and use Setup Manager to create answer files. Be able to edit the answer files and know the basic options that can be configured for answer files.

Upgrade from a Previous Version of Windows to Windows XP Professional

To upgrade to Windows XP Professional, you must follow a particular path. Only the following operating systems can be directly upgraded to Windows XP Professional:

- Windows 98 (all releases)
- Windows Me
- Windows NT 4 Workstation (requires Service Pack 4 or higher)
- Windows 2000 Professional

There is no supported direct upgrade path for Windows 3.*x*, Windows 95, Windows NT 3.51, or any version of NT 4 Server or Windows 2000 Server.

The hardware requirements for upgrading are the same as those for a clean installation. To upgrade to Windows XP Professional, your computer hardware must meet the following requirements:

- Pentium 233MHz or higher processor (300MHz or higher is recommended)
- 64MB of RAM (128MB or higher memory is recommended)
- 1.5GB of available hard disk space (2GB or more is recommended)
- VGA or better resolution monitor (SVGA is recommended)

Critical Information

The following upgrade checklist (valid for upgrading from Windows 98 or Windows Me, Windows NT 4 Workstation, and Windows 2000 Professional) will help you plan and implement a successful upgrade strategy.

- Verify that your computer meets the minimum hardware requirements for Windows XP Professional. Be sure that all of your hardware is on the HCL.
- Run the Windows XP Upgrade Advisor tool from the Microsoft website, which also includes documentation on using the utility, to audit the current configuration and status

of your computer. It will generate a report of any known hardware or software compatibility issues based on your configuration. You should resolve any reported issues before you upgrade to Windows XP Professional.

- Back up your data and configuration files. Before you make any major changes to your computer's configuration, you should back up your data and configuration files and then verify that you can successfully restore your backup.
- Delete any unnecessary files or applications, and clean up any program groups or program items you don't use.
- Verify that there are no existing problems with your drive prior to the upgrade. Perform a disk scan, a current virus scan, and defragmentation.
- Uncompress any partitions that have been compressed with DriveSpace or DoubleSpace. You cannot upgrade partitions that are currently compressed.
- Once you verify that your computer and components are on the HCL, make sure that you have the Windows XP drivers for the hardware. You can verify this with the hardware manufacturer.
- Make sure that your BIOS is current. Windows XP requires that your computer has the most current BIOS. If it does not, the computer may not be able to use advanced power-management features or device-configuration features. In addition, your computer may cease to function during or after the upgrade. Use caution when performing BIOS updates, as installing the incorrect BIOS can cause your computer to fail to boot.
- Take an inventory of your current configuration. This inventory should include documentation of your current network configuration, the applications that are installed, the hardware items and their configuration, the services that are running, and any profile and policy settings.
- Perform the upgrade. In this step, you upgrade from your previous operating system to Windows XP Professional.
- Verify your configuration. After Windows XP Professional has been installed, use the inventory to compare and test each element that was inventoried prior to the upgrade to verify that the upgrade was successful.

Migrating Existing User Environments to a New Installation

Windows XP Professional ships with a utility called the *User State Migration Tool (USMT)* that is used by administrators to migrate users from one computer to another via command-line utilities.

In the following sections you will learn more about the USMT, requirements for the USMT, and how the USMT tool is used.

Overview of the User State Migration Tool

The USMT consists of two executable files, `ScanState.exe` and `LoadState.exe`. These files are located on the Windows XP Professional distribution CD under the `\valueadd\Msft\Usmt`

folder. In addition, there are four migration rule information files: `Miggapp.inf`, `Migsys.inf`, `Miguser.inf`, and `Sysfiles.inf`. The purpose of these files is as follows:

- `ScanState.exe` collects user data and settings information based on the configuration of the `Migapp.inf`, `Migsys.inf`, `Miguser.inf`, and `Sysfiles.inf` files.
- `LoadState.exe` then deposits the information that is collected from the source computer to a computer running a fresh copy of Windows XP Professional.

This process cannot be run on a computer that has been upgraded to Windows XP Professional.

The information that is migrated includes the following: Internet Explorer settings, Outlook Express settings and store, Outlook settings and store, Dial-up connections, Phone and modem options, Accessibility, Classic Desktop, screen saver selection, Fonts, Folder options, Taskbar settings, Mouse and keyboard settings, Sounds settings, Regional options, Office settings, Network drives and printers, Desktop folder, My Documents folder, My Pictures folder, Favorites folder, Cookies folder, and Common Office file types.

Requirements for the User State Migration Tool

In order to use the USMT, minimum requirements need to be met for the source computer, the intermediate store device, and the destination computer.

The source computer requirements are as follows:

- The source computer must be running one of the following operating systems: Windows 95, Windows 98, Windows Me, Windows NT 4 Workstation, or Windows 2000 Professional.
- The source computer must have access to the intermediate store, which holds the configuration information until it is transferred to the destination computer. Examples of intermediates store devices are tape drive or CD-RW device. The intermediate store that is used must have sufficient free storage to save all of the information that will be transferred.

The destination computer requirements are as follows:

- The destination computer must be running Windows XP Professional.
- The destination computer must have access to the intermediate store.
- The destination computer must have sufficient disk space to accommodate the user state data that is being transferred.

Using the User State Migration Tool

In its simplest form, the USMT is used in the following manner:

1. `ScanState.exe` is run on the source computer, and the user state data is copied to an intermediate store. The intermediate store (for example, a CD-RW) must be large enough to accommodate the data that will be transferred. `ScanState` is commonly executed as a shortcut sent to the user that they will deploy in the evening or through a scheduled script.

2. The target computer is installed with a fresh copy of Windows XP Professional.
3. `LoadState.exe` is run on the target computer, and the intermediate store is accessed to restore the user settings.

Migrating Files and Settings

Windows XP Professional ships with a utility called the *File and Settings Transfer (FAST) Wizard* that is used by administrators to migrate files and settings from one computer to another. This option is used when you purchase a new computer with Windows XP Professional already installed and you want to migrate files and settings from an existing computer that is running a previous version of Windows.

The settings that can be transferred include

- Personalized settings for Internet Explorer
- Personalized settings for Microsoft Outlook Express
- Desktop settings
- Display settings
- Dial-up connection settings

The FAST Wizard works through the following process:

1. On the source computer that contains the files and settings to be transferred, you access the File and Transfer and File Settings Wizard on the Windows XP Professional CD, from the `\Support\Tools` folder through Windows Explorer. Double-click the `Fastwiz.exe` command to start the wizard. The wizard will walk you through the process of selecting the files and settings that will be transferred and the media that will be used for storing the files and settings.
2. Files and settings will be copied to an intermediate storage device—for example, tape or CD-RW.
3. The target Windows XP Professional computer uses Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ File and Settings Transfer Wizard to start the transfer to their computer. The wizard will walk them through the process of locating the files and settings that are to be transferred.

Exam Essentials

Know how to use the USMT and what actions can be accomplished through this utility. Be able to use the ScanState utility to copy user state data to a file server and then use the LoadState utility to apply user state data to client computers.

Be able to transfer data and custom settings from an older computer to a new or existing computer that has Windows XP Professional installed. Know how to use the FAST Wizard and understand what information can be transferred using it.

Perform Post-Installation Updates and Product Activation

Once you are done with the Windows XP Professional installation, you can keep your operating system up-to-date through post-installation updates. Product activation is Microsoft's way of reducing software piracy.

Critical Information

You can perform post-installation updates of Windows XP Professional through Windows Update. *Windows Update* is a utility that connects to Microsoft's website and checks to ensure that you have the most up-to-date version of XP Professional files. To access Windows Update, confirm that your computer is connected to the Internet and access Start ➢ Help and Support. From the Help and Support dialog box, select Windows Update. Your computer will be scanned, and a list of suggested downloads will be customized and listed for you to select from. Some of the common update categories include

- Critical updates and Service Packs
- Windows XP updates
- Drivers

You can deploy the latest Windows XP updates and drivers during installation through the following steps:

1. Download the latest updates and drivers through Windows Update and save them to a network share point.
2. When you install Windows XP using `Winnt` or `Winnt32`, use the /DUShare option to point to the location of the network share that contains the Windows Update files.

Service Packs are updates to the Windows XP operating system that include bug fixes and product enhancements. Some of the options that might be included in Service Packs are security fixes or updated versions of software, such as Internet Explorer.

You can download Service Packs from Microsoft.com or you can pay for a CD of the Service Pack to be mailed to you. Before you install a Service Pack, you should read the Release Note that is provided for each Service Pack on Microsoft's website.

Windows Service Packs are distributed as self-extracting files. You can install a Service Pack simultaneously with a Windows XP Professional installation or you can apply a Service Pack to the operating system after it has been installed.

- If you are installing Windows XP Professional and the Service Pack at the same time, you would use the `Winnt` or `Winnt32` command-line utilities.
- If you were installing a Service Pack after you had installed Windows XP, you would need to extract the Service Pack files, and then use the Update command-line utility with the `–s` switch and point to the location of the Service Pack files.

Performing Product Activation

Unless you have a corporate license for Windows XP Professional, you will need to perform post-installation activation. This can be done online or through a telephone call. After Windows XP is installed, you will be prompted to activate the product. There is a 30-day grace period when you will be able to use the operating system without activation. After the grace period expires, you will not be able to successfully log on to the computer without activation if you restart or log out of the computer. When the grace period runs out, the Product Activation Wizard will automatically start; it will walk you through the activation process.

Exam Essentials

Be able to install Windows Updates during the installation process. You should know how to download the Windows Update files to a network share and use the local network share to install the Windows Update files during a Windows XP Professional installation.

Know how to keep Windows current by using Service Packs. Be able to apply a Service Pack during installation or after Windows XP has been installed.

Know how to activate Windows XP. Understand that Microsoft has a 30-day grace period for activating Windows XP Professional. After 30 days with no product activation, users will not be able to log on to the Windows XP operating system.

Troubleshoot Failed Installations

In the following sections, you will learn more about troubleshooting and correcting common installation problems. Specifically you will learn about

- Troubleshooting installation problems that relate to the `Boot.ini` file
- Ensuring that the computer boot device is properly configured
- Installing non-supported hard drives
- Troubleshooting installation errors using installation log files
- Using the default desktop in Windows XP Professional
- Uninstalling Windows XP Professional

Critical Information

If the text-based portion of the installation completes successfully, but the GUI-based portion of the installation fails, the error may be caused by a device driver that is failing to load properly. If you suspect that this is causing the installation error, you can edit a file called `Boot.ini` to list the drivers that are being loaded during the boot process. The `Boot.ini` file is located in the root of the system partition.

In order to cause the device drivers to be listed during the boot process, you need to edit the `Boot.ini` file to include the `/sos` switch, as shown here:

```
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS = "Microsoft Windows XP
Professional" /sos
```

Ensuring That Computer Boot Device Is Properly Configured

If your computer has multiple boot devices installed, you should ensure that the proper boot order has been configured in the computer BIOS. For example, your computer has an IDE hard drive and a SCSI drive. You can boot your computer successfully to the IDE drive and install Windows XP Professional on the SCSI drive. If the computer is configured to boot to the IDE drive, then when the computer reboots during the installation, you will get an error stating that the computer can't boot. In this case, you would configure the computer's BIOS to boot using the SCSI drive.

Installing Non-Supported Hard Drives

If your computer is using a hard disk that does not have a driver included on the Windows XP Professional CD, you will receive an error message stating that the hard drive cannot be found. You should verify that the hard drive is properly connected and functional. You will need to obtain a disk driver from the manufacturer for Windows XP, then specify that you are using a manufacturer-supplied driver (by pressing the F6 key when prompted) during the text-mode portion of the installation process.

Troubleshooting with Installation Log Files

When you install Windows XP Professional, the Setup program creates several log files. You can view these logs to check for any problems during the installation process. Two log files are particularly useful for troubleshooting:

- The action log includes all of the actions that were performed during the setup process and a description of each action. These actions are listed in chronological order. The action log is stored as `\Windir\setupact.log`.
- The error log includes any errors that occurred during the installation. For each error, there is a description and an indication of the severity of the error. This error log is stored as `\Windir\setuperr.log`.

Default Desktop Used With Windows XP Professional

When you install Windows XP Professional, the default desktop that is used will only display the Recycle Bin. This really isn't an installation error, but users who have used previous versions of Windows may perceive this as an error if they want the traditional icons that appear with Windows (My Computer, My Network Places, My Documents) to be displayed on their desktop. You can configure the desktop to display these icons through Control Panel. First select Display Program, then select the Desktop tab, click Customize Desktop, and then select the icons you want to be displayed on the desktop.

Uninstalling Windows XP Professional

In the event that you upgrade a computer to Windows XP Professional and your installation encounters problems (for example, legacy applications do not work with Windows XP Professional), you can revert to the previous operating system through Control Panel by selecting Add or Remove Programs, selecting Uninstall Windows XP, and then clicking Change/Remove. This will work as long as the original operating system that was upgraded was Windows 98 or Windows Me and that the boot partition was formatted with FAT16 or FAT32.

Exam Essentials

Know how to install Windows XP Professional if you are using an unsupported disk drive. If you are using a disk drive that is not supported by Windows XP Professional, restart the installation and Press F6 when prompted, then supply the disk driver.

Be able to configure your computer's boot device. If your computer has multiple boot devices installed, be able to select the appropriate boot device that Windows XP is using within the computer's BIOS setup.

Know how to configure the desktop to display specific icons. By default, Windows XP Professional will only display the Recycle Bin icon. Users of previous Windows operating systems may perceive this as an installation error, and you should know how to configure the desktop to display traditional Windows desktop icons.

Be able to roll back a computer to its previous operating system if it was upgraded to Windows XP Professional. If you upgrade a computer to Windows XP Professional from Windows 98 or Windows Me, be able to roll back the installation using Control Panel.

Review Questions

1. You have 10 users who have been using Windows 2000 Professional. You just purchased 10 new computers that are running Windows XP Professional. What is the easiest way to migrate the user state data from the Windows 2000 Professional computers to the Windows XP Professional computers?
   - **A.** Use the Windows Backup utility to back up the data from the Windows 2000 Professional computers and then restore it to the Windows XP computers.
   - **B.** Use the `ScanState` utility on the old computers to copy the user state data to a network server, then use the `LoadState` utility on the new computers to restore the user state data.
   - **C.** Copy the users' registry settings from the old computers to a network share, then copy them to the new computers.
   - **D.** Use the `SaveUST` utility on the old computers to copy the user state data to a network server, then use the `RestoreUST` utility on the new computers to restore the user state data.
2. Your computer has three drives, an IDE primary drive and two SCSI drives. You install Windows XP Professional to the first SCSI drive. During the installation, your computer reboots and you receive an error message that the computer can't boot. What is the most likely error?
   - **A.** You need to press F6 when prompted during the installation to supply the SCSI disk driver.
   - **B.** You need to configure your computer's BIOS to boot from the SCSI drive.
   - **C.** You need to restart the installation and use the Recovery Console to supply the SCSI disk driver.
   - **D.** You need to restart the installation and use the Last Known Good option to boot to the correct partition.
3. Your computer is brand new and has the latest SCSI drive. You boot to the Windows XP Professional CD and start the installation. After the system reboots the first time, you get an error message letting you know the installation cannot continue because no hard drives are detected. How do you correct this error?
   - **A.** You need to press F6 when prompted during the installation to supply the SCSI disk driver.
   - **B.** You need to configure your computer's BIOS to boot from the SCSI drive.
   - **C.** Restart the installation and use the Recovery Console to supply the SCSI disk driver.
   - **D.** Restart the installation and use the Last Known Good option to boot to the correct partition.
4. How do you uninstall Windows XP on a computer that has been upgraded from Windows 98?
   - **A.** Use System Restore to restore to the checkpoint that was created prior to Windows XP Professional being installed.
   - **B.** Use the Last Known Good Configuration prior to logging into Windows XP Professional for the first time.
   - **C.** Use Control Panel and select Add or Remove Programs, then select Uninstall Windows XP.
   - **D.** You will have to reinstall Windows 98.

5. Your company has 25 users using Windows XP Professional. You want them to be able to install the latest updates and drivers. You want to do this without creating a large amount of traffic through your ISP. What is the easiest and most cost effective way to make these updates available?
   - **A.** Let the users know they should check Microsoft's website on a regular basis and download any updates.
   - **B.** Download the latest updates to a network share.
   - **C.** Download the latest updates and distribute them to your users via CD.
   - **D.** Deploy the Service Packs using Microsoft SMS services.

6. One of your users asked you to upgrade their Windows 2000 Professional computer to Windows XP Professional. Everything has been working properly for several weeks. This morning when the user tried to log on, they were unable to access Windows XP Professional. What should you do?
   - **A.** Reinstall Windows XP Professional.
   - **B.** Make sure that the latest Service Pack is installed on the user's computer.
   - **C.** Activate the copy of Windows XP Professional.
   - **D.** Instead of logging into the domain, log on to a local account and change the group policy so that the account is not logged out.

7. Your company recently purchased 100 new computers that need to have Windows XP Professional installed on them. You want to use the System Preparation Tool to create an image on a reference computer, which will then be distributed to target computers that will use automated installations. During the installations, you want to automate the responses to the queries generated by the installation process. What is the easiest way to manage this process?
   - **A.** Use a RIS server to host the answer file; the reference computer will automatically use answer files stored on RIS servers.
   - **B.** Create an answer file that is distributed to each target computer via a network connection.
   - **C.** Create an answer file that is distributed to each target computer via a floppy disk.
   - **D.** Create an answer file on the reference computer before the Sysprep utility is run.

8. Your company recently purchased 100 new computers for the Sales department. Each computer needs to be installed with Windows XP Professional, Windows Office 2003, and some customized Sales applications. You want to automate the deployment using the System Preparation Tool to automate the installations. Which of the following options should you use?
   - **A.** Create an image that will be used by Sysprep by installing Windows XP Professional on the reference computer, copying the installation files to the reference computer for each of the applications that need to be installed, and then creating the Sysprep image.
   - **B.** Create an image that will be used by Sysprep by installing Windows XP Professional on the reference computer, installing each of the applications that will be used, and then creating the Sysprep image.
   - **C.** Copy the Windows XP Professional files and the installation files to the reference computer, then create the Sysprep image.
   - **D.** The System Preparation Tool does not allow you to automate the installation of applications.

9. Which of the following services are required on a RIS server? Choose all that apply.
   A. DHCP
   B. DNS
   C. WINS
   D. Active Directory

10. You want to use RIS to install Windows XP Professional on 25 computers that are not PXE enabled. What utility should you use to create a remote boot floppy disk?
   A. `rbfg`
   B. `makeboot`
   C. `RISboot`
   D. `PXEboot`

Answers to Review Questions

1. B. The USMT consists of two executable files, `ScanState.exe` and `LoadState.exe`. `ScanState.exe` collects user data and settings information based on the configuration of the `Migapp.inf`, `Migsys.inf`, `Miguser.inf`, and `Sysfiles.inf` files. `LoadState.exe` then deposits the information that is collected from the source computer to a computer running a fresh copy of Windows XP Professional.

2. B. If your computer has multiple boot devices installed, you should ensure that the proper boot order has been configured in the computer BIOS. If the computer is configured to boot to the IDE drive, then when the computer reboots during the installation, you will get an error stating that the computer can't boot. In this case, you would configure the computer's BIOS to boot using the SCSI drive.

3. A. If your computer is using a hard disk that does not have a driver included on the Windows XP Professional CD, you will receive an error message stating that the hard drive cannot be found. You should verify that the hard drive is properly connected and functional. You will need to obtain a disk driver from the manufacturer for Windows XP, then specify that you are using a manufacturer-supplied driver (by pressing the F6 key when prompted) during the text-mode portion of the installation process.

4. C. In the event that you upgrade a computer to Windows XP Professional and your installation encounters problems (for example, legacy applications do not work with Windows XP Professional), you can revert to the previous operating system through Control Panel by selecting Add or Remove Programs, selecting Uninstall Windows XP, and then clicking Change/Remove. This will work as long as the original operating system that was upgraded was Windows 98 or Windows Me and as long as the boot partition was formatted with FAT16 or FAT32.

5. B. To deploy the updates, download the latest updates and drivers through Windows Update and save them to a network share point. When you install Windows XP using Winnt or Winnt32, use the /DUShare option to point to the location of the network share that contains the Windows Update files.

6. C. Unless you have a corporate license for Windows XP Professional, you will need to perform post-installation activation. This can be done online or through a telephone call. After Windows XP is installed, you will be prompted to activate the product. There is a 30-day grace period when you will be able to use the operating system without activation. After the grace period expires, you will not be able to successfully log on to the computer without activation if you restart or log out of the computer. When the grace period runs out, the Product Activation Wizard will automatically start; it will walk you through the activation process.

7. D. If you have created an answer file for use with disk images, you should save them on the reference computer prior to using the Sysprep utility. This will allow the installation to run without requiring any user input.

8. B. The System Preparation Tool (`Sysprep.exe`) is used to prepare a computer for disk imaging, which can be done with third-party image software or with disk-duplicator hardware. Disk imaging (also sometimes called disk cloning or disk duplication) is the process of creating a reference computer for the automated deployment. The reference, or source, computer has Windows XP Professional installed and is configured with the settings and applications that should be installed on the target computers. An image is then created that can be transferred to other computers, thus installing the operating system, settings, and applications that were defined on the reference computer.

9. A, B, C. The RIS server must be running Windows 2000 Server or Windows Server 2003, with TCP/IP. DHCP, DNS, and Active Directory must be running on the network.

10. A. PXE is a technology that is used to boot to the network when no operating system or network configuration has been installed and configured on a client computer. The RIS boot disk is a PXE ROM emulator for network adapters that don't have a PXE boot ROM or for a PC that doesn't support booting from the network. In order to use a RIS boot disk, the network adapter must be PCI compliant. The RIS boot disk is generated with the Remote Boot Floppy Generator (`rbfg.exe`) utility.

Chapter 2

Implementing and Conducting Administration of Resources

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Monitor, manage, and troubleshoot access to files and folders.**
  - Configure, manage, and troubleshoot file compression.
  - Control access to files and folders by using permissions.
  - Optimize access to files and folders.
- ✓ **Manage and troubleshoot access to shared folders.**
  - Create and remove shared folders.
  - Control access to shared folders by using permissions.
  - Manage and troubleshoot Web server resources.
- ✓ **Connect to local and network print devices.**
  - Manage printers and print jobs.
  - Control access to printers by using permissions.
  - Connect to an Internet printer.
  - Connect to a local print device.
- ✓ **Configure and manage file systems.**
  - Convert from one file system to another file system.
  - Configure NTFS, FAT32, or FAT file systems.
- ✓ **Manage and troubleshoot access to and synchronization of offline files.**

Managing resources is a huge part of network administration. You manage file resources through NTFS permissions and sharing network folders. Network print devices allow multiple users to share network printers. Windows XP allows you to manage file systems based on your needs. You can also use offline folders to make files available to a user, even when they are not connected to the network.

Monitor, Manage, and Troubleshoot Access to Files and Folders

Monitoring, managing, and troubleshooting access to files and folders is a very common administrative task. In this section, you will learn about file compression, NTFS permissions, and optimizing access to files and folders.

Critical Information

Data compression is the process of storing data in a form that takes less space than does uncompressed data. If you have ever "zipped" or "packed" a file, you have used data compression. With Windows XP, data compression is available only on NTFS partitions. You can manage data compression through Windows Explorer or the `Compact` command-line utility.

Files as well as folders in the NTFS file system can be either compressed or uncompressed. Files and folders are managed independently, which means that a compressed folder can contain uncompressed files, and an uncompressed folder can contain compressed files.

Access to compressed files by DOS or Windows applications is transparent. For example, if you access a compressed file through Microsoft Word, the file will be uncompressed automatically when it is opened, and then automatically compressed again when it is closed.

Data compression is available only on NTFS partitions. If you copy or move a compressed folder or file to a FAT partition (or a floppy disk), Windows XP will automatically uncompress the folder or file.

The following steps are used to enable data compression:

1. Select Start ➢ All Programs ➢ Accessories ➢ Windows Explorer.
2. In Windows Explorer, find and select the folder you want to compress.
3. Right-click the folder and select Properties. In the General tab of the folder Properties dialog box, note the value listed for Size on Disk. Then click the Advanced button.

4. In the Advanced Attributes dialog box, check the Compress Contents to Save Disk Space option. Then click the OK button.
5. In the Confirm Attribute Changes dialog box, select the option to Apply Changes to This Folder, Subfolders and Files. (If this confirmation dialog box does not appear, you can display it by clicking the Apply button in the Properties dialog box.) Click the OK button to confirm your changes.
6. In the General tab of the folder Properties dialog box, note the value that now appears for Size on Disk. This size should have decreased because you compressed the folder.

To uncompress folders and files, repeat the steps of this exercise and uncheck the Compress Contents to Save Disk Space option in the Advanced Attributes dialog box.

Setting Disk Quotas

Disk quotas are used to specify the amount of disk space a user is allowed on specific NTFS volumes. You can specify disk quotas for all users, or you can limit disk space on a per-user basis.

Before you administer disk quotas, keep in mind the following aspects of disk quota management:

- Disk quotas can be specified only for NTFS volumes.
- Disk quotas apply only at the volume level, even if the NTFS partitions reside on the same physical hard drive.
- Disk usage is calculated on file and folder ownership. When a user creates, copies, or takes ownership of a file, that user is the owner of the file.
- When a user installs an application, the free space that will be seen by the application is based on the disk quota availability, not on the actual amount of free space on the volume. The user also only sees the space available as defined by the quota limitation.
- The calculation of disk quota space used is based on actual file size. There is no mechanism to support or recognize file compression.

Disk quotas are not applied to or enforced for the Administrator account or for members of the Administrators group.

The following sections describe how to set up and monitor disk quotas.

Configuring Disk Quotas

You configure disk quotas through the NTFS volume Properties dialog box or through from Windows Explorer by right-clicking the drive letter in the Explorer listing and select Properties. In the volume's Properties dialog box, click the Quota tab to see the dialog box shown in Figure 2.1. When you open the Quota tab, you will see that disk quotas are disabled by default.

FIGURE 2.1 The Quota tab of the volume Properties dialog box

Table 2.1 describes the options that can be configured through the Quota tab.

TABLE 2.1 Disk Quota Configuration Options

Option	Description
Enable quota management.	Specifies whether quota management is enabled for the volume.
Deny disk space to users exceeding the quota limit.	Specifies that users who exceed their disk quota will not be able to override their disk allocation. Those users will receive "out of disk space" error messages.
Select the default quota limit for new users on this volume.	Allows you to define quota limits for new users. Options include not limiting disk space, limiting disk space, and specifying warning levels.
Select the quota logging options for this volume.	Specifies whether logged events that relate to quotas will be recorded. You can enable the logging of events for users exceeding quota limits or users exceeding warning limits.

Notice the traffic light icon in the upper-left corner of the Quota tab. It indicates the status of disk quotas, as follows:

- A red light means that disk quotas are disabled.
- A yellow light means that Windows XP is rebuilding disk quota information.
- A green light means that the disk quota system is enabled and active.

The next sections explain how to set quotas for all new users as default quotas, and how to set quotas for a specific user.

Setting Default Quotas

When you set default quota limits for new users on a volume, those quotas apply only to users who have not yet created files on that volume. Users who already own files or folders on the volume will be exempt from the quota policy. Users who have not yet created a file on the volume will be bound by the quota policy.

To set the default quota limit for new users, access the Quota tab of the volume Properties dialog box and check the Enable Quota Management box. Click the Limit Disk Space To radio button, and enter a number in the first box next to the option. In the drop-down list in the second box, specify whether disk space is limited by KB (kilobytes), MB (megabytes), GB (gigabytes), TB (terabytes), PB (petabytes), or EB (exabytes). If you choose to limit disk space, you can also set a warning level, so that users will be warned if they come close to reaching their limit.

If you want to apply disk quotas for all users, apply the quota when the volume is first created. That way, no users will have already created files on the volume, and thus, they will not be exempt from the quota limit.

Setting an Individual Quota

You can also set quotas for individual users. There are several reasons for setting quotas this way:

- You can set restrictions on other users and at the same time allow a user who routinely updates your applications to have unlimited disk space.
- You can set warnings at lower levels for a user who routinely exceeds disk space.
- You can apply the quota to users who already had files on the volume before the quota was implemented and thus have been granted unlimited disk space.

To set an individual quota, click the Quota Entries button in the bottom-right corner of the Quota tab. This brings up the dialog box shown in Figure 2.2. To modify a user's quota, double-click that user. This brings up a dialog box similar to the one shown in Figure 2.3. Here, you can specify whether the user's disk space should be limited, and you can set the limit and the warning level. If the user does not appear in the Quota Entries dialog box, you can add them by selecting Quota ➢ New Quota Entry and specifying the user through the Select Users dialog box.

FIGURE 2.2 The Quota Entries for Volume dialog box

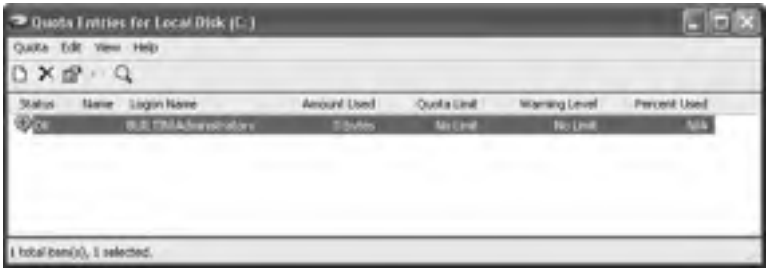


FIGURE 2.3 The quota settings for a user

Monitoring Disk Quotas

If you implement disk quotas, you will want to monitor the quotas on a regular basis. This allows you to check disk usage by all users who own files on the volume with those quotas applied.

Disk quota monitoring is accomplished through the Quota Entries dialog box (see Figure 2.2), which appears when you click the Quota Entries button in the Quota tab of the volume Properties dialog box. The dialog box shows the following information:

- The status of the user's disk quota, represented as follows:
  - A green arrow in a dialog bubble means the status is OK.
  - An exclamation point in a yellow triangle means the warning threshold has been exceeded.
  - An exclamation point in a red circle means the user threshold has been exceeded.
- The name and logon name of the user who has stored files on the volume
- The amount of disk space consumed by the user on the volume
- The user's quota limit
- The user's warning level
- The percentage of disk space consumed by the user in relation to their disk quota

Controlling Access to Files and Folders by Using Permissions

NTFS permissions control access to NTFS files and folders. This is based on the technology that was originally developed for Windows NT. Ultimately, the person who owns the object has complete control over the object. You configure access by allowing or denying NTFS permissions to users and groups. Normally, NTFS permissions are cumulative, based on group memberships if

the user has been allowed access. However, if the user had been denied access through user or group membership, those permissions override the allowed permissions. Windows XP Professional offers five levels of NTFS permissions:

Full Control

This permission allows the following rights:

- Traverse folders and execute files (programs) in the folders. The ability to traverse folders allows you to access files and folders in lower subdirectories, even if you do not have permissions to access specific portions of the directory path.
- List the contents of a folder and read the data in a folder's files.
- See a folder's or file's attributes.
- Change a folder's or file's attributes.
- Create new files and write data to the files.
- Create new folders and append data to files.
- Delete subfolders and files.
- Delete files.
- Compress files.
- Change permissions for files and folders.
- Take ownership of files and folders.

If you select the Full Control permission, all permissions will be checked by default, and can't be unchecked.

Modify

This permission allows the following rights:

- Traverse folders and execute files in the folders.
- List the contents of a folder and read the data in a folder's files.
- See a file's or folder's attributes.
- Change a file's or folder's attributes.
- Create new files and write data to the files.
- Create new folders and append data to files.
- Delete files.

If you select the Modify permission, the Read & Execute, List Folder Contents, Read, and Write permissions will be checked by default and can't be unchecked.

Read & Execute

This permission allows the following rights:

- Traverse folders and execute files in the folders.
- List the contents of a folder and read the data in a folder's files.
- See a file's or folder's attributes.

If you select the Read & Execute permission, the List Folder Contents and Read permissions will be checked by default, and can't be unchecked.

List Folder Contents

This permission allows the following rights:

- Traverse folders.
- List the contents of a folder.
- See a file's or folder's attributes.

Read

This permission allows the following rights:

- List the contents of a folder and read the data in a folder's files.
- See a file's or folder's attributes.
- View ownership.

Write

This permission allows the following rights:

- Overwrite a file.
- View file ownership and permissions.
- Change a file's or folder's attributes.
- Create new files and write data to the files.
- Create new folders and append data to files.

Any user with Full Control access can manage the security of a folder. However, to access folders, a user must have physical access to the computer as well as a valid logon name and password. By default, regular users can't access folders over the network unless the folders have been shared. Sharing folders is covered in the "Managing Network Access" section later in this chapter.

You apply NTFS permissions through Windows Explorer. Right-click the file or folder to which you want to control access, and select Properties from the pop-up menu. This brings up the file's or folder's Properties dialog box. Figure 2.4 shows a folder Properties dialog box.

The tabs in the file or folder Properties dialog box depend on the options that have been configured for your computer. For files and folders on NTFS partitions, the dialog box will contain a Security tab, which is where you configure NTFS permissions. (The Security tab is not present in the Properties dialog box for files or folders on FAT partitions, because FAT partitions do not support local security.) The Security tab lists the users and groups that have been assigned permissions to the file or folder. When you click a user or group in the top half of the dialog box, you see the permissions that have been allowed or denied for that user or group in the bottom half of the dialog box.

FIGURE 2.4 The Properties dialog box for a folder

If the Security tab does not appear for your NTFS partition, and you are not a part of a domain, then Simple File Sharing is probably enabled, which will keep this option from appearing. To disable Simple File Sharing, select My Computer ➢ Tools ➢ Folder Options. In Advanced Settings, clear the box for Use Simple File Sharing (Recommended).

In the following subsections you will learn how to implement NTFS permissions and how to control permission inheritance.

Adding and Removing User and Group NTFS Permissions

To manage NTFS permissions, take the following steps:

1. In Windows Explorer, right-click the file or folder to which you want to control access, select Properties from the pop-up menu, and click the Security tab of the Properties dialog box.
2. Click the Add button to open the Select Users or Groups dialog box, as shown in Figure 2.5. You can select users from the computer's local database or from the domain you are in (or trusted domains) by typing in the user or group name in the Enter the Object Name to Select portion of the dialog box; then click the Add button.
3. You return to the Security tab of the folder Properties dialog box. Highlight each user, computer, or group in the top list box individually, and in the Permissions list, specify the NTFS permissions to be allowed or denied. When you are finished, click the OK button.

FIGURE 2.5 The Select Users or Groups dialog box

Through the Advanced button of the Security tab, you can configure more granular NTFS permissions, such as Traverse Folder, Execute File, and Read Attributes permissions.

To remove the NTFS permissions for a user, computer, or group, highlight that entity in the Security tab and click the Remove button.

Controlling Permission Inheritance

Normally, the directory structure is organized in a hierarchical manner. This means you are likely to have subfolders in the folders to which you apply permissions. In Windows XP Professional, by default, the parent folder's permissions are applied to any files or subfolders in that folder, as well as any subsequently created objects. These are called inherited permissions.

You can specify how permissions are inherited by subfolders and files through the Advanced options from the Security tab of the folder Properties dialog box, by checking the Advanced button. This calls up the Permissions tab of the Advanced Security Settings dialog box, as shown in Figure 2.6. The options that can be selected include

- Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.
- Replace permission entries on all child objects with entries shown here that apply to child objects.

If an Allow or a Deny check box in the Permissions list in the Security tab has a shaded check mark, this indicates that the permission was inherited from an upper-level folder. If the check mark is not shaded, it means the permission was applied at the selected folder. This is known as an explicitly assigned permission. Knowing which permissions are inherited and which are explicitly assigned is useful when you need to troubleshoot permissions.

FIGURE 2.6 The Permissions tab of the Advanced Security Settings dialog box

Understanding Ownership and Security Descriptors

When an object is initially created on an NTFS partition, an associated security descriptor is created. A security descriptor contains the following information:

- The user or group that owns the object
- The users and groups that are allowed or denied access to the object
- The users and groups whose access to the object will be audited

After an object is created, the *owner* of the object has full permissions to change the information in the security descriptor, even for members of the Administrators group. You can view the owner of an object from the Security tab of the specified folder's Properties) and click the Advanced button (shown in Figure 2.4). Then click the Owner tab to see who the owner of the object is, as shown in Figure 2.7. From this dialog box you can change the owner of the object.

While the owner of an object can set the permissions of an object so that the Administrator can't access it, the Administrator or any member of the Administrators group can take ownership of an object, and thus manage its permissions. When you take ownership of an object, you can specify whether you want to replace the owner on subdirectories and objects of the object. The new owner of the NTFS object will have Full Control permission and any existing permissions that have been applied to the object will be lost.

Optimizing Access to Files and Folders

You can optimize access to files and folders through the use of NTFS permissions and through sharing folders over the network. You will learn how to share folders for network access in the next section.

FIGURE 2.7 The Owner tab of the Advanced Security Settings dialog box

Exam Essentials

Understand how file compression is used to manage disk space. Be able to compress and uncompress folders and files as needed.

Be able to apply and use disk quotas. Even though this is not a specific test objective, you may see questions on how disk quotas are implemented. You should know how these are applied and used to manage disk space.

Understand how NTFS permissions are implemented. Know what is allowed by each NTFS permission. Know how NTFS permissions work together through user and group memberships. Be able to determine what effective rights are based on what has been allowed and what has been denied through NTFS permissions.

Know how ownership is used on NTFS objects. If an NTFS object becomes inaccessible, know how to take ownership of the object. Understand how NTFS permissions are effected when you take ownership of an object.

Manage and Troubleshoot Access to Shared Folders

Sharing is the process of allowing network users to access a folder located on a Windows XP Professional computer. A network share provides a single location to manage shared

data used by many users. Sharing also allows an administrator to install an application once, as opposed to installing it locally at each computer, and to manage the application from a single location.

The following sections describe how to create and manage shared folders, configure share permissions, and provide access to shared resources. You will also learn how to manage a shared folder through a web server.

Critical Information

To create a *shared folder*, you must be logged on as a member of the Administrators or Power Users group (or Server Operators if you are a part of a domain). You enable and configure sharing through the Sharing tab of the folder Properties dialog box, as shown in Figure 2.8.

When you share a folder, you can configure the options listed in Table 2.2.

TABLE 2.2 Share Folder Options

Option	Description
Do Not Share This Folder	Makes the folder available only through local access
Share This Folder	Makes the folder available through local access and network access
Share Name	A descriptive name by which users will access the folder
Comment	Additional descriptive information about the share (optional)
User Limit	The maximum number of connections to the share at any one time (default is to allow up to 10 users access to a share on a Windows XP Professional computer)
Permissions	How users will access the folder over the network
Caching	How folders are cached when the folder is offline

If you share a folder and then decide that you do not want to share it, just select the Do Not Share This Folder radio button in the Sharing tab of the folder Properties dialog box.

In Windows Explorer, you can easily tell that a folder has been shared by the hand icon under the folder.

FIGURE 2.8 The Sharing tab of the folder Properties dialog box

In addition:

- Only folders, not files, can be shared.
- Share permissions can be applied only to folders and not files.
- If a folder is shared over the network and a user is accessing it locally, then share permissions will not apply to the local user.
- If a shared folder is copied, the original folder will still be shared, but not the copy.
- If a shared folder is moved, the folder will no longer be shared.
- If the shared folder will be accessed by a mixed environment of clients including some that do not support long filenames, you should use the 8.3 naming format for files.
- Folders can be shared through the `Net Share` command-line utility.

The following steps are used to create a shared folder:

1. Right-click the folder you want to share and select Properties.
2. Click the Sharing tab. In the Sharing tab Properties dialog box, click the Share This Folder radio button.
3. Type in the Share Name within text box.
4. Optionally you can configure a comment and the maximum number of users that can access the share.

Controlling Access to Shared Folders by Using Permissions

You can control users' access to shared folders by assigning *share permissions*. Share permissions are less complex than NTFS permissions and can be applied only to folders (unlike NTFS permissions, which can be applied to files and folders).

To assign share permissions, click the Permissions button in the Sharing tab of the folder Properties dialog box. This brings up the Share Permissions dialog box, as shown in Figure 2.9.

FIGURE 2.9 The Share Permissions dialog box

You can assign three types of share permissions:

Full Control Allows full access to the shared folder.

Change Allows users to change data within a file or to delete files.

Read Allows a user to view and execute files in the shared folder.

Read is the default permission on shared folders for the Everyone group.

Shared folders do not use the same concept of inheritance as NTFS folders. If you share a folder, there is no way to block access to lower-level resources through share permissions.

The following steps are used to apply permissions to a shared folder:

1. Right-click the shared folder, select Sharing and Security, and from the Sharing tab click the Permissions button.
2. In the Share Permissions dialog box, click the Add button.
3. In the Select Users and Groups dialog box, type in the user or group you want to add permissions for and click the OK button. Select the permissions you want to apply to the user or group and click the OK button.

Managing and Troubleshooting Web Server Resources

Windows XP Professional comes with *Internet Information Services (IIS)*, which allows you to create and manage websites. This software provides a wide range of options for configuring the content, performance, and access controls for your websites. IIS can be used to publish resources on the Internet or a private intranet.

The IIS software that is included with Windows XP Professional is designed for small-scale use, mainly for users who are developing web services for home or office use. IIS Professional version edition can support only 10 incoming client connections. IIS Professional version also does not support all of the features of IIS that are included with the server versions of IIS. In previous versions of Windows client operating systems, the scaled-down version of IIS was called Peer Web Services (PWS). Windows XP Professional does not ship with PWS, and if you upgraded to Windows XP Professional, then PWS can't be upgraded. The IIS Professional version software is included with Windows XP Professional, but is not installed by default.

In this section, you will learn how to install IIS and how to configure and manage website properties. The final section includes tips for troubleshooting problems with website access.

Installing Internet Information Services

IIS is installed on a Windows XP computer through the Add or Remove Programs option in Control Panel. Before you can install IIS, your computer must have TCP/IP installed and configured. To install IIS on a Windows XP Professional computer, you take the following steps:

1. Select Start ➢ Control Panel ➢ Add or Remove Programs.
2. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.
3. In the Windows Components dialog box, check the Internet Information Services box and click the Next button.
4. Configuration changes will be made to your computer and files will be copied. You may be prompted to provide the Windows XP Professional CD.
5. The Completing the Windows Components Wizard dialog box will appear. Click the Finish button.

Managing a Website

To access Internet Information Services, select Start ➢ Administrative Tools ➢ Internet Information Services.

Through Internet Information Services, you can configure many options for your website, such as website identification and connection settings, performance settings, and access controls. To access a website's properties, right-click the website you want to manage in the Internet Information Services window and select Properties from the pop-up menu.

The website Properties dialog box has eight tabs with options for configuring and managing your website. The options that relate to managing files and folders are

Web Site Allows you to configure website identification, connections, and logging.

Home Directory Allows you to configure the content location, access permissions, content control, and application settings.

Directory Security Allows you to configure anonymous access and authentication control, IP address and domain name restrictions, and secure communications.

Setting Website Properties

The Web Site tab includes options for identifying the website, controlling connections, and enabling logging.

The description of the website appears in the Internet Information Services window. By default, the website description is the same as the name of the website. You can enter another description in the Description text box.

You also configure the IP address that is associated with the site. The IP address must already be configured for the computer. If you leave the IP address at the default setting of All Unassigned, all of the IP addresses that are assigned to the computer and that have not been assigned to other websites will be used.

The TCP port specifies the port that will be used to respond to HTTP requests by default. The default TCP port that is used is TCP port 80. If you change this value, clients attempting to connect to the website must specify the correct port value. This option can be used for additional security.

Common ports that are used by IIS and can be modified for additional security include FTP on port 21, Telnet on port 23, and HTTP on port 80.

Configuring Home Directory Options

The Home Directory tab, shown in Figure 2.10, includes options for the content location, access permissions, content control, and application settings.

FIGURE 2.10 The Home Directory tab of the website Properties dialog box

CONTENT LOCATION

The home directory is used to provide web content. The default directory is called `inetpub\wwwroot`. You have three choices for the location of the home directory:

- A directory on the local computer
- A share on another computer (stored on the local network and identified by a UNC name)
- A redirection to a resource using a URL

ACCESS PERMISSIONS AND CONTENT CONTROL

Access permissions define what access users have to the website. Content control specifies whether logging and indexing are enabled. By default, users have only Read access, and logging and indexing are enabled. The access permissions and content control options are described in Table 2.3.

TABLE 2.3 Access Permissions and Content Control Options

Option	Description
Script Source Access	Allows users to access source code for scripts, such as ASP (Active Server Pages) applications, if the user has either Read or Write permissions.
Read	Allows users to read or download files located in your home folder. This is used if your folder contains HTML files. If your home folder contains CGI applications or ISAPI applications, you should uncheck this option so that users can't download your application files.
Write	Allows users to modify or add to your web content. This access should be granted with extreme caution.
Directory Browsing	Allows users to view website directories. This option is not commonly used because it exposes your directory structure to users who access your website without specifying a specific HTML file.
Log Visits	Allows you to log access to your website. In order to log access, the Enable Logging box in the Web Site tab of the Properties dialog box also must be checked.
Index This Resource	Allows you to index your home folder for use with the Microsoft Indexing Service.

Web service access permissions and NTFS permissions work together. The more restrictive of the two permissions will be the effective permission.

APPLICATION SETTINGS

Application, in this context, is defined as the starting point of a specific folder (and its subfolder and files) that has been defined as an application. For example, if you specify that your home folder is an application, every folder in your content location can participate in the application.

The Execute Permissions setting specifies how applications can be accessed within this folder. If you select None, no applications or scripts can be executed from this folder. The Scripts Only setting allows you to run script engines, even if no execute permissions have been set. This permission is used for folders that contain ASP scripts. The other option is Scripts and Executables, which allows all file types (including binary files with `.exe` and `.dll` extensions) to be executed.

The Application Protection setting specifies how applications will be run. There are three choices:

- Low (IIS Process) means that the application runs in the same process as the web service.
- Medium (Pooled) means that the application is run in an isolated pooled process with other applications.
- High (Isolated) means that each application runs as a separate isolated application.

Setting Directory Security

The Directory Security tab, shown in Figure 2.11, includes options for anonymous access and authentication control, IP address and domain name restrictions, and secure communications.

FIGURE 2.11 The Directory Security tab of website Properties dialog box

Sharing Web Folders through Folder Properties

Once you have installed IIS on your Windows XP Professional computer, you can easily share the folders through the folder properties. Select the Web Sharing tab, as shown in Figure 2.12. To share the folder you select either

- Share On (select the website that will host the shared folder) or
- Share This Folder radio button

When you click the Share This Folder radio button, you can configure the alias that will be used, the access permissions, and the application permissions as shown in Figure 2.13.

FIGURE 2.12 The Web Sharing tab of a folders Properties dialog box

FIGURE 2.13 The Edit Alias dialog box

Troubleshooting Website Access

If users are unable to access your website, the problem may be caused by improper access permissions, an improperly configured home folder or default document, or use of the wrong TCP port. Here are some tips for troubleshooting website access problems:

- Determine whether anonymous access is allowed. If so, verify that the username and password that have been configured through IIS match the name of the user account and password that are in the Windows XP, Windows 2000 domain, or Windows 2003 domain user database.
- Confirm that access has not been denied based on the IP address or domain name.
- Make sure that the proper access permissions have been configured.
- Confirm that the home folder is properly configured and that the default document has been properly configured.
- Make sure that the TCP port is set to port 80 or that you are accessing the website using the proper TCP port number.
- Make sure that the NTFS permissions have not been set on the home folder so that they deny access to website users.

Exam Essentials

Be able to create and remove a shared folder. Know what permissions are required to create a shared folder. Know what properties can be configured for a shared folder.

Know how to control access to shared folders by using permissions. Be able to determine what effective permissions will be when NTFS and share permissions have been applied to the same folder.

Be able to share folders through a web server. Know how to install IIS and manage folders and folder permissions through a web server.

Connect to Local and Network Print Devices

This section covers how to manage print devices. You will learn how to manage a *printer*, manage print jobs, and connect to an Internet printer.

Critical Information

Administrators or users with the Manage Printers permission can manage the printer's servicing of print jobs and of the print documents in a print queue. When you manage a printer, you manage all the documents in a queue. When you manage print documents, you manage specific documents.

As you would expect, you manage printers and print documents from the Printers and Faxes utility (select Start ➢ Printers and Faxes). The following sections describe the printer management and print document management options.

Managing Printers

To manage a printer, right-click the printer you want to manage. From the pop-up menu (Figure 2.14), select the appropriate option for the area you want to manage. Table 2.4 describes these options.

TABLE 2.4 Printer Management Options

Option	Description
Set as Default Printer	Specifies the default printer that will be used when the user does not send a job to an explicit printer (if the computer is configured to access multiple printers).
Printing Preferences	Brings up the Printing Preferences dialog box, which allows you to configure printer settings for page layout and paper quality. You can also access this dialog box through the General tab of the printer Properties dialog box, as described earlier in this chapter.
Pause Printing	While a printer is paused, print jobs can be submitted to the printer, but they will not be forwarded to the print device until you resume printing (by unchecking this option). You might use Pause Printing when you need to troubleshoot the printer or maintain the print device.
Sharing	Allows the printer to be shared or not shared.
Use Printer Offline	Pauses the printer. Print documents will remain in the print queue, even if you restart the computer.
Create Shortcut	Allows you to create a shortcut for the printer, which would typically be placed on the desktop.
Delete	Removes the printer. You might use this option if you no longer need the printer, if you want to move the printer to another print server, or if you suspect the printer is corrupt and you want to delete and re-create it.
Rename	Allows you to rename the printer. You might use this option to give a printer a more descriptive name or a name that follows naming conventions.
Properties	Allows you to manage the properties of a printer.

FIGURE 2.14 The printer management options

Managing Printer Properties

Printer properties allow you to configure options such as the printer name, whether the printer is shared, and printer security. To access the printer Properties dialog box, open the Printers folder, right-click the printer you want to manage, and choose Properties from the pop-up menu.

As shown in Figure 2.15, the printer Properties dialog box has at least six tabs: General, Sharing, Ports, Advanced, Security, and Device Settings. The following sections describe the properties on these tabs.

FIGURE 2.15 Printer Properties dialog box

The Properties dialog boxes for some printers will contain additional tabs to allow advanced configuration of the printer.

Configuring General Properties

The General tab of the printer Properties dialog box contains information about the printer. It also lets you set printing preferences and print test pages. The information here (name of the printer, its location, and comments about it) reflects your entries when you set the printer up (as described in the preceding section). You can add or change this information in the text boxes.

Configuring Sharing Properties

The Sharing tab of the printer Properties dialog box allows you to specify whether the computer will be configured as a local printer (do not share) or as a shared network printer (share this printer). If you choose to share the printer, you also need to specify a share name, which will be seen by the network users. By default, Windows XP will suggest a share name that is eight characters or less, so that the printer will be accessible by MS-DOS workstations. However, if you are in an environment that does not have MS-DOS workstations that will attach to your printer share, you can create longer share names.

Configuring Port Properties

Windows XP Professional supports local ports (physical ports) and standard TCP/IP ports (logical ports). A port is defined as the interface that allows the computer to communicate with the print device. Local ports are used when the printer attaches directly to the computer. In the case where you are running Windows XP Professional in a small workgroup, you would likely run printers attached to the local port LPT1. Standard TCP/IP ports are used when the printer is attached to the network by installing a network card in the printer. The advantage of network printers is that they are faster than local printers and can be located anywhere on the network. When you specify a TCP/IP port, you must know the IP address of the network printer.

In the Ports tab, shown in Figure 2.16, you configure all the ports that have been defined for printer use. Along with deleting and configuring existing ports, you can also set up printer pooling and redirect print jobs to another printer, as described in the next sections.

PRINTER POOLING

Printer pools are used to associate multiple physical print devices with a single logical printer. You would use a printer pool if you had multiple physical printers in the same location that were the same type and could use a single print driver. The advantage of using a printer pool is that the first available print device will print your job. This is useful in situations where a group of print devices is shared by a group of users, such as a secretarial pool.

All of the print devices in a printer pool must be able to use the same print driver.

FIGURE 2.16 The Ports tab of the printer Properties dialog box

To configure a printer pool, click the Enable Printer Pooling check box at the bottom of the Ports tab, and then check all the ports to which the print devices in the printer pool will attach. If you do not select the Enable Printer Pooling option, you can select only one port per printer.

REDIRECTING PRINT JOBS TO ANOTHER PRINTER

If your print device fails, you can redirect all the jobs scheduled to be printed at that print device, to another print device that has been configured as a printer. For this redirection to work, the second print device must be able to use the same print driver as the first print device.

To redirect print jobs, click the Add Port button in the Ports tab, click the New Port button. In the Port Name dialog box, type the UNC name of the printer that you want to redirect the jobs to, in the format **`\\computername\printer`**.

Configuring Advanced Properties

The Advanced tab of the printer Properties dialog box, shown in Figure 2.17, allows you to control many characteristics of the printer. You can configure the following options:

- The availability of the printer
- The priority of the printer
- The driver the printer will use
- Spooling properties
- How documents are printed
- Printing defaults
- The print processor that will be used
- The separator page

FIGURE 2.17 The Advanced tab of the printer Properties dialog box

These options are covered in the following sections.

PRINTER AVAILABILITY

Availability, or scheduling, specifies when a printer will service jobs. Usually, you control availability when you have multiple printers that use a single print device. For example, you might use this option if you have large jobs that tie up the print device for extended periods of time. You could schedule the large jobs to print only during a specified time, say between 10:00 p.m. and 4:00 a.m.

To set this up, you could create two printers on the same port, perhaps printers named LASER and REPORTS on the LPT1 port. (Both printers are on the same port since the same physical print device services them.) You would configure LASER to always be available, and REPORTS to be available only from 10:00 p.m. to 4:00 a.m. You would then instruct your users to send short jobs to LASER and long jobs to REPORTS, with the understanding that print jobs sent to REPORTS would print only during the specified hours.

By default, the Always Available radio button in the Advanced tab is selected, so users can use the printer 24 hours a day. To limit the printer's availability, select the Available From radio button and specify the range of time when the printer should be available.

PRINTER PRIORITY

Priority is another option that you might configure if you have multiple printers that use a single print device. When you set priority, you specify how jobs are directed to the print device. For example, you might use this option when two groups share a printer and you need to control the priority by which the device prints incoming jobs. In the Advanced tab of the printer Properties dialog box, you can set the Priority value to a number from 1 to 99, with 1 as the lowest priority and 99 as the highest priority.

As an example, suppose that the accounting department uses a single print device. The managers there want their print jobs always to print before jobs created by the other accounting department staff. To configure this arrangement, you could create a printer called MANAGERS on port LPT1 with a priority of 99. You would then create a printer on port LPT1 called WORKERS with a priority of 1. Through the Security tab of the printer Properties dialog box, you would allow only managers to use the MANAGERS printer and allow the other accounting users to use the WORKERS printer (Security tab options are covered later in this chapter). When the print manager polls for print jobs, it will always poll the higher-priority printer before the lower-priority printer.

The print manager is responsible for polling the print queue for print jobs and directing the print jobs to the correct port.

PRINT DRIVER

The Driver setting in the Advanced tab shows the *print driver* that is associated with your printer. If you have configured multiple printers on the computer, you can choose to use any of the installed drivers. Clicking the New Driver button starts the Add Printer Driver Wizard, which allows you to update or add new print drivers.

SPOOLING

When you configure spooling options, you specify whether print jobs are spooled or sent directly to the printer. *Print spoolers* are used to save the print jobs to disk in a queue before they are sent to the printer. Consider spooling as the traffic controller of printing—it keeps all the print jobs from trying to print at the same time.

By default, spooling is enabled, with printing beginning immediately. Your other option is to wait until the last page is spooled before printing. An analogy for these choices is the actions you can take in a grocery store's cashier line. Let's say you have an entire cart full of groceries and the guy behind you has only a few things. Even if you've started loading your groceries onto the belt, as long as the cashier hasn't started with your items, you can choose to let the person with fewer items go before you, or you can make him wait. If the cashier has already started totaling your groceries, then you don't have that choice. Windows XP Professional spooling options allow you to configure your print environment similarly.

In the Advanced tab, you can leave the Start Printing Immediately option selected, or you can choose the Start Printing After Last Page Is Spooled option. If you choose the latter option, a smaller print job that finishes spooling first will print before your print job, even if your job started spooling before it did. If you specify Start Printing Immediately, the smaller job will have to wait until your print job is complete.

The other spooling option is Print Directly to the Printer, which bypasses spooling altogether. This option doesn't work well in a multiuser environment where multiple print jobs are sent to the same device. However, it is useful in troubleshooting printer problems. If you can print to a print device directly, but you can't print through the spooler, then you know that your spooler is corrupt or has other problems.

PRINT OPTIONS

The Advanced tab of a printer's properties contains check boxes for four print options:

Hold Mismatched Documents Is useful when you're using multiple forms with a printer. By default, this feature is disabled and jobs are printed on a first-in-first-out (FIFO) basis. You might enable this option if you need to print on both plain paper and certificate forms. Then all the jobs with the same form will print first.

Print Spooled Documents First Specifies that the spooler will print jobs that have finished spooling before large jobs that are still spooling, even if that large print job has a higher priority. This option is enabled by default, which increases printer efficiency.

Keep Printed Documents Specifies that print jobs should not be deleted from the print spooler (queue) when they are finished printing. By default, this option is disabled. You normally want to delete the print jobs as they print, because saving print jobs can take up substantial disk space.

Enable Advanced Printing Features Specifies that any advanced features supported by your printer, such as Page Order and Pages Per Sheet, should be enabled. By default, this option is turned on. You would disable it if compatibility problems occurred. For example, if you are using the driver for a similar print device that does not support all the features of the print device the driver was written for, you should disable the advanced printing features.

PRINT PROCESSOR

Print processors are used to specify whether Windows XP Professional needs to do additional processing to print jobs.

SEPARATOR PAGES

Separator pages are used at the beginning of each document to identify the user who submitted the print job. If your printer is not shared, a separator page is generally a waste of paper. If the printer is shared by many users, the separator page can be useful for distributing finished print jobs.

Device Settings Properties

The properties that you see on the Device Settings tab of the printer Properties dialog box depend on the printer and print driver that you have installed. You might configure these properties if you want to manage the associations of forms to tray assignments. For example, you could configure the upper tray to use letterhead and the lower tray to use regular paper.

Managing Print Documents

As an Administrator or a user with the Manage Printers or Manage Documents permission, you can manage print documents within a print queue. For example, if a user has sent the same job multiple times, you might need to delete the duplicate print jobs.

To manage print documents, in the Printers folder double-click the printer that contains the documents. This opens a dialog box with information about the documents in its print queue. Select Document from the menu bar to access the pull-down menu of options that you can use to manage documents, as shown in Figure 2.18. These menu options are described in Table 2.5.

FIGURE 2.18 The Document menu options

Controlling Access to Printers by Using Permissions

You can control which users and groups can access Windows XP printers by configuring the print permissions. In Windows XP Professional, you can allow or deny access to a printer. If you deny access, the user or group will not be able to use the printer, even if their user or group permissions allow such access.

You assign print permissions to users and groups through the Security tab of the printer Properties dialog box, as shown in Figure 2.19. Table 2.6 defines the print permissions that can be assigned.

TABLE 2.5 Document Management Options

Option	Description
Pause	Places the printing of this document on hold
Resume	Allows the document to print normally (after it has been paused)
Restart	Resends the job from the beginning, even if it has already been partially printed
Cancel	Deletes the job from the print spooler
Properties	Brings up the document Properties dialog box, containing options such as user notification when a print job is complete, document priority, document printing time, page layout, and paper quality

FIGURE 2.19 The Security tab of the printer Properties dialog box

TABLE 2.6 Print Permissions

Print Permission	Description
Print	A user or group can connect to a printer and can send print jobs to it.
Manage Printers	Allows administrative control of the printer. With this permission, a user or group can pause and restart the printer, change the spooler settings, share or unshare a printer, change print permissions, and manage printer properties.
Manage Documents	Allows users to manage documents by pausing, restarting, resuming, and deleting queued documents. Users cannot control the status of the printer.
Special Permissions	Special Permissions are used to customize the print options with allow or deny access of the following permissions: Print, Manage Printers, Manage Documents, Read Permissions, Change Permissions, and Take Ownership.

By default, whenever a printer is created, default print permissions are assigned. The default permissions are normally appropriate for most network environments. Table 2.7 shows the default print permissions that are assigned.

TABLE 2.7 Default Print Permissions

Group	Print	Manage Printers	Manage Documents
Administrators	X	X	X
Power Users	X	X	X
Creator Owner	X		X
Everyone	X		

In the next sections, you will learn about assigning print permissions, advanced settings, and driver setting properties in detail.

Usually, you can accept the default print permissions, but you might need to modify them for special situations. For example, if your company bought an expensive color laser printer for the marketing department, you probably wouldn't want to allow general access to that printer. In this case, you would deselect the Allow check box for the Everyone group, add the Marketing group to the Security tab list, and then allow the Marketing group the Print permission.

To add print permissions, take the following steps:

1. In the Security tab of the printer Properties dialog box, click the Add button.
2. The Select Users or Groups dialog box appears. In the Enter the Object Names to Select section, type in the user or group name that you want to add. After you specify all the users and groups you want to assign permissions to, click the OK button.
3. Highlight the user or group you want to manage permissions for. Select Allow or Deny Access for the Print, Manage Printers, and Manage Documents permissions. Click the OK button when you are finished assigning permissions.

To remove an existing group from the permissions list, highlight the group and click Remove. That group will no longer be listed in the Security tab and cannot be assigned permissions.

Connecting to an Internet Printer

Windows XP automatically supports Internet printing when IIS is installed on a Windows Server 2003 or a Windows XP Professional client. Any printers that are shared on the Windows XP Server are then automatically made accessible to Internet users through a protocol called Internet Printing Protocol (IPP). Windows XP clients automatically include IPP print support, and the users can browse and print to Internet printers through Internet Explorer 4.01 or higher.

To install a printer from the Internet or an intranet, use the printer's URL as the name of the printer. To support all browsers, an administrator must choose basic authentication. Internet Explorer supports LAN Manager Challenge/Response and Kerberos version 5 authentication.

Adding an Internet Printer

To install an Internet printer on a Windows Server 2003 or Windows XP Professional client, you must first install IIS; then you can create a shared printer. Once you have created a shared printer, complete the following steps:

1. Select Start ➢ Printers and Faxes.
2. In the Printers folder, click the Add a Printer option.
3. The Welcome to the Add Printer Wizard starts. Click the Next button.
4. The Local or Network Printer dialog box appears. Select A Network Printer, Or A Printer Attached To Another Computer, and click the Next button.
5. The Specify a Printer dialog box appears. Click the Connect to a Printer on the Internet or on a Home or Office Network option. In the URL box, type **`http://`*`computername`*`/printers/`*`share_name`*`/.printer`** and click the Next button.

Connecting to an Internet Printer Using a Web Browser

You can manage printers from any browser, but you must use Internet Explorer 4.01 or later to connect to a printer using a browser (the browser must support frames).

To connect to an Internet printer using a web browser, take the following steps:

1. Open the web browser, type **`http://print_server/printers`** in the address bar, and press Enter. If prompted, type your username, domain name, and password.
2. Click the link for the printer you want to connect to.
3. Under Printer Actions, click Connect.

Connecting to a Local Print Device

Users can access a local printer or a shared printer. Once a printer has been shared, users with the Print permission can connect to the network printer through their network connection.

To connect to a network printer, access My Computer from the Start menu and from Other Places, click My Network Places, expand Entire Network, and click View Entire Contents. Expand Microsoft Windows Network, then Workgroup, then *computername*. Finally, double-click the printer to connect to it.

Exam Essentials

Be able to create and manage printers. Know how to configure your printer to use printer pooling, set up scheduling, and set print priorities.

Be able to control access to printers through permissions. Be able to assign appropriate permissions to different users and groups to control how printers are accessed.

Know how to manage printing through the Internet. Be able to send and manage print jobs through the Internet.

Configure and Manage File Systems

Your file system is used to store and retrieve the files stored on your hard drive. Windows XP Professional supports the *FAT16*, *FAT32*, and NTFS file systems. You should choose FAT16 or FAT32 if you want to dual-boot your computer, because these file systems are backward compatible with other operating systems. Choose NTFS, however, if you want to take advantage of features such as local security, file compression, and file encryption.

Critical Information

Table 2.8 summarizes the capabilities of each file system, and they are described in more detail in the following sections.

TABLE 2.8 File System Capabilities

Feature	FAT16	FAT32	NTFS
Supporting operating systems	Most	Windows 95 OSR2, Windows 98, Windows Me, Windows 2000, Windows XP, and Windows Server 2003	Windows NT, Windows 2000, Windows XP, and Windows Server 2003
Long filename support	Yes	Yes	Yes
Efficient use of disk space	No	Yes	Yes
Compression support	No	No	Yes
Quota support	No	No	Yes
Encryption support	No	No	Yes

TABLE 2.8 File System Capabilities *(continued)*

Feature	FAT16	FAT32	NTFS
Support for local security	No	No	Yes
Support for network security	Yes	Yes	Yes
Maximum volume size	2GB	32GB	2TB

Converting from One File System to Another File System

In Windows XP, you can convert both FAT16 and FAT32 partitions to NTFS. File system conversion is the process of converting one file system to another without the loss of data. If you format a drive as another file system, as opposed to converting that drive, all the data on that drive will be lost.

To convert a partition, you use the *Convert* command-line utility. The syntax for the `Convert` command is as follows:

```
Convert [drive:] /fs:ntfs
```

For example, if you wanted to convert your D: drive to NTFS, you would type the following from a command prompt:

```
Convert D: /fs:ntfs
```

When the conversion process begins, it will attempt to lock the partition. If the partition cannot be locked—perhaps because the partition contains the Windows XP operating system files or the system's page file—the conversion will not take place until the computer is restarted.

You can use the `/v` switch with the `Convert` command. This switch specifies that you want to use verbose mode, and all messages will be displayed during the conversion process. You can also use the `/NoSecurity` switch, which specifies that all converted files and folders will have no security applied by default, so they can be accessed by anyone.

Configuring NTFS, FAT32, or FAT File Systems

When you create a disk partition through the Disk Management utility, you can format it as a FAT or NTFS file system. Once you format the partition, the only thing you configure are NTFS options, which were defined earlier in this chapter.

Exam Essentials

Be able to convert a FAT partition to NTFS. Know all of the options associated with converting a FAT partition to NTFS.

Manage and Troubleshoot Access to and Synchronization of Offline Files

Through the Offline Files tab of the Folder Options dialog box (Figure 2.20), you can configure your Windows 2000 Server or Windows Server 2003 computer to use offline files and folders. This feature allows network files and folders to be stored on Windows XP clients. Then if the network location is not available, users can still access network files. In earlier versions of Windows, users who tried to access a network folder would receive an error message. With offline folders, users can still access the network folder even when they are not attached to the network.

Offline files and folders are particularly useful for mobile users who use the same set of files when they are attached to the network and when they are traveling. Offline files and folders are also useful on networks where users require specific files to perform their jobs, because they will be able to access those files even if the network server goes down (for scheduled maintenance or because of a power outage or another problem). Offline files and folders also improve performance even when the network is available, because users can use the local copy of the file instead of accessing files over the network.

FIGURE 2.20 The Offline Files tab of the Folder Options dialog box

Critical Information

Configuring offline files and folders requires a minimum of two computers:

- The network computer that contains the network version of the files and folders
- The Windows XP client computer that will access the network files while they are online or offline

To use offline files and folders, you must complete the following tasks:

1. Attach to the shared file or folder that you want to access offline.
2. Configure your computer to use offline files and folders.
3. Make files and folders available for offline access.
4. Specify how offline files and folders will respond to network disconnection.

Configuring Folders for Offline Access

You configure your computer to use offline files and folders through the Offline Files tab of the Folder Options dialog box (see Figure 2.20). In this tab, verify that the Enable Offline Files box is checked (this option is enabled by default). To configure automatic synchronization between the offline and online files, make sure that the Synchronize All Offline Files before Logging Off option is checked (this option is also enabled by default). To use this option, you must disable the Fast User Switching option in Control Panel under User Accounts.

On the Offline Files tab, you can also configure several other options. These include the reminder balloon options that are associated with offline files, the amount of disk space that can be used by offline files, whether a shortcut is created for offline files on the desktop, and whether you want to encrypt the offline files local cache.

If you don't configure offline files and folders to be synchronized automatically when you log on to or log off from your computer, you will need to perform the synchronization manually. To manually synchronize a file or folder, right-click the file or folder that has been configured for offline use and select Synchronize from the pop-up menu.

To make a file or folder available for offline access, take the following steps:

1. Access the shared file or folder that you wish to use offline. Right-click the file or folder and select Make Available Offline from the pop-up menu).
2. The Welcome to the Offline Files Wizard starts (this wizard will run only the first time you create an offline file or folder). Click the Next button.
3. The Offline Files Wizard dialog box asks how to synchronize offline files. By default, the option to Automatically Synchronize the Offline Files When I Log On and Log Off My Computer is selected. If you would prefer to manually synchronize files, deselect this option. Click the Next button to continue.
4. The next Offline Files Wizard dialog box allows you to configure reminders and to create a shortcut to the Offline Files folder. Reminders periodically prompt you that you are not connected to the network and are working offline. The Offline Files shortcut is an easy way

to access folders that have been configured for offline use. If you are online when you access this folder, you are working online. You can select or deselect either of these options. Then click the Finish button.

5. If the folder you have selected contains subfolders, you will see the Confirm Offline Subfolders dialog box. This dialog box allows you to choose whether the subfolders should also be made available offline. Make your selection and click the OK button.

The offline files will be copied (synchronized) to the local computer.

Preventing a Folder from Being Accessed Offline

Once a computer has been configured to support offline files and folders, you can access any share that has been configured with default properties. If you create a share and you do not want the files to be accessible offline, you can configure the share properties for offline access through the share's caching properties.

Files are manually cached when a computer makes a request to a file or folder on the network that has been made available for offline access. By default, the Manual Caching for Documents setting is enabled. The default cache size for automatically cached files is 10 percent of the total disk space of the hard disk. If files are marked as manually cached, they are automatically marked as Always Available Offline In The Offline Files folder.

To configure the offline folder's caching, access the share's Properties dialog box (Folder Properties, Sharing tab). Click the Caching button. In the Caching Settings dialog box (Figure 2.21), uncheck the option Allow Caching of Files in This Shared Folder. With this option disabled, users can access the data while they are on the network, but they can't use the share offline.

By default, `*.sim`, `*.mdb`, `*.ldb`, `*.mdw`, `*.mde`, `*.pst`, and `*.db?` are not cached. You can override this setting or specify which files will not be cached through Group Policy.

FIGURE 2.21 Caching Settings for a shared folder

Configuring Your Computer's Behavior after Losing the Network Connection

Through the Offline Files tab of the Folder Options dialog box, you can specify whether your computer will begin working offline when a network connection is lost. To make this setting, click the Advanced button in the bottom-right corner of the dialog box. This brings up the Offline Files—Advanced Settings dialog box, as shown in Figure 2.22. Here, you can specify Notify Me and Begin Working Offline (the default selection) or you can select Never Allow My Computer to Go Offline. If you have created offline files and folders for multiple servers, you can use the Exception List portion of the dialog box to specify different behavior for each server.

FIGURE 2.22 The Offline Files—Advanced Settings dialog box

To reconnect to a network share after using offline files, all of the following conditions must be met:

- The network connection must not be a slow link.
- No offline files from the network share can contain changes that require synchronization.
- No offline files from the network share can be open on the user's local computer.

If any of these conditions are not met, the user will continue to work offline even though a network connection is available, and any changes that are made to local files will require synchronization with the network share.

The Offline Files Database

When you enable offline files, the local computer stores information that is related to offline files in the Offline Files Database. By default, this database is stored in the *\systemroot\CSC* folder on the client computer. CSC stands for Client Side Cache and is a term associated with

files that are cached with offline folders. When a user requests a file that is offline, the database mimics the network resource. All file system permissions are maintained by the database. The Offline Files folder is used to display all files stored within the database. Only members of the Administrator group are able to directly access the CSC folder. Files should not be directly deleted through the CSC folder.

The CSC folder can be moved through the `Cachemov` command-line utility. If you move the CSC folder, you must ensure that the location that the cached files will be moved to has adequate disk space and that the user who is using offline files has appropriate permissions to the new location.

Troubleshooting Offline Files

If you are configuring offline files and folders, and you don't see the Make Available Offline option available as a folder property, check the following:

- Are you connected to a network share on a computer that uses SMB (Server Message Blocks)? Offline files and folders won't work from a network computer that does not use SMB.
- Have you configured your computer to use offline files and folders? Before you can make a file or folder available offline, this feature must be enabled through the Offline Files tab of the Folder Options dialog box (select Tools ➢ Folder Options in Windows Explorer).
- Has the folder that you want to access been shared, and do you have proper permissions to access the folder? If you don't see a folder that you want to configure for offline use, it may not be shared or you may not have proper share (and NTFS) permissions to the folder.
- Are files using the extensions `.mdb`, `.ldb`, `.mdw`, `.mde`, or `.db`, which are not synchronized by default?
- If you are a member of the Active Directory, is group policy configured to specify that file extensions you are using are not to be synchronized?
- Do you have network errors that are preventing synchronization?
- Is there sufficient disk space on the client computer to support synchronization?
- Does the user have Read or Write permissions to the files they want to synchronize?

Exam Essentials

Be able to configure, use, and troubleshoot offline folders. Know what steps are required to use offline folders. Configure caching for offline folders. Know how to troubleshoot offline folders.

Review Questions

1. You are the network administrator of a large network. One of your users is running out of disk space on her Windows XP computer. You implement file compression as a way to manage the disk space until you can upgrade her disk drive. Currently the file `Test.doc` is compressed and the user wants to use Microsoft Word to edit the file. What is the easiest way to edit the file?
   - **A.** The user should uncompress the file using Windows Explorer before she edits it.
   - **B.** The user should use the `Extract` command on the file before editing it.
   - **C.** The user should use the `Compact -u` command on the file before editing it.
   - **D.** The file will automatically be uncompressed by Word when it is accessed.

2. Which of the following statements are true when using disk quotas with Windows XP Professional? Choose all that apply.
   - **A.** Disk quotas can be used on NTFS or FAT32 volumes.
   - **B.** Disk quotas can be applied on a per folder basis.
   - **C.** If a user takes ownership of a folder, the space taken up by the folder will be applied to their disk quota.
   - **D.** A user will only see the free space on the disk allowed by their quota settings, not the actual free disk space that is physically available.

3. You are the network administrator of a large network. One of your users recently left the company and you now need to access files on their Windows XP Professional computer. Which of the following statements best describes what will happen when you take ownership of the users NTFS folders?
   - **A.** The NTFS permissions will default to the group Everyone having Full Control permissions.
   - **B.** The new owner will have Full Control permission and all other permissions will be lost.
   - **C.** The new owner will have Full Control permission and all other permissions will be retained.
   - **D.** The NTFS permissions will default to the group Everyone having Read permission and the new owner will have Full Control permission.

4. You use Windows XP Professional within a small workgroup. When you try to share a folder, you don't see a Sharing tab on the folder properties. Which of the following options would allow you to share a folder? Choose all that apply.
   - **A.** Being a member of the Administrators group for the computer
   - **B.** Being the owner of a folder
   - **C.** Having Full Control permissions to the folder
   - **D.** Being a member of the Server Operators group for the computer

5. Your network has three printers that are used by the accounting department. You want the users to be able to send their print jobs and have them printed by the first available printer. Which of the following requirements must be met before you can implement a printer pool?

   A. All of the printers have to be attached directly to the network as opposed to a local computer.

   B. All of the printers have to be able to use the same port.

   C. All of the printers have to be configured with the same IP address.

   D. All of the printers have to be able to use the same print driver.

6. You have just created a shared printer for the Sales group within a Windows XP Professional workgroup. What are the default permissions that will be applied to the new printer? Choose all that apply.

   A. Group Everyone will have Print and Manage Documents permissions applied.

   B. The Administrators group will have all permissions applied by default.

   C. The Creator Owner of a document can print and manage their own documents.

   D. No permissions will be applied to group Everyone.

7. Your company has two offices that connect to each other via the Internet. You want to create a printer that can be accessed through the Internet so a user from a remote office can send print jobs to a printer in the local office. Which of the following options is used to support Internet printers?

   A. IIS

   B. Active Directory

   C. DNS

   D. IEP

8. You want to implement file compression on your D: drive to maximize disk space. The drive is currently configured as FAT32. You want to configure the drive as NTFS without losing any data. Which of the following options should you use?

   A. Convert the drive through the Disk Administrator utility.

   B. Convert the drive through the Windows Explorer utility.

   C. Convert the drive through the `NTFSConfig` utility.

   D. Convert the drive through the `Convert` utility.

9. You have configured Offline folders on a Windows 2003 Server within your network. Your Windows XP Professional users should be able to use offline folders with the shares on the server, with the exception of the `\\Server2\Contacts` folder, which should only be able to be accessed from the network. How do you disable offline folders for the Contacts folder?

A. From the Sharing tab, click the Caching button and do not allow caching of files within this folder.

B. From the Sharing tab, unclick the following option: Allow This Folder to Be Accessed Offline.

C. Modify the NTFS permissions of the folder to disallow offline access.

D. Modify the share permissions of the folder to disallow offline access.

10. You use Windows XP Professional on a laptop computer. You use offline files to manage your data when you work from home. Your disk has been partitioned with a C: and D: drive. Your C: drive is running out of disk space and you are having trouble with the offline files. You want to move the offline file storage from your C: drive to your D: drive. Which of the following options should you use?

A. Windows Explorer utility

B. `Offline` command line utility

C. `Cachemov` command line utility

D. Disk Administrator utility

Answers to Review Questions

1. D. Access to compressed files by DOS or Windows applications is transparent. For example, if you access a compressed file through Microsoft Word, the file will be uncompressed automatically when it is opened, and then automatically compressed again when it is closed.

2. C, D. Disk quotas can be specified only for NTFS volumes. Disk quotas apply only at the volume level, even if the NTFS partitions reside on the same physical hard drive. Disk usage is calculated on file and folder ownership. When a user creates, copies, or takes ownership of a file, that user is the owner of the file. When a user installs an application, the free space that will be seen by the application is based on the disk quota availability, not on the actual amount of free space on the volume. The user also only sees the space available as defined by the quota limitation. The calculation of disk quota space used is based on actual file size. There is no mechanism to support or recognize file compression.

3. B. While the owner of an object can set the permissions of an object so that the administrator can't access the object, the administrator or any member of the Administrators group can take ownership of an object, and thus manage the object's permissions. When you take ownership of an object, you can specify whether you want to replace the owner on subdirectories and objects of the object. The new owner of the NTFS object will have Full Control permission and any existing permissions that have been applied to the object will be lost.

4. A, D. To share a folder, you must be logged on as a member of the Administrators or Power Users group (or Server Operators if you are a part of a domain). You enable and configure sharing through the Sharing tab of the folder's Properties dialog box.

5. D. Printer pools are used to associate multiple physical print devices with a single logical printer. You would use a printer pool if you had multiple physical printers in the same location that were the same type and could use a single print driver. The advantage of using a printer pool is that the first available print device will print your job. This is useful in situations where a group of print devices is shared by a group of users, such as a secretarial pool.

6. B, C. By default Administrators and Power Users have Print, Manage Printers, and Manage Documents print rights when a printer is created. The Creator Owner has Print and Manage Documents (for their own documents). The Everyone group has print permission.

7. A. To install an Internet printer on a Windows Server 2003 or Windows XP Professional client, you must first install IIS.

8. D. In Windows XP, you can convert both FAT16 and FAT32 partitions to NTFS. File system conversion is the process of converting one file system to another without the loss of data.

9. A. To configure the offline folder's caching, access the share's Properties dialog box (Folder Properties, Sharing tab). Click the Caching button. In the Caching Settings dialog box, uncheck the option Allow Caching of Files in This Shared Folder. With this option disabled, users can access the data while they are on the network, but they can't use the share offline.

10. C. The CSC folder can be moved through the `Cachemov` command-line utility. If you move the CSC folder, you must ensure that the location that the cached files will be moved to has adequate disk space and that the user who is using offline files has appropriate permissions to the new location.

Chapter 3

Implementing and Conducting Administration of Resources

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Implement, manage, and troubleshoot disk devices.**
  - Install, configure, and manage DVD and CD-ROM devices.
  - Monitor and configure disks.
  - Monitor, configure, and troubleshoot volumes.
  - Monitor and configure removable media, such as tape devices.
- ✓ **Implement, manage, and troubleshoot display devices.**
  - Configure multiple-display support.
  - Install, configure, and troubleshoot a video adapter.
- ✓ **Configure Advanced Configuration Power Interface (ACPI).**
- ✓ **Implement, manage, and troubleshoot input and output (I/O) devices.**
  - Monitor, configure, and troubleshoot I/O devices, such as printers, scanners, multimedia devices, mouse, keyboard, and smart card reader.
  - Monitor, configure, and troubleshoot multimedia hardware, such as cameras.
  - Install, configure, and manage modems.
  - Install, configure, and manage Infrared Data Association (IrDA) devices.
  - Install, configure, and manage wireless devices.

- Install, configure, and manage USB devices.
- Install, configure, and manage hand held devices.
- Install, configure, and manage network adapters.

✓ **Manage and troubleshoot drivers and driver signing.**

✓ **Monitor and configure multiprocessor computers.**

In this chapter you will learn how to manage resources. Resources include disk devices, display devices, power options, I/O devices, drivers and driver signing, and multiple processors.

Implement, Manage, and Troubleshoot Disk Devices

In this section you will learn how to manage disk devices. Disk devices include hard drives, DVDs, CD-ROMs, and removable media. You will also learn how disks can be configured and how to configure and troubleshoot volumes.

Critical Information

You can manage disk devices through the *Device Manager* utility. DVDs and CD-ROMs are listed together under DVD/CD-ROM Drives in Device Manager. Double-click DVD/CD-ROM Drives, then double-click the device you wish to manage. This brings up the device Properties dialog box, which has five tabs:

General Lists the device type, manufacturer, and location. It also shows the device status, which indicates whether the device is working properly. If the device is not working properly, you can click the Troubleshoot button at the lower right of the dialog box to get some help with resolving the problem.

Properties Allows you to set options such as volume and playback settings.

DVD Region Plays regionally encoded DVDs for a maximum of five regional changes.

Volumes Is used to display CD properties such as disk, type, status, partition style, capacity, unallocated space, and reserved space.

Driver Shows information about the currently loaded driver, as well as buttons that allow you to see driver details, uninstall the driver, roll back the driver, or update the driver.

Right-clicking DVD/CD-ROM Drives in Device Manager allows you the option of updating the driver, disabling the device, uninstalling the device, scanning for hardware changes, or viewing the properties of the device.

Monitoring and Configuring Disks and Volumes

Windows XP Professional supports two types of disk storage: *basic storage* and *dynamic storage*. Basic storage is backward compatible with other operating systems and can be configured to support up to four partitions. Dynamic storage is supported by Windows 2000, Windows XP, and Windows Server 2003 and allows storage to be configured as volumes. The following sections describe the basic storage and dynamic storage configurations.

Basic Storage

Basic storage consists of primary and extended partitions. The first partition that is created on a hard drive is called a *primary partition*, and is usually represented as drive C:. Primary partitions use all of the space that is allocated to the partition and use a single drive letter to represent the partition. Each physical drive can have up to four partitions. You can set up four primary partitions, or you can have three primary partitions and one *extended partition*. With an extended partition, you can allocate the space however you like, and each sub-allocation of space is represented by a different drive letter.

One of the advantages of using multiple partitions on a single physical hard drive is that each partition can have a different file system. For example, the C: drive might be FAT32 and the D: drive might be NTFS. Multiple partitions also make it easier to manage security requirements.

Laptop computers support only basic storage.

Dynamic Storage

Dynamic storage is a Windows XP feature that consists of a dynamic disk divided into dynamic volumes. Dynamic volumes cannot contain partitions or logical drives, and they are not accessible through DOS.

Dynamic storage supports three dynamic volume types: *simple volumes*, *spanned volumes*, and *striped volumes*. These are similar to disk configurations that were used with Windows NT Workstation 4. However, if you've upgraded from NT Workstation 4, you are using basic storage, and you can't add volume sets. Fortunately, you can upgrade from basic storage to dynamic storage. Windows XP Professional does not support mirrored volumes.

To set up dynamic storage, you create a dynamic disk or upgrade a basic disk to a dynamic disk. Then you create dynamic volumes within the dynamic disk. You create dynamic storage with the Windows XP Disk Management utility, which is discussed after the following descriptions of the dynamic volume types:

Simple Volumes A simple volume contains space from a single dynamic drive. The space from the single drive can be contiguous or noncontiguous. Simple volumes are used when you have enough disk space on a single drive to hold your entire volume.

Spanned Volumes A spanned volume consists of disk space on two or more dynamic drives; up to 32 dynamic drives can be used in a spanned volume configuration. Spanned volume sets are used to dynamically increase the size of a dynamic volume. When you create spanned volumes, the

data is written sequentially, filling space on one physical drive before writing to space on the next physical drive in the spanned volume set. Typically, administrators use spanned volumes when they are running out of disk space on a volume and want to dynamically extend the volume with space from another hard drive. You do not need to allocate the same amount of space to the volume set on each physical drive.

Because data is written sequentially, you do not see any performance enhancements with spanned volumes as you do with striped volumes (discussed next). The main disadvantage of spanned volumes is that if any drive in the spanned volume set fails, you lose access to all of the data in the spanned set.

Striped Volumes A striped volume stores data in equal stripes between two or more (up to 32) dynamic drives. Since the data is written sequentially in the stripes, you can take advantage of multiple I/O performance and increase the speed at which data reads and writes take place. Typically, administrators use striped volumes when they want to combine the space of several physical drives into a single logical volume and increase disk performance.

The main disadvantage of striped volumes is that if any drive in the striped volume set fails, you lose access to all of the data in the striped set.

Using the Disk Management Utility

The Disk Management utility is a graphical tool for managing disks and volumes within the Windows XP environment. In this section, you will learn how to access the Disk Management utility and use it to manage basic tasks, basic storage, and dynamic storage. You will also learn about troubleshooting disks through disk status codes.

To have full permissions to use the Disk Management utility, you must be logged on with Administrative privileges. To access the utility, right-click My Computer from the Start menu and select Manage, then in Computer Management, select Disk Management. You could also use Control Panel ➢ Performance and Maintenance ➢ Administrative Tools ➢ Computer Management. Expand the Storage folder to see the Disk Management utility. The Disk Management utility's opening window, shown in Figure 3.1, shows the following information:

- The volumes that are recognized by the computer
- The type of disk, either basic or dynamic
- The type of file system used by each partition
- The status of the partition and whether the partition contains the system or boot partition
- The capacity (amount of space) allocated to the partition
- The amount of free space remaining on the partition
- The amount of overhead associated with the partition

Windows XP Professional includes a new command-line utility called `Diskpart`, which can be used as a command-line alternative to the Disk Management utility. You can view all of the options associated with the `Diskpart` utility by typing `Diskpart /?` from a command prompt.

FIGURE 3.1 The Disk Management window

With the Disk Management utility, you can perform a variety of basic tasks including the following:

- View disk properties
- View volume and local disk properties
- Add a new disk
- Create partitions and volumes
- Upgrade a basic disk to a dynamic disk
- Change a drive letter and path
- Delete partitions and volumes

Adding a New Disk

To increase the amount of disk storage you have, you can add a new disk. This is a fairly common task that you will need to perform as your application programs and files grow larger. How you add a disk depends on whether your computer supports hot swapping of drives. Hot swapping is the process of adding a new hard drive while the computer is turned on. Most computers do not support this capability.

The following list specifies configuration options:

Computer doesn't support hot swapping If your computer does not support hot swapping, you must first shut down the computer before you add a new disk. Then add the drive according to the manufacturer's directions. When you're finished, restart the computer. You should find the new drive listed in the Disk Management utility.

Computer supports hot swapping If your computer does support hot swapping, you don't need to turn off your computer first. Just add the drive according to the manufacturer's directions. Then open the Disk Management utility and select Action ➢ Rescan Disks. You should find the new drive listed in the Disk Management utility.

You must be a member of the Administrators group in order to install a new drive.

Upgrading a Basic Disk to a Dynamic Disk

To take advantage of the features offered by Windows XP dynamic disks, you must upgrade your basic disks to dynamic disks.

When you install Windows XP Professional or upgrade your computer from Windows NT 4 to Windows XP Professional, your drives are configured as basic disks. Windows XP will not read a disk that has been configured with disk spanning or disk striping under Windows NT 4.0. In this case, you will need to upgrade your computer to Windows 2000 Professional first and then convert your disk from basic to dynamic. When you upgrade to Windows XP Professional, it will recognize the disk as dynamic, your spanned or striped disk will be recognized, and your data will be preserved.

Upgrading basic disks to dynamic disks is a one-way process as far as preserving data is concerned, and it is a potentially dangerous operation. If you decide to revert to a basic disk, you will have to first delete all volumes associated with the drive; then, in the Disk Management utility, you can select Convert to Basic Disk. Before you do this upgrade (or make any major change to your drives or volumes), create a new backup of the drive or volume and verify that you can successfully restore the backup.

Deleting Partitions and Volumes

You might delete a partition or volume if you want to reorganize your disk or make sure that data will not be accessed.

Once you delete a partition or volume, it is gone forever.

Troubleshooting Disks and Volumes

The Disk Management utility can be used to troubleshoot disk errors through a set of status codes; however, if a disk will not initialize, no status code will be displayed. Disks will not initialize if there is not a valid disk signature.

Using Disk Management Status Codes

The main window of the Disk Management utility displays the status of disks and volumes. The following list contains the possible status codes and a description of each code; these are very useful in troubleshooting disk problems.

Online Indicates that the disk is accessible and that it is functioning properly. This is the normal disk status.

Online (Errors) Only used with dynamic disks. Indicates that I/O errors have been detected on the dynamic disk. One possible fix for this error is to right-click the disk and select Reactivate Disk to attempt to return the disk to Online status. This fix will work only if the I/O errors were temporary. You should immediately back up your data if you see this error and suspect that the I/O errors are not temporary.

Healthy Specifies that the volume is accessible and functioning properly.

Healthy (At Risk) Used to indicate that a dynamic volume is currently accessible, but I/O errors have been detected on the underlying dynamic disk. This option is usually associated with Online (Errors) for the underlying disk.

Offline or Missing Only used with dynamic disks. Indicates that the disk is not accessible. This can occur if the disk is corrupt or the hardware has failed. If the error is not caused by hardware failure or major corruption, you may be able to re-access the disk by using the Reactivate Disk option to return the disk to Online status. If the disk was originally offline and then the status changed to Missing, it indicates that the disk has become corrupt, been powered down, or was disconnected.

Unreadable This can occur on basic or dynamic disks. Indicates that the disk is inaccessible and might have encountered hardware errors, corruption, or I/O errors, or that the system disk configuration database is corrupt. This message may also appear when a disk is spinning up while the Disk Management utility is rescanning the disks on the computer.

Failed Can be seen with basic or dynamic volumes. Specifies that the volume can't be started. This can occur because the disk is damaged or the file system is corrupt. If this message occurs with a basic volume, you should check the underlying disk hardware. If the error occurs on a dynamic volume, verify that the underlying disks are online.

Unknown Used with basic and dynamic volumes. Occurs if the boot sector for the volume becomes corrupt—for example, from a virus. This error can also occur if no disk signature is created for the volume.

Incomplete Occurs when you move some, but not all, of the disks from a multidisk volume. If you do not complete the multivolume set, then the data will be inaccessible.

Foreign Can occur if you move a dynamic disk from one computer to another computer running Windows 2000 (any version) or Windows XP Professional. This error is caused because configuration data is unique to computers where the dynamic disk was created. You can correct this error by right-clicking the disk and selecting the option Import Foreign Disks. Any existing volume information will then be visible and accessible.

Troubleshooting Disks That Fail to Initialize

When you add a new disk to your computer in Windows XP Professional, the disk does not initially contain a disk signature, which is required for the disk to be recognized by Windows XP Professional. Disk signatures are at the end of the sector marker on the Master Boot Record (MBR) of the drive. When you install a new drive and run the Disk Management utility, a wizard starts and lists all new disks that have been detected. The disk signature is written through this process. If you cancel the wizard before the disk signature is written, you will see the disk status Not Initialized.

To initialize a disk, you right-click the disk you want to initialize and select the Initialize Disk option. If you are running a 32-bit edition of Windows XP Professional, you will write the disk signature to the MBR of the drive. If you are using Windows XP 64-bit edition, you can write the signature to the MBR or the GUID Partition Table (GPT).

Monitoring and Configuring Removable Media

Removable media are devices such as tape devices and Zip drives. Like DVD and CD-ROM devices, removable media can also be managed through Device Manager.

Removable media are listed under Disk Drives in Device Manager. Double-click Disk Drives, and then double-click the removable media device you wish to manage. This brings up the device Properties dialog box. The General and Driver tabs are similar to those for CD-ROM and DVD devices, as described earlier. The Disk Properties tab contains options for the specific removable media device.

In order to access removable media, the user needs to be a member of the Backup Operators group.

Exam Essentials

Be able to manage hard disks. Be able to install and configure hard disks. Know how to create and manage volumes. Be able to troubleshoot disk and volume problems. Know how to use the Disk Management utility.

Know how to manage basic and dynamic disks. Be able to list the features that are only available with dynamic disks. Know how to convert a basic disk to a dynamic disk.

Know how to manage removable media. Know what options can be used for removable media and how removable media is managed.

Implement, Manage, and Troubleshoot Display Devices

A video adapter is the device that outputs the display to your monitor. You install a video adapter in the same way that you install other hardware. If it is a Plug and Play device, all you need to do is shut down your computer, add the video adapter, and turn on your computer. Windows XP Professional will automatically recognize the new device.

You can configure several options for your video adapters, and if you have multiple monitors with their own video adapters, you can configure multiple-display support. The following sections describe video adapter configuration and how to configure your computer to support multiple monitors.

Critical Information

The options for video adapters are on the Settings tab of the Display Properties dialog box, as shown in Figure 3.2. To access this dialog box, select Control Panel ➢ Appearance and Themes ➢ Display, then select the Settings tab. Alternately, you could right-click an empty area on your desktop and select Properties from the pop-up menu, then select the Setting tab.

The Color Quality option in the Settings tab sets the color quality (for example, to 32-bit quality or 16-bit quality), for your video adapter. The Screen Resolution option allows you to set the resolution for your video adapter.

To configure advanced settings for your video adapter, click the Advanced button in the lower-right corner of the Settings tab. This brings up the Properties dialog box for the monitor, as shown in Figure 3.3. There are five tabs (described momentarily) with options for your video adapter and monitor.

General Allows you to configure the font size for the display. You can also specify what action Windows XP will take after you change your display settings.

Adapter Allows you to view and configure the properties of your video adapter.

FIGURE 3.2 The Settings tab of the Display Properties dialog box

FIGURE 3.3 The Properties dialog box for a display monitor

Monitor Allows you to view and configure the properties of your monitor, including the refresh frequency (how often the screen is redrawn).

Troubleshoot Allows you to configure how Windows XP uses your graphics hardware. For example, you can configure hardware acceleration settings.

Color Management Allows you to select color profiles (the colors that are displayed on your monitor).

A lower refresh frequency setting can cause your screen to flicker. Setting the refresh frequency too high can damage some hardware.

Configuring Multiple-Display Support

Windows XP Professional allows you to extend your Desktop across a maximum of 10 monitors. This means you can spread your applications across multiple monitors.

To set up multiple-display support, you must have a video adapter installed for each monitor, and you must use either Peripheral Connection Interface (PCI) or Accelerated Graphics Port (AGP) video adapter cards. To use the video adapter that is built into the system board for multiple-display support, the chip set must use the PCI or AGP standard.

If your computer has the video adapter built into the system board, you should install Windows XP Professional before you install the second video adapter. This is because Windows XP will disable the video adapter that is built into the system board if it detects a second video adapter. When you add a second video adapter after Windows XP is installed, it will automatically become the primary video adapter.

The following steps are used to configure multiple-display support:

1. Turn off your computer and install the PCI or AGP adapters. Plug your monitors into the video adapters and turn on your computer. Assuming that the adapters are Plug and Play, Windows XP will automatically recognize your new adapters and load the correct drivers.
2. Open the Display Properties dialog box (right-click an empty area on your desktop and select Properties) and click the Settings tab. You should see an icon for each of the monitors.
3. Click the number of the monitor that will act as your additional display. Then select the Extend My Windows Desktop onto This Monitor check box. Repeat this step for each additional monitor you wish to configure. You can arrange the order in which the displays are arranged by dragging and dropping the monitor icons in the Settings tab of the Display Properties dialog box.
4. When you are finished configuring the monitors, click OK to close the dialog box.

Troubleshooting Multiple-Display Support

If you are having problems with multiple-display support, use the following troubleshooting guidelines:

The Extend My Windows Desktop onto This Monitor option isn't available. If the Settings tab of the Display Properties dialog box doesn't give you the option Extend My Windows Desktop onto This Monitor, confirm that your secondary adapter is supported for multiple-display support. Confirm that you have the most current drivers (that are XP compliant and support dual-mode capabilities) loaded. Confirm that Windows XP is able to detect the secondary video adapter. Try selecting the secondary adapter rather than the primary adapter in the Display Properties dialog box.

No output appears on the secondary display. Confirm that your secondary adapter is supported for multiple-display support, especially if you are using the built-in motherboard video adapter. Confirm that the correct video driver has been installed for the secondary display. Restart the computer to see if the secondary video driver is initialized. Check the status of the video adapter in Device Manager. Try switching the order of the video adapters in the computer's slots. See if the system will recognize the device as the primary display.

An application is not properly displayed. Disable the secondary display to determine if the problem is specific to multiple-display support. Run the application on the primary display. If you are running MS-DOS applications, try running the application in full-screen mode. For Windows applications, try running the application in a maximized window.

Exam Essentials

Be able to install and configure a video adapter. Know what options can be configured for a video adapter and how to troubleshoot a video adapter if needed.

Be able to support multiple monitors. Know how to configure multiple display support and how to troubleshoot it if you have problems.

Configure Advanced Configuration Power Interface (ACPI)

Windows XP Professional includes several features that are particularly useful for laptop computers. For example, through Power Options in Control Panel (found in the Performance and Maintenance section), you can set power schemes and enable power management features with Windows XP. You will also learn how to manage card services for mobile computers.

Critical Information

In this section you will learn how to manage power states, how to manage power options, and how to troubleshoot power management.

Managing Power States

In Windows XP, the *Advanced Configuration Power Interface (ACPI)* specifies six different levels of power states:

- Complete shutdown of PC
- Hibernation
- Standby (three levels)
- Fully active PC

The similarity between *hibernation* and *standby* is that they both allow you to avoid shutting down your computer to save power. The key difference is in your computer's state of shutdown.

Hibernation falls short of a complete shutdown of the computer. With hibernation, the computer saves all of your desktop states as well as any open files. To use the computer again, press the power button. The computer starts more quickly than from a complete shutdown because it does not have to go through the complete startup process. You will have to again log on to the computer. You will also notice that all the documents that were open when the computer went into hibernation are still available. With hibernation, you can easily resume work where you left off. You can configure your computer to hibernate through Power Options, or by entering Start ➢ Shut Down and then selecting Hibernate from the drop-down menu. This option will appear only if hibernation has been enabled through Power Options.

Standby does not save data automatically as hibernation does. With standby you can access your computer more quickly than a computer that is in hibernation, usually through a mouse click or keystroke, and the desktop appears as it was prior to the standby. The response time depends on the level of your computer's standby state. On an ACPI-compliant computer, there are three levels of standby, each level putting the computer into a deeper sleep. The first level turns off power to the monitor and hard drives. The second level turns off power to the CPU and cache. The third level supplies power to RAM only and preserves

the desktop in memory. You will see an option to configure standby only on Windows XP computers in which a battery has been detected. You can configure your computer for standby through Power Options, or through Start ➢ Shut Down and then selecting Standby from the drop-down menu. This option will appear only if standby has been enabled through Power Options.

Put your computer in standby mode if you will be away for a few minutes. Use hibernation mode if you will be away for a more extended period of time.

To determine whether Windows XP is running in ACPI mode

1. Click Start ➢ Control Panel ➢ Performance and Maintenance.
2. Double-click Administrative Tools, and click Computer Management.
3. Click Device Manager, then click System Devices.

If Microsoft ACPI-Compliant System is listed under System Devices, then the computer is operating in ACPI mode. During Windows XP Setup, ACPI is installed only on systems that have an ACPI-compatible BIOS.

You may be able to upgrade your computer's BIOS to make it ACPI compatible. Check with your computer's manufacturer for upgrade information.

Using ACPI Settings

You configure power options through the Power Options Properties dialog box, as shown in Figure 3.4. To access this dialog box, access Control Panel ➢ Performance and Maintenance ➢ Power Options. On a laptop, this dialog box has five tabs: Power Schemes, Alarms, Power Meter, Advanced, and Hibernate. If your computer is a stand-alone PC, you will see a tab for UPS, Uninterruptible Power Supply, which is used to provide an alternate power source in the event that your computer loses regular power. The Power Options for laptop computers are described in the following sections.

Configuring Power Schemes

The Power Schemes tab helps you select the most appropriate power scheme for your computer. Power schemes control automatic turn-off of the monitor and hard disks, based on a specified period of inactivity. This feature allows you to conserve your laptop's battery when the computer isn't being used. From the drop-down list, you can select one of the preconfigured power schemes listed in Table 3.1. Alternatively, you can create a custom power scheme by clicking the Save As button, giving the power scheme a new name, and choosing power scheme options.

TABLE 3.1 Windows XP Power Schemes

Power Scheme	Turn Off Monitor	Turn Off Hard Disks
Home/Office Desk	After 20 minutes	Never
Portable/Laptop	After 15 minutes	After 30 minutes
Presentation	Never	Never
Always On	After 20 minutes	Never
Minimal Power Management	After 15 minutes	Never
Max Battery	After 15 minutes	Never

Configuring Alarms

The Alarms tab of Power Options Properties (shown in Figure 3.5) is used to specify Low Battery Alarm and Critical Battery Alarm. With Low Battery Alarm and Critical Battery Alarm, you can specify that notification, action (such as hibernation), or run program events be triggered when the power level reaches a specified threshold.

FIGURE 3.4 The Power Options Properties dialog box

FIGURE 3.5 Alarms tab of Power Options Properties

This tab is only present on a laptop computer with a battery installed.

Configuring Power Meter Options

The Power Meter tab is used to show you what your current power source is, either AC power or battery. You can also see what percentage the battery is charged to.

Configuring Advanced Options

Among the advanced options, you can configure several power options, including

- Whether the Power Management icon will be displayed on the Taskbar.
- Whether the user will be prompted for a Windows XP password when the computer resumes from standby.

If Windows XP Professional is installed on a laptop computer, you will also see options for managing power buttons in the following instances:

- When I Close the Lid of My Portable Computer
- When I Press the Power Button on My Computer

In these instances, you can specify that you want the computer to go on standby or power-off mode. With the When I Close the Lid of My Portable Computer, you also have the additional option of doing nothing.

Configuring Hibernation

Hibernation for a computer means that anything stored in memory is also stored on your hard disk. This ensures that when your computer is shut down, you do not lose any of the information that is stored in memory. When you take your computer out of hibernation, it returns to its previous state.

To configure your computer to hibernate, use the Hibernate tab of the Power Options Properties dialog box, as shown in Figure 3.6. Simply select the Enable Hibernation check box.

If you are using ACPI on your Windows XP computer and your BIOS does not support ACPI, you may experience problems such as the computer's inability to shut down. In this case, you should upgrade your computer with a BIOS that supports ACPI, or you can disable ACPI support on the computer.

Exam Essentials

Know how to manage power options on a laptop. Be able to configure power states, enable ACPI, and configure hibernation. Know how to troubleshoot power options.

FIGURE 3.6 The Hibernate tab of Power Options Properties

Implement, Manage, and Troubleshoot Input and Output (I/O) Devices

Your input/output (I/O) devices are the ones that allow you to get information into and out of your computer. Examples of I/O devices are keyboards, mice, printers, and scanners. Your

devices may be connected to your computer by standard cabling, or they may use wireless technology (such as Infrared Data Association [IrDA] or Radio Frequency [RF]) or be connected through a Universal Serial Bus (USB) port.

Critical Information

The following subsections describe how to manage your printer, keyboard, mouse, wireless devices, imaging devices, and USB devices.

Installing a Printer

Before you can access your physical print device under Windows XP Professional, you must first create a *logical printer*. Windows XP Professional will automatically try and install the printer for you if it is a Plug and Play printer and there is a driver available, If the printer does not automatically install itself, you can create one through the Add Printer Wizard in Control Panel ➢ Printers and Faxes. To create a new printer in Windows XP Professional, you must be logged on as a member of the Administrators or Power Users group.

The computer on which you run the Add Printer Wizard and create the printer automatically becomes the print server for that printer. As the print server, the computer must have enough processing power to support incoming print jobs and enough disk space to hold all of the print jobs that will be queued.

Managing printers is covered in greater detail in Chapter 2, "Implementing and Conducting Administration of Resources."

Configuring the Keyboard

Most of the time you leave the keyboard settings at default values. However, if needed, you can configure advanced keyboard options.

You can configure keyboard options through the Keyboard Properties dialog box, shown in Figure 3.7. To access this dialog box, open Control Panel, then choose Printers and Other Hardware, and then select the Keyboard icon.

You must have a keyboard attached to your computer before you can install Windows XP Professional.

This dialog box has two tabs with options that control your keyboard's behavior:

- The Speed tab lets you configure how quickly characters are repeated when you hold down a key. You can also specify the cursor blink rate.
- The Hardware tab specifies the device settings for your keyboard.

FIGURE 3.7 The Keyboard Properties dialog box

Configuring the Mouse

You can configure your mouse through the Mouse Properties dialog box, shown in Figure 3.8. To access this dialog box, open Control Panel, then Printers and Other Hardware, and then select the Mouse option.

FIGURE 3.8 The Mouse Properties dialog box

The Mouse Properties dialog box has five tabs with options that control your mouse's behavior:

Buttons Allows you to configure the mouse properties for right-handed or left-handed use. You can also configure the speed that is used to indicate a double-click. The ClickLock option is used to highlight and drag a selection without holding down the mouse button while the object is being moved. ClickLock is not enabled by default.

Pointers Lets you select a predefined pointer scheme that is used by your mouse, for example, Dinosaur (system scheme) that uses dinosaur themed pointers. You can also create custom pointer schemes.

Pointer Options Lets you specify how fast your mouse pointer moves. You can also configure the snap-to-default feature, which automatically moves the pointer to a default button in a dialog box when new dialog boxes are opened. Visibility options are used to configure if pointer trails are displayed, if the pointer is hidden while typing, and whether the location of the pointer is shown when the CTRL key is pressed.

Wheel Is used to configure wheel scrolling.

Hardware Specifies the device settings for your mouse.

Managing Imaging Devices (Multimedia and Scanners)

A scanner is a device that can read text or graphics that are on paper and translate the information to digital data that the computer can understand. Digital cameras take pictures in a digital format that can be read by the computer.

After you install a scanner or digital camera on a Windows XP Professional computer, you can manage the device through the Scanners and Cameras Properties dialog box. You access this dialog box by selecting the Scanners and Cameras icon in Control Panel from the Printers and Other Hardware option.

The Scanners and Cameras Properties dialog box lists the devices that are recognized by your computer. You can click the Add an Imaging Device option to add a scanner or camera, the Remove button to remove the selected device, or the Troubleshoot button to run a Troubleshooter Wizard. Clicking the Properties button displays a dialog box with additional options.

The scanner or camera Properties dialog box has three tabs with options and information about the device:

General Lists the manufacturer, description, port, and status of the device. It also contains a button that you can click to test the scanner or camera.

Events Allows you to associate an event with an application. For example, you can specify that when you scan a document, it should be automatically linked to the imaging program, and the imaging program will start and display the document you just scanned.

Color Management Allows you to associate a color profile with the scanner or camera.

Installing, Configuring, and Managing Modems

Dial-up networking allows remote users (for example, a person working from home or someone with a laptop on a business trip) to dial into a corporate network or the Internet. The most common

method for remote network access is using a modem. This section will cover how to install and configure modems for use with Windows XP Professional.

If you install a Plug and Play modem on your Windows XP computer, it should be recognized automatically, and an appropriate driver should be loaded. Some modems are not automatically recognized with Windows XP Professional. In this case, you would manually install the modem through the Add/Remove Hardware Wizard and supply the device driver for Windows XP Professional that was provided through the modem manufacturer.

You can configure and manage the modems installed on your computer through Device Manager. To access Device Manager, select Start, then right-click My Computer and select Manage from the pop-up menu. Select System Tools, then Device Manager. In the Device Manager window, select Modems and then double-click the modem you want to manage. This brings up the modem's Properties dialog box, as shown in Figure 3.9. Most modems' Properties dialog boxes have six tabs: General, Modem, Diagnostics, Advanced, Driver, and Resources (if you are using a laptop, you will also see Power Management). The options on these tabs are covered in the following sections.

Avoid changing the default modem properties unless advised to by your modem manufacturer or the entity you are connecting to (for example, your Internet service provider). If you make incorrect alterations to the modem configuration, your modem may not work.

FIGURE 3.9 The modem Properties dialog box

Configuring General Modem Properties

The General tab of the modem Properties dialog box (see Figure 3.9) displays the device type, the manufacturer of the modem, and location (slot within the PC where the modem is installed).

The General tab also displays the current status of the modem. Typically the status should be The Device Is Working Properly. If the modem is not working properly, you can click the Troubleshoot button to start a Troubleshooting Wizard that will help you determine the cause of the problem.

Configuring Modem Properties

The Modem tab shows the port to which the modem is attached. From this tab, you can set the following options:

- The speaker volume for the modem, which would typically be turned down if everything was working properly, but might be turned up if you were trying to troubleshoot a modem that was not working properly.
- The maximum port speed (specified in bits per second), which should be left at the default value.
- Dial control, to wait for a dial tone before dialing, so that dialing is not initiated prior to confirming that a valid dial tone exists.

Running Modem Diagnostics

Through the Diagnostics tab, you can query the modem. This process can be used in troubleshooting to ensure that the modem is properly responding to requests. Click the Query Modem button, and Device Manager will test the modem by issuing a series of modem commands. These commands and the responses sent back from the modem are listed in the Command/Response dialog box.

The View Log button is used to view the log file that records a log of all of the commands sent to the modem by communication programs or the operating system. By default, this log is overwritten each time you run a new query. The Append to Log option can be specified if you don't want the log file to be overwritten. The log file is stored as `\systemroot\yourmodemmodel.txt`.

Configuring Advanced Modem Properties

The Advanced tab allows you to specify additional initialization commands, which might be required for troubleshooting modem problems, and the default Country/Region you are in, which sets configuration options based on regional phone systems. You can also configure advanced port settings and change default preferences by clicking their associated buttons, as explained in the following sections.

Viewing Driver Details and Updating Drivers

The Driver tab of the modem Properties dialog box displays information about the modem driver that is currently loaded. In the top half of the dialog box you can see

- Driver Provider (which will be Microsoft if the driver was installed from the Windows XP Professional CD)
- Driver Date
- Driver Version
- Driver Signer

Viewing Modem Resources

The Resources tab lists the resources that are used by your modem. Resources include memory, I/O memory, and interrupt request (IRQ) settings. You can use this information to detect resource conflicts, which may arise if you have non–Plug and Play hardware installed on your computer. The bottom of the dialog box will list any conflicts that have been detected with other devices that are installed on the computer.

Troubleshooting Remote Access Connections

If your remote access connection is not working properly, there are many possible causes. The following list categorizes common problems and the options that can be used to troubleshoot, identify, and resolve configuration errors:

If you suspect the problem is with your modem

- Verify that the modem you are using is on the Hardware Compatibility List (HCL) and that you have the most current driver.
- If you are using an external modem, verify that it is turned on and connected to the proper port, and that the modem cable is not defective. If you require a 9-to-25-pin serial connector, do not use one that came with a mouse, as most are not manufactured to support modem signals.
- Use modem logging and modem diagnostics to test the modem.

If you suspect the problem is with your access line

- If you are using an unknown line type (for example, in a hotel), verify the line type you are using. Analog modems only use analog phone lines, and digital modems only use digital lines. The remote client and the server that is being accessed must also use a common access method, analog or digital.
- Verify that you dialed the correct number for the remote server. If you need to dial an external line-access number (usually 9), verify that it is properly configured.
- If the modem is having problems connecting, there may be excessive static on the phone line that is preventing the modem from connecting at the configured speed. Attempt to connect using lower speed and call the phone company to have the quality of the line checked.

Installing, Configuring, and Managing Infrared Data Association (IrDA) Devices and Wireless Devices

Wireless devices use wireless transmission rather than transmitting over cable. Following are two of the technologies used for wireless transmission:

- Infrared Data Association (IrDA), which is a standard for transmitting data through infrared light waves
- Radio Frequency (RF), which is a standard for transmitting data through radio waves

Common examples of wireless devices include keyboards, mice, and network cards. You should follow the vendor's instructions to install wireless devices. Wireless devices are configured in the same manner as other devices on your computer. For example, you can set options for a wireless keyboard through the Keyboard Properties dialog box.

The following steps are used to establish an infrared connection:

1. Ensure that the infrared device that you want to use is properly configured.
2. Align the wireless device so that the infrared transceiver on the device is within a meter of the receiver.

You can verify that your computer supports IrDA functionality through Control Panel, Printers and Other Hardware. Click System on the left side, then from the Hardware tab, click Device Manager. If you have an infrared transceiver on your computer, you will see Infrared Devices listed. If your computer has infrared capabilities and it is not listed in Device Manager, you should check your computer BIOS to ensure that the IrDA support is enabled.

Installing, Configuring, and Managing USB Devices

USB is an external bus standard that allows you to connect USB devices through a USB port. USB supports transfer rates up to 12Mbps. A single USB port can support up to 127 devices. Examples of USB devices include modems, printers, and keyboards.

Configuring USB Devices

If your computer supports USB, and USB is enabled in the BIOS, you will see Universal Serial Bus Controller listed in Device Manager. Double-click your USB controller to see the dialog box shown in Figure 3.10.

FIGURE 3.10 The USB controller Properties dialog box

The USB controller Properties dialog box has four tabs with options and information for your USB adapter:

General Lists the device type, manufacturer, and location. It also shows the device status, which indicates whether the device is working properly. If the device is not working properly, you can click the Troubleshoot button in the lower-right area of the dialog box.

Advanced Allows you to configure how much of the bandwidth each device that is connected to the USB adapter can use.

Driver Shows driver properties and lets you uninstall or update the driver.

Resources Shows all of the resources that are used by the USB adapter.

After the USB adapter is configured, you can attach USB devices to the adapter in a daisy-chain configuration.

Troubleshooting USB

Some of the errors you may encounter with USB and the associated fixes are as follows:

- You may have malfunctioning or incorrectly configured USB hardware. If you suspect that this is the case, and you have another computer running USB, you should try and run the USB hardware on the alternate computer. You should also check the status of the device in Device Manager. To support USB, the computer must have an IRQ assigned for the root USB controller in the computer's BIOS.
- You may have mismatched cabling. USB supports two standards, high-speed and low-speed. Make sure the cables are the proper type for your configuration.
- Make sure your BIOS and firmware is up-to-date. If the BIOS or firmware is not compatible with USB, you may see multiple instances of your device in Device Manager with no associated drivers for the multiple instances.
- The root hub may be improperly configured. USB controllers require that an IRQ be assigned in the computer's BIOS. If the controller is not properly configured, you will see the root hub displayed in Device Manager with a yellow exclamation point.
- If you are using a USB bus-powered hub, the device attached to the hub may require more power than the hub can provide. In this case, you should use a self-powered USB hub. You can determine if the hub is the problem by removing the hub and directly attaching the device to the computer's USB. You can also troubleshoot this error by attaching the device to a self-powered USB hub and seeing if it works.

If your computer has a built-in USB device and does not detect the device through Device Manager, confirm that the USB is enabled in the computer's BIOS and that the BIOS supports USB devices.

Installing, Configuring, and Managing Network Adapters

Network adapters are hardware used to connect computers (or other devices) to the network. Network adapters are responsible for providing the physical connection to the network and the physical address of the computer. These adapters (and all other hardware devices) need a driver to communicate with the Windows XP operating system.

In the following sections, you will learn how to install and configure network adapters, as well as how to configure authentication, including advanced settings, and how to manage network bindings for your adapters. Finally, you will learn how to troubleshoot network adapters that are not working.

Installing a Network Adapter

Before you physically install your network adapter, it's important to read the instructions that come with the hardware. If your network adapter is new, it should be self-configuring, with Plug and Play capabilities. After you install a network adapter that supports Plug and Play, it should work the next time you start up the computer.

New devices will auto-detect settings and be self-configuring. Older devices rely on hardware setup programs to configure hardware. Really old devices require you to manually configure the adapter through switches or jumpers.

When you install a network adapter that is not Plug and Play, the operating system should detect that you have a new piece of hardware and start a wizard that leads you through the process of loading the adapter's driver.

Configuring a Network Adapter

Once the network adapter has been installed, you can configure it through its Properties dialog box. To access this dialog box, select Start ➢ Control Panel ➢ Network and Internet Connections. From the Network and Internet Connections dialog box, click the Network Connections option. You will see your Local Area Connection as an icon. To view the properties of the network adapter, right-click Local Area Connection and select Properties. From within the General tab (shown in Figure 3.11), you will see your network adapter; click the Configure button to access the network adapter Properties dialog box, shown in Figure 3.12.

In the network adapter Properties dialog box, the properties are grouped on four tabs: General, Advanced, Driver, and Resources. These properties are explained in the following sections.

If you are using a laptop computer with ACPI features, you will also see a tab for Power Management.

GENERAL NETWORK ADAPTER PROPERTIES

The General tab of the network adapter Properties dialog box shows the name of the adapter, the device type, the manufacturer, and the location. The Device Status box reports whether the device is working properly. If the device is not working properly, you can click the Troubleshoot

button to have Windows XP display some general troubleshooting tips. You can also enable or disable the device through the Device Usage drop-down list options.

FIGURE 3.11 Local Area Connection Properties dialog box

FIGURE 3.12 The network adapter Properties dialog box

ADVANCED NETWORK ADAPTER PROPERTIES

The contents of the Advanced tab of the network adapter Properties dialog box vary depending on the network adapter and driver that you are using.

You should not need to change the settings on the Advanced tab of the network adapter Properties dialog box unless you have been instructed to do so by the manufacturer.

DRIVER PROPERTIES

The Driver tab of the network adapter Properties dialog box provides the following information about your driver:

- The driver provider, which is usually Microsoft or the network adapter manufacturer.
- The date that the driver was released.
- The driver version, which is useful in determining whether you have the latest driver installed.
- The digital signer, which is the company that provides the digital signature for driver signing.

RESOURCE PROPERTIES

Each device installed on a computer uses computer resources. Resources include IRQ, memory, and I/O resources. The Resources tab of the network adapter Properties dialog box lists the resource settings for your network adapter. This information is important for troubleshooting, because if other devices are trying to use the same resource settings, your devices will not work properly. The Conflicting Device List box at the bottom of the Resources tab shows whether any conflicts exist.

Exam Essentials

Know how to install and configure I/O devices. Be able to configure and manage keyboards, mice, printers, and scanners.

Be able to install and manage wireless devices. Be able to install, configure, and troubleshoot wireless devices.

Understand how USB works and how to manage it. Be able to install, configure, and troubleshoot USB devices.

Manage and Troubleshoot Drivers and Driver Signing

A *device driver* is software that allows a specific piece of hardware to communicate with the Windows XP operating system. Most of the devices on the Microsoft HCL have drivers that are

included on the Windows XP Professional distribution CD. Managing device drivers involves updating them when necessary and deciding how to handle drivers that may not have been properly tested.

Critical Information

In the following sections you will learn how to update drivers, troubleshoot drivers, use driver signing, and troubleshoot drivers.

Updating Drivers

Device manufacturers periodically update device drivers to add functionality or enhance driver performance. The updated drivers are typically posted on the manufacturer's website.

The following steps are used to update a driver:

1. Select Start, then right-click My Computer and select Manage from the pop-up menu.
2. The Computer Management window opens. Select System Tools, then Device Manager.
3. The right side of the window lists all the devices that are installed on your computer. Right-click the device whose driver you want to update.
4. Select Update Driver from the pop-up menu. The Hardware Update Wizard will start. Click the Next button.
5. In the Welcome to the Hardware Update Wizard dialog box, you can choose to have the wizard search for a suitable driver and install the software automatically, which is recommended, or you can have the wizard install the driver from a list or specific location. This exercise assumes you will be installing your new driver from an installation CD or floppy disk that came with the device and that you are using. In this case, select the Install from a list or specific location (Advanced) option. Make sure the installation CD or floppy is inserted, and click the Next button.
6. The files will be installed for your driver. Then you will see the Completing the Upgrade Device Driver Wizard dialog box. Click the Finish button to close this dialog box.
7. You may see a dialog box indicating that you must restart your computer before the change can be successfully implemented. If necessary, restart your computer.

Troubleshooting Drivers

If you have a device that is installed that is not working properly and you do not have the correct driver for the device or the device is not working properly, you can uninstall or disable the device through the following steps:

1. Select Start, then right-click My Computer and select Manage from the pop-up menu.
2. The Computer Management window opens. Select System Tools, then Device Manager.
3. Right-click the device you want to manage. A pop-up menu will appear, as shown in Figure 3.13 that will allow you to disable or uninstall the device depending on the option you select.

FIGURE 3.13 Options for managing a device

If you updated a driver that was working properly, but with the updated driver is not working properly, you should roll back the driver. When you roll back the driver, you uninstall the new driver and revert back to the previous driver.

The following steps are used for driver roll back:

1. Select Start, then right-click My Computer and select Manage from the pop-up menu.
2. The Computer Management window opens. Select System Tools, then Device Manager.
3. Double-click the device whose driver you want to roll back and select Update Driver.
4. Select the Driver tab (shown in Figure 3.14) and click the Roll Back Driver button. You will be asked to confirm that you want to roll back the driver.

FIGURE 3.14 The Driver tab of a devices Properties dialog box

Managing Driver Signing

In the past, poorly written device drivers have caused problems in Windows operating systems. Microsoft is now promoting a mechanism called *driver signing* as a way of ensuring that drivers are properly tested before they are released to the public.

Through the Driver Signing Options dialog box, you can specify how Windows XP Professional will respond if you choose to install an unsigned driver. To access this dialog box, from the Start menu, right-click My Computer, select Properties from the pop-up menu, and click the Hardware tab in the System Properties dialog box. This tab has Add Hardware Wizard, Device Manager, and Hardware Profiles options, as shown in Figure 3.15. Clicking the Driver Signing button in the Device Manager section opens the Driver Signing Options dialog box, as shown in Figure 3.16.

FIGURE 3.15 The Hardware tab of the System Properties dialog box

FIGURE 3.16 Driver signing options

In the Driver Signing Options dialog box, you can select from three options for file system verification:

- The Ignore option has Windows XP install all of the files, whether or not they are signed. You will not see any type of message about driver signing.
- The Warn option has Windows XP display a warning message before installing an unsigned file. You can then choose to continue with the installation or cancel it. This is the default setting.
- The Block option has Windows XP prevent the installation of any unsigned file. You will see an error message when you attempt to install the unsigned driver, and you will not be able to continue.

By default, when you apply driver settings, they are only applied to the user who is currently logged on. If you check the Make This Action the System Default option, the settings that you apply will be used by all users who log on to the computer.

You can run a utility called SigVerif from a command line. This utility will check all of your files for current verification status, and then display a list of all drivers that have not been digitally signed. The log file created (`sigverif.txt`) is accessed by clicking the Advanced button within the SigVerif dialog box.

Troubleshooting Driver Signing

If you suspect that you have a driver that is not properly signed or is not working properly, you should access the correct driver. You can get the latest driver from Microsoft through Windows Update. The advantage of using Windows Update is that the drivers have been thoroughly tested and are verified by Microsoft.

Exam Essentials

Know how to manage device drivers. Know how to update a driver or how to disable or remove a driver. Know how to roll back a driver in the event that an updated driver does not work properly.

Monitor and Configure Multiprocessor Computers

Normally, multiple processors are associated with servers. However, Windows XP Professional can support up to two processors.

Critical Information

In the following sections you will learn how to install and configure a second processor and how to monitor a second processor.

Installing and Configuring a Second Processor

If your computer is capable of supporting multiple processors, you should follow the computer manufacturer's instructions for installing the second processor. This usually involves updating the processor's driver to a driver that supports multiple processors through the Upgrade Device Driver Wizard.

Monitoring a Second Processor

Once you install a second processor, you can monitor the processors through the System Monitor utility. You can verify that multiple processors are recognized by the operating system, as well as configure multiple processors, through the Task Manager utility.

Exam Essentials

Be able to install a second processor. Know how to install and monitor a second processor.

Review Questions

1. Your laptop computer dual boots to Windows 2000 Professional and Windows XP Professional. You have a scanner that functions with Windows 2000 Professional but not Windows XP Professional. The driver for Windows XP Professional hasn't been released yet. When you access the device in Windows XP Professional, it causes your computer to blue screen. You want to keep Windows XP Professional from trying to access the device until you get the new driver. Which of the following actions should you take?
   - **A.** Disable the driver in Windows XP.
   - **B.** Use the roll back driver feature to roll back the Windows XP driver to the Windows 2000 Professional driver.
   - **C.** Stop the device in Device Manager.
   - **D.** Create a hardware profile that has the device uninstalled, and use this profile when you boot the computer to Windows XP Professional.

2. You have three USB devices that attach to your computer through a USB hub. All three devices work properly. When you try to attach a USB printer to the hub, it does not work. However when you attach the printer directly to the USB port, the printer works. What should you do?
   - **A.** Disable the other three USB devices.
   - **B.** Ensure that the USB hub meets ISO standard 5434.
   - **C.** Verify the USB support has been configured in the computers BIOS.
   - **D.** Replace the USB hub with a self-powered USB hub.

3. You have a Windows NT 4.0 Professional computer that uses spanned disks that was upgraded to Windows 2000 Professional. Now the computer will be upgraded to Windows XP Professional. You want to retain the disk configuration. What course of action should you take?
   - **A.** While in Windows 2000 Professional, upgrade your disk to a dynamic disk before you start the upgrade to Windows XP Professional.
   - **B.** Before you start the upgrade, back up your data. Create a new spanned disk set after you install Windows XP Professional and restore your data.
   - **C.** After you upgrade the computer to Windows XP Professional, use the `Diskpart` utility to access the drive and format it as a dynamic drive.
   - **D.** Do nothing. The spanned disk will automatically be configured to work with Windows XP Professional.

4. You have installed Windows XP Professional on your desktop computer, which has two hard drives installed. You want to mirror the disk drives for fault tolerance. Which action should you take?
   - **A.** Convert the drives to dynamic drives, then mirror the drives through Disk Administrator.
   - **B.** Convert the drives to dynamic drives, then mirror the drives through the `Diskpart` command-line utility.
   - **C.** Convert the drives to NTFS, then mirror the drives through the `Diskpart` command-line utility.
   - **D.** Windows XP Professional does not support mirrored drives.

5. You have a user who telecommutes from home using a laptop with Windows XP Professional installed. The user normally accesses your network from a cable modem but the cable service is down and she now needs to use the 56Kbps internal modem. She dials into the office and can get a connection, but after about 30 seconds, the connection drops. What course of action should she take?
   - **A.** She should configure the computer to use clear text passwords.
   - **B.** She should reduce the speed of the computer's modem port.
   - **C.** She should configure the modem to use CHAP encryption.
   - **D.** She should configure the modem for RRAS support.

6. You recently installed Windows XP Professional on a new computer. When you try to configure the screen resolution, you are only able to set the resolution for 640×480 with 16 colors. You have an identical computer and monitor that are configured for higher screen resolution that is using Windows XP Professional. What should you do to fix the problem on the new computer?
   - **A.** Install the most current driver for the video card.
   - **B.** Reset the video adapter properties through the Advanced button on the video card Properties page.
   - **C.** Restart the computer, and Windows XP will automatically detect the correct video driver.
   - **D.** Boot the computer to VGA settings mode and then change the screen resolution.

7. You have recently purchased a new printer. When you attach the printer to your computer, Windows XP Professional does not automatically recognize it. How should you install the printer?
   - **A.** Add the printer through Device Manager.
   - **B.** Use the Add Printer Wizard in Printers and Faxes.
   - **C.** Restart your computer to initiate the Found Hardware Wizard.
   - **D.** Install the printer through Print Manager.

8. You recently got an updated driver for your digital camera. After you installed the new driver, you were no longer able to access the digital camera. What is the easiest way to fix this problem?
   - **A.** Uninstall the new driver and reinstall the old driver.
   - **B.** Restore the old driver using Windows Backup.
   - **C.** Use the Roll Back Driver option.
   - **D.** Configure driver signing for Ignore Unsigned Drivers.

9. You are using a laptop with Windows XP Professional. Your computer goes into standby mode whenever it hasn't been accessed for 20 minutes. You want to configure the computer so that it goes into standby mode after 5 minutes, but only when the computer is running from batteries with no access. You never want it to go into standby mode when the laptop is plugged in. How do you configure this?

A. Access Power Options through Control Panel and make the appropriate modifications on the Power Scheme tab.

B. Configure the ACPI power options through the computer's BIOS settings.

C. Access Power Options through Control Panel and make the appropriate modifications on the Power Meter tab.

D. Configure the ACPI power options through ACPI in Device Manager.

10. You are the network administrator for a small company. All of your users have Windows XP Professional installed on their computers. You want each user to be able to install printers for their local computers without any administrator intervention. Which of the following options will allow the users to complete this task without excessive permissions?

A. Grant the users the Allow Manage Print Devices right on their computer.

B. Grant the users the Allow Install Print Drivers right on their computer.

C. Make the users members of the Power Users group on their computers.

D. Make the users members of the Administrators group on their computers.

Answers to Review Questions

1. A. You should disable the device. When the correct driver is available, you can enable the device and update the driver.

2. D. If you are using a USB bus-powered hub, the device attached to the hub may require more power than the hub can provide. In this case, you should use a self-powered USB hub. You can determine if the hub is the problem by removing the hub and directly attaching the device to the computer's USB. You can also troubleshoot this error by attaching the device to a self-powered USB hub and seeing if it works.

3. A. When you install Windows XP Professional or upgrade your computer from Windows NT 4 to Windows XP Professional, your drives are configured as basic disks. Windows XP will not read a disk that has been configured with disk spanning or disk striping under Windows NT 4.0. In this case you will need to upgrade your computer to Windows 2000 Professional first and then convert your disk from basic to dynamic. When you upgrade to Windows XP Professional, it will recognize the disk as dynamic and your spanned or striped disk will be recognized and your data will be preserved.

4. D. Dynamic storage supports three dynamic volume types: simple volumes, spanned volumes, and striped volumes. Windows XP Professional does not support mirrored volumes.

5. B. If the modem is having problems connecting, there may be excessive static on the phone line that is preventing the modem from connecting at the configured speed. The user should attempt to connect using lower speed and call the phone company to have the quality of the line checked.

6. A. If you do not have the correct video driver installed, Windows XP will install a generic VGA driver. You need to install the correct video driver so that you can set the screen resolution.

7. B. Before you can access your physical print device under Windows XP Professional, you must first create a logical printer. Windows XP Professional will automatically try and install the printer for you if it is a Plug and Play printer and there is a driver available. If the printer does not automatically install itself, you can create one through the Add Printer Wizard in Control Panel, Printers and Faxes.

8. C. If you updated a driver that was working properly, but you did so with a driver that is not working properly, you should roll back the driver. When you roll back the driver, you uninstall the new driver and revert to the previous driver.

9. A. The Power Schemes tab helps you select the most appropriate power scheme for your computer. Power schemes control automatic turn-off of the monitor and hard disks, based on a specified period of inactivity. This feature allows you to conserve your laptop's battery when the computer isn't being used.

10. C. To create a new printer in Windows XP Professional, the users must be logged on as members of the Administrators or Power Users group.

Chapter 4

Monitoring and Optimizing System Performance and Reliability

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Monitor, optimize, and troubleshoot performance of the Windows XP Professional desktop.**
  - Optimize and troubleshoot memory performance.
  - Optimize and troubleshoot processor utilization.
  - Optimize and troubleshoot disk performance.
  - Optimize and troubleshoot application performance.
  - Configure, manage, and troubleshoot Scheduled Tasks.
- ✓ **Manage, monitor, and optimize system performance for mobile users.**
- ✓ **Restore and back up the operating system, System State data, and user data.**
  - Recover System State data and user data by using Windows Backup.
  - Troubleshoot system restoration by starting in safe mode.
  - Recover System State data and user data by using the Recovery console.

This chapter covers how to monitor, optimize, and troubleshoot Windows XP performance for desktop computers and mobile users. You will also learn how to manage backups for the operating system, System State data, and user data.

Monitoring, Optimizing, and Troubleshooting Performance

To have an optimized system, you must monitor its performance. The two tools for monitoring Windows XP Professional are *System Monitor* and *Performance Logs and Alerts*. With these tools, you can track memory, processor activity, the disk subsystem, the network subsystem, and other computer subsystems.

Critical Information

The System Monitor utility is used to measure the performance of a local or remote computer on the network. System Monitor enables you to do the following:

- Collect data from your local computer or remote computers on the network. You can collect data from a single computer or multiple computers concurrently.
- View data as it is being collected in real-time, or historically from collected data.
- Have full control over the selection of what data will be collected by selecting which specific objects and counters will be collected.
- Choose the sampling parameters that will be used, meaning the time interval that you want to use for collecting data points and the time period that will be used for data collection.
- Determine the format in which data will be viewed in either graph, histogram, or report views.
- Create HTML pages for viewing data.
- Create specific configurations for monitoring data that can then be exported to other computers for performance monitoring.

In order to view data on remote computers, you need to have administrative rights to the remote computer.

Through System Monitor, you can view current data or data from a log file. When you view current data, you are monitoring real-time activity. When you view data from a log file, you are importing a log file from a previous session.

You can access System Monitor through Start ➢ All Programs ➢ Administrative Tools ➢ Performance or as a Microsoft Management Console (MMC) snap-in. The System Monitor snap-in is added as an ActiveX control. Figure 4.1 shows the main System Monitor window when it is initially opened without configuration.

Using Performance Logs and Alerts

The Performance Logs and Alerts snap-in to the MMC is shown expanded in Figure 4.2. With it, you can create counter logs and trace logs, and you can define alerts. You can view the log files with the System Monitor, as described in the previous section. You open Performance Logs and Alerts by selecting Start ➢ All Programs ➢ Administrative Tools ➢ Performance and clicking Performance Logs and Alerts.

Optimizing and Troubleshooting Memory Performance

When the operating system needs a program or process, the first place it looks is in physical memory. If the required program or process is not in physical memory, the system looks in logical memory (the page file). If the program or process is not in logical memory, the system then must retrieve the program or process from the hard disk. It can take thousands of times longer to access information from the hard disk than to get it from physical RAM. If your computer is using excessive paging, this indicates that your computer does not have enough physical memory.

FIGURE 4.1 The main System Monitor window

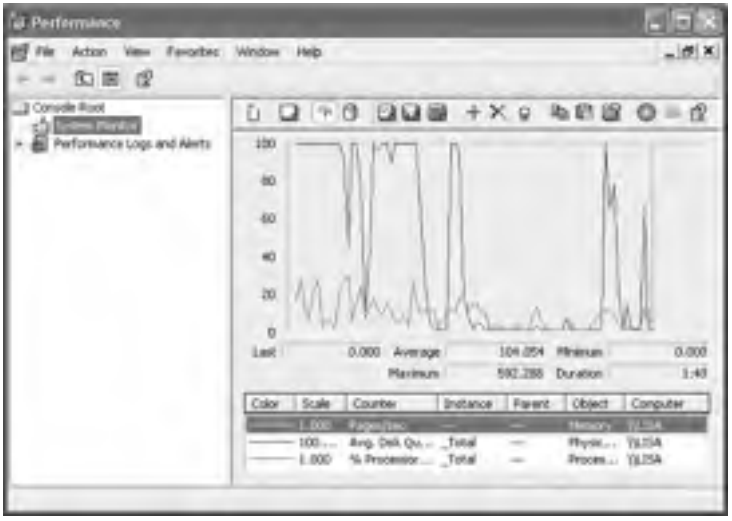
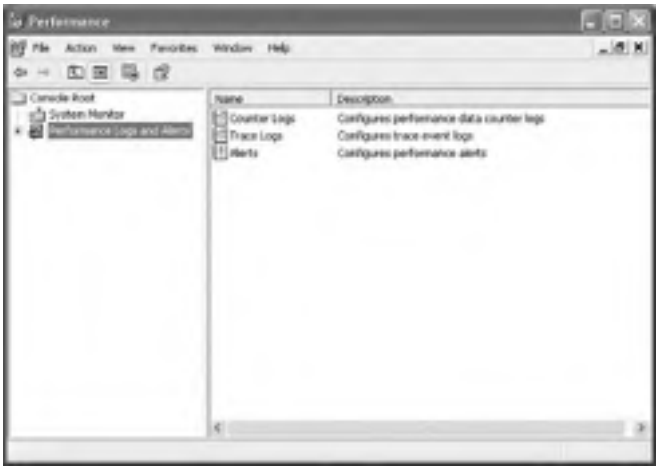


FIGURE 4.2 The expanded Performance Logs and Alerts snap-in



Insufficient memory is the most likely cause of system bottlenecks. If you have no idea what is causing a system bottleneck, memory is usually a good place to start checking. To determine how memory is being used, you need to examine two areas:

Physical memory The physical RAM you have installed on your computer. You can't have too much memory. It's actually a good idea to have more memory than you think you will need just to be on the safe side. As you've probably noticed, each time you add or upgrade applications, you require more system memory.

Page file *Page file* is the logical memory that exists on the hard drive. If you are using excessive paging (swapping between the page file and physical RAM), it's a clear sign that you need to add more memory.

The first step in memory management is determining how much memory your computer has installed and what the appropriate memory requirements are based on the operating system requirements and the applications and services you are running on your computer.

In this book, we use the following format for describing performance object counters: performance object > counter. For example, Memory > Available MBytes denotes the Memory performance object and the Available MBytes counter.

Key Counters to Track for Memory Management

Following are the three most important counters for monitoring memory:

Memory > Available MBytes Measures the amount of physical memory that is available to run processes on the computer. If this number is less than 4MB, it indicates that you have an

overall shortage of physical memory for your computer, or possibly, that you have an application that is not releasing memory properly. You should consider adding more memory or evaluating application memory usage.

Memory > Pages/Sec Shows the number of times the requested information was not in memory and had to be retrieved from disk. This counter's value should be below 20; for optimal performance, it should be 4 or 5. If the number is above 20, you should add memory or research paging file use more thoroughly. Sometimes a high Pages/Sec counter indicates a program using a memory-mapped file.

Paging File > % Usage Indicates the percentage of the allocated page file that is currently in use. If this number is consistently over 70 percent, you may need to add more memory or increase the size of the page file.

These counters work together to show what is happening on your system. Use the Paging File > % Usage counter value in conjunction with the Memory > Available MBytes and Memory > Pages/Sec counters to determine how much paging is occurring on your computer.

If you suspect that one of your applications has a memory leak (a memory leak happens when a program uses an area of memory and when done does not release it to be used by other programs), you should monitor the following counters:

- Memory > Available Bytes
- Memory > Committed Bytes
- Process > Private Bytes (for the application you suspect is leaking memory)
- Process > Working Set (for the application you suspect is leaking memory)
- Process > Handle Count (for the application you suspect is leaking memory)
- Memory > Pool Nonpaged Bytes
- Memory > Pool Nonpaged Allocs

Managing the Windows XP Page File

Typically, if your computer is experiencing excessive paging, the best way to optimize memory is to add more physical memory. However, there are some other options for managing the paging file for better performance. They include

- Spreading the page file across multiple hard disks, which allows the disk I/O associated with paging to be spread over multiple disk I/O channels, for faster access.
- Increasing the size of the page file if you have sufficient disk space. By default, Windows XP Professional creates a page file (`pagefile.sys`) that is 1.5 times the amount of physical memory that has been installed on your computer. You would want to consider increasing the page file size if the Paging File > %Usage counter was near 100%.

Here are the main counters for tracking page file usage:

- Paging File > %Usage
- Paging File > %Usage Peak (bytes)

If a paging file reaches the maximum size, the user will see a warning displayed and the system might halt. This is another reason to monitor the page file and increase the size.

Tuning and Upgrading Memory

If you suspect that you have a memory bottleneck, the following options can be used to tune or upgrade memory:

- Increase the amount of physical memory that is installed on the computer.
- If your computer has multiple disk channels, create multiple page files across the disk channels.
- Verify that your paging file is sized correctly.
- Try to run less memory-intensive applications.
- Try to avoid having your paging file on the same partition as the system files.

Optimizing and Troubleshooting Processor Utilization

Processor bottlenecks can develop when the threads of a process require more processing cycles than are currently available. In this case, the process will wait in a processor queue and system responsiveness will be slower than if process requests could be immediately served. The most common causes of processor bottlenecks are processor-intensive applications and other subsystem components that generate excessive processor interrupts (for example, disk or network subsystems).

In a workstation environment, processors are usually not the source of bottlenecks. You should still monitor this subsystem to make sure that processor utilization is at an efficient level.

Key Counters to Track for Processor

You can track processor utilization through the Processor and System objects to determine whether a processor bottleneck exists. The following are the two most important counters for monitoring the system processor:

Processor > %Processor Time Measures the time that the processor spends responding to system requests. If this value is consistently above an average of 85 percent, you may have a processor bottleneck. The Processor > %User Time and Processor > %Privileged Time counters combine to show the total %Processor Time counter. You can monitor these counters individually for more detail.

Processor > Interrupts/Sec Shows the average number of hardware interrupts received by the processor each second. If this value is more than 1,000 on a Pentium computer, you might have a problem with a program or hardware that is generating spurious interrupts.

System > Processor Queue Length Used to determine whether a processor bottleneck is due to high levels of demand for processor time. If a queue of two or more items exists, a processor bottleneck may be indicated.

If you suspect that a processor bottleneck is due to excessive hardware I/O requests or improperly configured interrupt requests (IRQs), then you should also monitor the System > File Control Bytes/Sec counter.

Tuning and Upgrading the Processor

If you suspect that you have a processor bottleneck, you can try the following solutions:

- Use applications that are less processor-intensive.
- Upgrade your processor.
- If your computer supports multiple processors, add one. Windows XP Professional can support up to two processors, which will help if you use multithreaded applications. You can also use processor affinity to help manage processor-intensive applications. Processor affinity is the ability to choose which processor a program can use.

Optimizing and Troubleshooting Disk Performance

Disk access is the amount of time your disk subsystem takes to retrieve data that is requested by the operating system. The two factors that determine how quickly your disk subsystem will respond to system requests are the average disk access time on your hard drive and the speed of your disk controller.

Key Counters to Track for the Disk Subsystem

You can monitor the PhysicalDisk object, which is the sum of all logical drives on a single physical drive, or you can monitor the LogicalDisk object, which represents a specific logical disk. Following are the most important counters for monitoring the disk subsystem. These counters can be tracked for both the PhysicalDisk object and the LogicalDisk object.

PhysicalDisk > %Disk Time Shows the amount of time the physical disk is busy because it is servicing read or write requests. If the disk is busy more than 90 percent of the time, you will improve performance by adding another disk channel and splitting the disk I/O requests between the channels.

PhysicalDisk > %Current Disk Queue Length Indicates the number of outstanding disk requests that are waiting to be processed. This value should be less than 2.

PhysicalDisk > %Disk Reads/sec Specifies the numbers of time the disk has been read in the last second. In the event that the disk becomes fragmented, this number can increase over time even when you are monitoring the same set of files.

Tuning and Upgrading the Disk Subsystem

When you suspect that you have a disk subsystem bottleneck, the first thing you should check is your memory subsystem. Insufficient physical memory can cause excessive paging, which in turn affects the disk subsystem. If you do not have a memory problem, you can try the following solutions to improve disk performance:

- Use faster disks and controllers.
- Confirm that you have the latest drivers for your disk host adapters.

- Use Disk Manager to use disk striping to take advantage of multiple I/O channels.
- Balance heavily used files on multiple I/O channels.
- Add another disk controller for load balancing.
- If you have files that are heavily fragmented, use Disk Defragmenter to consolidate files so that disk space and data access are optimized.
- If you are on a network, distribute applications that have high disk I/O through the Distributed File System (DFS) to balance workload.

Optimizing and Troubleshooting Application Performance

The *Task Manager* utility shows the applications and processes that are currently running on your computer, as well as CPU and memory usage information. Task Manager is easier to use than System Monitor or Performance Logs and Alerts since it doesn't require any configuration. To access Task Manager, press Ctrl+Alt+Delete. Alternatively, right-click an empty area in the Taskbar and select Task Manager from the pop-up menu.

The Task Manager dialog box has five main tabs, Applications, Processes, Performance, Networking, and Users. The options for Applications, Processes, and Performance, which relate to application performance, are covered in the following subsections.

Managing Application Tasks

The Applications tab of the Task Manager dialog box, shown in Figure 4.3, lists all of the applications that are currently running on the computer. For each task, you will see the name of the task and the current status (running, not responding, or stopped).

FIGURE 4.3 The Applications tab of the Task Manager dialog box

To close an application, select it and click the End Task button at the bottom of the dialog box. To make the application window active, select it and click the Switch To button. If you want to start an application that isn't running, click the New Task button and specify the location and name of the program you wish to start.

Managing Process Tasks

The Processes tab of the Task Manager dialog box, shown in Figure 4.4, lists all the processes that are currently running on the computer. This is a convenient way to get a quick look at how your system is performing. Unlike System Monitor, Task Manager doesn't require that you first configure the collection of this data; it's gathered automatically.

For each process, you will see Image Name (the name of the process), User Name (the user account that is running the process), CPU (the amount of CPU utilization for the process), and Mem Usage (the amount of memory that is being used by the process).

From the Processes tab, you can organize the listing and control processes as follows:

- To organize the processes based on usage, click the column headings. For example, if you click the CPU column, the listing will start with the processes that use the most CPU resources. If you click the CPU column a second time, the listing will be reversed.
- To manage a process, right-click it and choose an option from the pop-up menu. You can choose to end the process, end the process tree, or set the priority of the process (to Realtime, High, Abovenormal, Normal, Belownormal, or Low). If your computer has multiple processors installed, you can also set processor affinity (the process of associating a specific process with a specific processor) for a process.
- To customize the counters that are listed, select View ➢ Select Columns. This brings up the Select Columns dialog box, shown in Figure 4.5, where you can select the information that you want to see listed on the Processes tab.

FIGURE 4.4 The Processes tab of the Task Manager dialog box

FIGURE 4.5 Selecting information for the Task Manager's Processes tab

In the following subsections you will learn how to stop processes and manage process priority.

STOPPING PROCESSES

You may need to stop a process that isn't executing properly. To stop a specific process, select the process you want to stop in the Task Manager's Processes tab and click the End Process button. Task Manager displays a Warning dialog box. Click the Yes button to terminate the process.

If you right-click a process, you can end the specific process or you can use the option End Process Tree. The End Process Tree option ends all processes that have been created either directly or indirectly by the process.

Some of the common processes that can be managed through Task Manager are listed in Table 4.1.

TABLE 4.1 Common Processes

Process	Description
System Idle Process	A process that runs when the processor is not executing any other threads
`smss.exe`	Session Manager subsystem
`csrss.exe`	Client-server runtime server service
`mmc.exe`	Microsoft Management Console program (used to track resources used by MMC snap-ins such as System Monitor)
`explorer.exe`	Windows Explorer interface
`Ntvdm.exe`	MS-DOS and Windows 16-bit application support

MANAGING PROCESS PRIORITY

You can manage process priority through the Task Manager utility or through the `start` command-line utility. To change the priority of a process that is already running, use the Processes tab of Task Manager. Right-click the process you want to manage and select Set Priority from the pop-up menu. You can select from Realtime, High, Abovenormal, Normal, Belownormal, and Low priorities.

To start applications and set their priority at the same time, use the `start` command. The options that can be used with the `start` command are listed in Table 4.2.

TABLE 4.2 Options for the `start` Command-Line Utility

Option	Description
`/low`	Starts an application in the idle priority class.
`/normal`	Starts an application in the Normal priority class.
`/high`	Starts an application in the High priority class.
`/realtime`	Starts an application in the Realtime priority class.
`/abovenormal`	Starts an application in the Abovenormal priority class.
`/belownormal`	Starts an application in the Belownormal priority class.
`/min`	Starts the application in a minimized window.
`/max`	Starts the application in a maximized window.
`/separate`	Starts a Windows 16-bit application in a separate memory space. By default, Windows 16-bit applications run in a shared memory space—an NTVDM, or NT Virtual DOS Machine.
`/shared`	Starts a DOS or Windows 16-bit application in a shared memory space.

Running a process-intensive application in a higher priority class can significantly impact Windows XP Professional performance.

Configuring, Managing, and Troubleshooting Scheduled Tasks

Windows XP Professional includes a Task Scheduler utility that allows you to schedule tasks to occur at specified intervals. You can set any of your Windows programs to run automatically at a specific time and at a set interval, such as daily, weekly, or monthly. For example, you might schedule your Windows Backup program to run daily at 2:00 a.m.

The following steps are used to create a scheduled task:

1. Select Start ➢ Control Panel ➢ Performance and Maintenance, and select Scheduled Tasks.
2. In the Scheduled Tasks window, double-click the Add Scheduled Task icon.
3. When the first page of the Scheduled Task Wizard appears, click the Next button to continue.
4. The first Scheduled Task Wizard dialog box lists applications you can run. You can select an application from the list or click the Browse button to locate any application or program to which your computer has access. After you select an application, click the Next button.
5. The next wizard dialog box prompts you to select a name for the task and specify when it will be performed. Make your selection and click the Next button.
6. Depending on the selection you made for the task's schedule, you may see another dialog box for setting the specific schedule. For example, if you chose to run the task weekly, the next dialog box lets you select the start time for the task, choose to run the task every *x* weeks, and pick the day of the week that the task should be run. Make your selection and click the Next button.
7. Next, you are prompted to enter the username and the password that will be used to start the task. After you enter this information, click the Next button.
8. The final dialog box shows your selections for the scheduled task. If this information is correct, click the Finish button.

Managing Scheduled Task Properties

You can manage a scheduled task through its properties dialog box; Figure 4.6 shows the properties for the Calculator job. To access this dialog box, open the Scheduled Tasks window (Start ➢ Control Panel ➢ Performance and Maintenance, and then select Scheduled Tasks). Right-click the task you wish to manage, and choose Properties from the pop-up menu.

FIGURE 4.6 The Task properties for the scheduled task

The scheduled task properties dialog box has three tabs, Task, Schedule, and Settings, with options for managing how and when the task is run and who can manage it. These options are described in the following sections.

TASK PROPERTIES

Through the Task tab, you can configure the following options:

- The command-line program that is used to run the task
- The folders containing related files that might be required to run the specified task (this is the Start In information)
- Any comments that you want to include for informational purposes
- The username and password to be used to run the specified task (this is the Run As information)
- Whether the scheduled task is enabled

SCHEDULE PROPERTIES

The Schedule tab, shown in Figure 4.7, shows the schedule configured for the task. You can change any of these options to reschedule the task.

SETTINGS PROPERTIES

The Settings tab (Figure 4.8) offers several configuration settings for the scheduled task:

- The options in the Scheduled Task Completed section allow you to delete the task if it will not be run again and specify how long the task should be allowed to run before it is stopped.

FIGURE 4.7 The Schedule properties for the scheduled task

- The options in the Idle Time section are useful if the computer must be idle when the task is run. You can specify how long the computer must be idle before the task begins and whether the task should be stopped if the computer ceases to be idle.
- The options in the Power Management section are applicable when the computer on which the task runs may be battery powered. You can specify that the task should not start if the computer is running from batteries and choose to stop the task if battery mode begins.

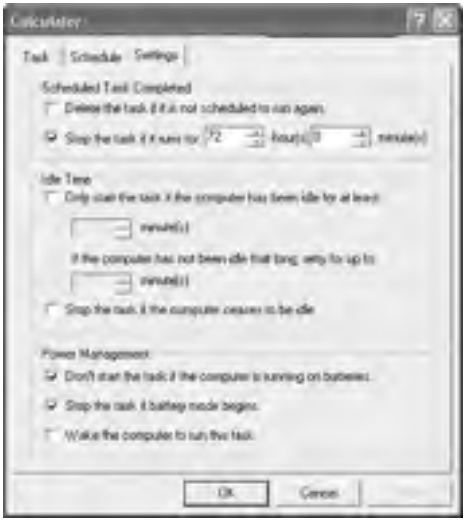
If you are using Task Scheduler and your jobs are not running properly, make sure that the Task Scheduler service is running and is configured to start automatically. You should also ensure that the user who is configured to run the scheduled task has sufficient permissions to run the task.

Troubleshooting Scheduled Tasks

If you are trying to use Scheduled Tasks and the tasks are not being executed properly, one of the following troubleshooting options may resolve the problem.

- If a scheduled task does not run as expected, right-click the task and select Properties. From the Task tab, verify that the Enabled check box is selected. From the Schedule tab, verify the schedule that has been defined for the task to run.
- If the scheduled task is a command-line utility, make sure that you have properly defined the command-line utility, including any options that are required for the utility to run properly.

FIGURE 4.8 The Settings tab of the scheduled task dialog box



- Verify that the user who is configured to run the scheduled task has the necessary permissions to the task that will be run.
- Within the Scheduled Tasks window, check the task status within the Status column. The status types are defined as follows:
  - Blank, which indicates that the task is not running, or that it was run successfully
  - Running, which means that the task is currently being run
  - Missed, which specifies that one or more attempts to run the task were missed
  - Could not start, which indicates that the most recent attempt to start the task failed
- Verify that the Scheduled Tasks service has been enabled on the computer if no tasks can be run on the computer.

If no user is logged into the computer when the task is scheduled to be run, the task will still run, but it will not be visible.

Exam Essentials

Be able to optimize memory, processor, and disk performance. Know the key counters that are used to track performance. Know when a counter indicates a bottleneck and how to resolve the bottleneck.

Know how to monitor and manage application performance. Be able to use Task Manager to monitor applications. Know how to set processor affinity. Be able to manage application priorities through Task Manager or the `start` command-line utility.

Know how to use scheduled tasks. Be able to create and troubleshoot a scheduled task.

Manage, Monitor, and Optimize System Performance for Mobile Users

In the following sections, you will learn how to manage, monitor, and optimize system performance for mobile users by managing power schemes and by using standby and hibernation, and hardware profiles.

Critical Information

The power schemes help you select the most appropriate power scheme for your laptop. Power schemes control automatic turn-off of the monitor and hard disks based on a specified period of inactivity. This feature allows you to conserve your laptop's battery when the computer isn't

being used. From the drop-down list, you can select one of the preconfigured power schemes listed in Table 4.3. Alternatively, you can create a custom power scheme by clicking the Save As button, giving the power scheme a new name, and choosing power scheme options.

TABLE 4.3 Windows XP Power Schemes

Power Scheme	Turn Off Monitor	Turn Off Hard Disks
Home/Office Desk	After 20 minutes	Never
Portable/Laptop	After 15 minutes	After 30 minutes
Presentation	Never	Never
Always On	After 20 minutes	Never
Minimal Power Management	After 15 minutes	Never
Max Battery	After 15 minutes	Never

Using Standby and Hibernation

In Windows XP, the Advanced Configuration Power Interface (ACPI) specifies six different levels of power states:

- Complete shutdown of PC
- Hibernation
- Standby (three levels)
- Fully active PC

The similarity between hibernation and standby is that they both allow you to avoid shutting down your computer to save power. The key difference is in your computer's state of shutdown.

Hibernation falls short of a complete shutdown of the computer. With hibernation, the computer saves all of your desktop state as well as any open files. To use the computer again, press the power button. The computer starts more quickly than from a complete shutdown because it does not have to go through the complete startup process. You will have to again log on to the computer. You will also notice that all the documents that were open when the computer went into hibernation are still available. With hibernation, you can easily resume work where you left off. You can configure your computer to hibernate through Power Options, or by entering Start ➢ Shut Down and then selecting Hibernate from the drop-down menu. This option will appear only if hibernation has been enabled through Power Options.

Standby does not save data automatically as hibernation does. With standby, you can access your computer more quickly than a computer that is in hibernation, usually through a mouse click or keystroke, and the desktop appears as it was prior to the standby. The response time

depends on the level of your computer's standby state. On an ACPI-compliant computer, there are three levels of standby, each level putting the computer into a deeper sleep. The first level turns off power to the monitor and hard drives. The second level turns off power to the CPU and cache. The third level supplies power to RAM only and preserves the Desktop in memory. You will see an option to configure standby only on Windows XP computers in which a battery has been detected. You can configure your computer for standby through Power Options, or by selecting Start ➢ Shut Down and then choosing Standby from the drop-down menu. This option will appear only if standby has been enabled through Power Options.

Using Hardware Profiles

A hardware profile contains all of the settings for a computer. Any time you make configuration changes to your computer, the changes are automatically saved in the hardware profile. If your computer uses multiple configuration settings—for example, a laptop that uses different devices at different locations—you can create multiple hardware profiles for the different configurations the computer uses. If you have only one hardware profile, it is loaded by default when the computer starts. If you have multiple hardware profiles, you are prompted to select the hardware profile you want to use when the computer is started. You are able to specify what profile is used by default.

To create alternate hardware profiles, you would take the following steps:

1. Select Start ➢ Control Panel ➢ Performance and Maintenance ➢ System.
2. From the Hardware tab, select the Hardware Profiles button.
3. From the Hardware Profiles dialog box, shown in Figure 4.9, click the Copy button to create a new profile.

FIGURE 4.9 Hardware Profiles dialog box

4. In the Copy Profile dialog box, specify a name for the new profile and click the OK button.
5. Restart Windows XP Professional, and select the new profile when prompted during the startup process.
6. Make any changes needed to the hardware profile. For example, if you have a laptop computer and you want to conserve power for unused devices with this profile, access Device Manager and disable the devices that will not be used.
7. Any changes you make to the profile will be saved automatically when the computer is shut down.

If you are no longer using multiple hardware profiles, you should delete the unused profile so the user will not be prompted to select a hardware profile during the Windows XP Professional startup process.

Exam Essentials

Be able to optimize system performance on a laptop. Understand how to use and optimize power schemes, standby and hibernation, and hardware profiles to manage your laptop.

Restoring and Backing Up the Operating System, System State Data, and User Data

Backups are the best protection you can have against system failure. You can create backups through the Backup utility, which offers options to run the Backup and Restore Wizard and the Automated System Recovery Wizard.

Critical Information

The Windows XP *Backup utility* allows you to create and restore backups. Backups protect your data in the event of system failure by storing the data on another medium, such as another hard disk or a tape. If your original data is lost due to corruption, deletion, or media failure, you can restore the data using your backup. *System State data* includes the Registry, the COM_ registration database, and the system boot files.

To access the Backup utility, select Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Backup. In the Welcome to the Backup or Restore Wizard dialog box, select the Advanced Mode option. This brings up the Backup Utility window, as shown in Figure 4.10.

From this window, you can start the Backup Wizard, the Restore Wizard, or the Automated System Recovery Wizard. These options, as well as some additional backup options, are all covered in the following sections.

FIGURE 4.10 The Advanced Mode window of the Backup Utility

External tape drives, which attach to your parallel port, are not supported by the Windows XP Professional operating system when using the Backup utility. However, you can use third-party backup software to support this configuration.

Using the Backup Wizard

The *Backup Wizard* takes you through all the steps that are required for a successful backup. Before you start the Backup Wizard, be sure you are logged on as an administrator or a member of the Backup Operators group.

Configuring Backup Options

You can configure specific backup configurations by selecting backup options. To access these options, start the Backup utility and select Tools ➢ Options. In the Options dialog box that appears, you'll have five tabs: General, Restore, Backup Type, Backup Log, and Exclude Files. The following sections describe the options on these tabs, used for controlling the backup and restore processes.

Configuring General Backup Options

The General tab, as seen in Figure 4.11, contains options for configuring backup sessions. Table 4.4 describes these options.

FIGURE 4.11 The General tab of the Backup utility's Options dialog box

TABLE 4.4 General Backup Options

Option	Description
Compute selection information before backup and restore operations.	Estimates the number of files and bytes that will be backed up or restored during the current operation and displays this information prior to the backup or restore operation.
Use the catalogs on the media to speed up building restore catalogs on disk.	Specifies that you want to use an on-media catalog to build an on-disk catalog, which can be used to select the folders and files to be restored during a restore operation.
Verify data after the backup completes.	Makes sure that all data has been backed up properly.
Back up the contents of mounted drives.	Specifies that the data should be backed up on mounted drives; otherwise, only path information on mounted drives is backed up.
Show alert message when I start the Backup utility and Removable Storage is not running.	Notifies you if Removable Storage is not running (when you are backing up to tape or other removable media).

TABLE 4.4 General Backup Options *(continued)*

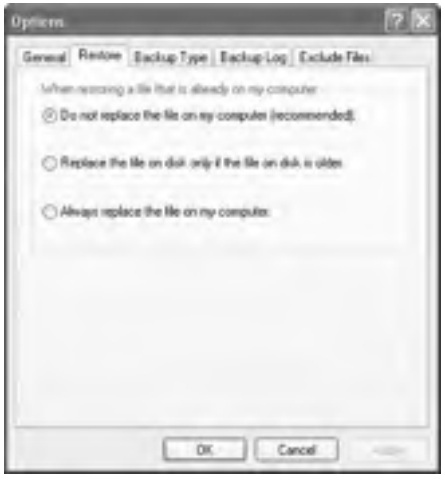
Option	Description
Show alert message when I start the Backup utility and there is recognizable media available.	Notifies you when you start Backup if new media has been added to the Removable Storage import pool.
Show alert message when new media is inserted.	Notifies you when new media is detected by Removable Storage.
Always allow use of recognizable media without prompting.	Specifies that if new media is detected by Removable Storage, that media should be directed to the Backup media pool.

Configuring Restore Options

The Restore tab of the Options dialog box, shown in Figure 4.12, contains three options that relate to how files are restored when the file already exists on the computer:

- Do not replace the file on my computer (recommended).
- Replace the file on disk only if the file on disk is older.
- Always replace the file on my computer.

FIGURE 4.12 The Restore tab of the Backup utility's Options dialog box



Selecting a Backup Type

In the Backup Type tab (Figure 4.13), you can specify the default backup type that will be used. You should select this default backup type based on the following criteria:

- How much data you are backing up
- How quickly you want to be able to perform the backup
- The number of tapes you are willing to use should you need to perform a restore operation

Table 4.5 describes the backup type options.

TABLE 4.5 Backup Type Options

Option	Description
Normal	Backs up all files, and sets the archive bit as marked for each file that is backed up. Requires only one tape for the restore process.
Copy	Backs up all files, and does not set the archive bit as marked for each file that is backed up. Requires only one tape for the restore process.
Differential	Backs up only the files that have not been marked as archived, and does not set the archive bit for each file that is backed up. Requires the last normal backup and the last differential tape for the restore process.
Incremental	Backs up only the files that have not been marked as archived, and sets the archive bit for each file that is backed up. For the restore process, requires the last normal backup and all the incremental tapes that have been created since the last normal backup.
Daily	Backs up only the files that have been changed today and does not set the archive bit for each file that is backed up. Requires each daily backup and the last normal backup for the restore process.

Setting Backup Log Options

The Backup Log tab (Figure 4.14) allows you to specify the amount of information that is logged during the backup process. Table 4.6 describes the backup log options.

TABLE 4.6 Backup Log Options

Option	Description
Detailed	Logs all information, including the names of the folders and files that are backed up.
Summary	Logs only key backup operations, such as starting the backup.
None	Specifies that a log file will not be created.

FIGURE 4.13 The Backup Type tab of the Backup utility's Options dialog box

FIGURE 4.14 The Backup Log tab of the Backup utility's Options dialog box

Excluding Files

Use the Exclude Files tab of the Options dialog box (Figure 4.15) to explicitly exclude specific files during the backup process. For example, you might choose to exclude the page file or application files by clicking the Add New button and selecting the files you want to be excluded. The top of the dialog box allows you to specify the files that will be excluded for all users of the computer. The bottom of the dialog box allows you to exclude files that will not be backed up for the current user.

FIGURE 4.15 The Exclude Files tab of the Backup utility's Options dialog box

Using the Restore Wizard

Having a complete backup won't help you if your system should fail, unless you can successfully restore that backup. To be sure that you can restore your data, you should test the restoration process before anything goes wrong. You can use the Restore Wizard for testing purposes, as well as when you actually need to restore your backup.

Using the Automated System Recovery Wizard

Windows XP Professional and Windows Server 2003 now include a new feature of the Backup utility called the Automated System Recovery Wizard. The Automated System Recovery Wizard is used for system recovery in the event of system failure. It is a two-part system recovery that consists of a backup component and a restore component. The system information that is backed up by *Automated System Recovery (ASR)* includes System State data, system services, and disk configuration information (information about basic and dynamic disks and the file signature associated with each disk).

This utility is only used to back up system data and does not back up folders and files.

You should only use the Automated System Recovery Wizard for system recovery after you have tried to boot the computer to Safe Mode and used the Last Known Good Configuration option. You should always try the easiest and least invasive methods of recovery before trying more complex recovery options.

Troubleshooting System Restoration by Starting in Safe Mode

The Windows XP advanced startup options can be used to troubleshoot errors that keep Windows XP Professional from successfully booting.

To access the Windows XP advanced startup options, press the F8 key when prompted during the beginning of the Windows XP Professional boot process. This will bring up the Windows XP Advanced Options menu, which offers numerous options for booting Windows XP. If Windows XP Professional starts without displaying the Boot Loader menu, you should press F8 after the firmware Power On Self Test (POST) process, before Windows XP Professional displays graphical output, to access the Advanced Options menu.

These advanced startup options are covered in the following three sections.

Starting in Safe Mode

When your computer will not start, one of the fundamental troubleshooting techniques is to simplify the configuration as much as possible. This is especially important when you do not know the cause of your problem and you have a complex configuration. After you have simplified the configuration, you can determine whether the problem is in the basic configuration or is a result of your complex configuration. If the problem is in the basic configuration, you have a starting point for troubleshooting. If the problem is not in the basic configuration, you should proceed to restore each configuration option you removed, one at a time. This helps you to identify what is causing the error.

If Windows XP Professional will not load, you can attempt to load the operating system through *Safe Mode*. When you run Windows XP in Safe Mode, you are simplifying your Windows configuration as much as possible. Safe Mode loads only the drivers needed to get the computer up and running. The drivers that are loaded with Safe Mode include basic files and drivers for the mouse (unless you have a serial mouse), monitor, keyboard, hard drive, standard video driver, and default system services. Safe Mode is considered a diagnostic mode, so you do not have access to all of the features and devices in Windows XP Professional that you have access to when you boot normally, including networking capabilities.

A computer booted to Safe Mode will show "Safe Mode" in the four corners of your Desktop. If you boot to Safe Mode, check all of your computer's hardware and software settings in Device Manager and try to determine why Windows XP Professional will not boot properly. After you take steps to fix the problem, try to boot to Windows XP Professional as you normally would.

The following steps are used to start a computer in safe mode.

1. If your computer is currently running, select Start ➢ Shutdown ➢ Restart.
2. During the boot process, press the F8 key to access the Windows XP Advanced Options menu. If you do not see the Boot Loader menu, which displays the operating system selections, press F8 after the firmware POST process and before Windows XP Professional displays graphical output, in order to access the Advanced Options menu.
3. Highlight Safe Mode and press Enter. Then log on as Administrator.
4. When you see the Desktop dialog box letting you know that Windows XP is running in Safe Mode, click the OK button.

Enabling Boot Logging

Boot logging creates a log file that tracks the loading of drivers and services. When you choose the Enable Boot Logging option from the Advanced Options menu, Windows XP Professional loads normally, not in Safe Mode. This allows you to log all of the processes that take place during a normal boot sequence.

This log file can be used to troubleshoot the boot process. When logging is enabled, the log file is written to `\Windir\Ntbtlog.txt`.

The boot log file is cumulative. Each time you boot to any Advanced Options menu mode (except Last Known Good Configuration), you are writing to this file. This allows you to make changes, reboot, and see if you have fixed any problems. If you want to start from scratch, you should manually delete this file and reboot to an Advanced Options menu selection that supports logging.

Using Other Advanced Options Menu Modes

In this section, you will learn about the additional Advanced Options menu modes. These include the following:

Safe Mode with Networking This is the same as the Safe Mode option but adds networking features. You might use this mode if you need networking capabilities to download drivers or service packs from a network location.

Safe Mode with Command Prompt This starts the computer in Safe Mode, but instead of loading the Windows XP graphical interface, it loads a command prompt. Experienced troubleshooters use this mode.

Enable VGA Mode This loads a standard VGA driver without starting the computer in Safe Mode. You might use this mode if you changed your video driver, did not test it, and tried to boot to Windows XP with a bad driver that would not allow you to access video. The Enable VGA Mode bails you out by loading a default driver, which provides access to video so that you can properly install (and test!) the correct driver for your computer.

When you boot to any Safe Mode, you automatically use VGA mode.

Last Known Good Configuration This boots Windows XP using the Registry information that was saved the last time the computer was successfully booted. You would use this option to restore configuration information if you have improperly configured the computer and have not successfully rebooted the computer. When you use the Last Known Good Configuration option, you lose any system configuration changes that were made since the computer last successfully booted.

Debugging Mode This runs the Kernel Debugger, if it is installed. The Kernel Debugger is an advanced troubleshooting utility.

Boot Normally This boots to Windows XP in the default manner, which means you are not using any of the Advanced Startup options. This option is on the Advanced Options menu in case you accidentally hit F8 during the boot process, but really wanted to boot Windows XP normally.

Recovering System State Data and User Data by Using the Recovery Console

If your computer will not start, and you have tried unsuccessfully to boot to Safe Mode, there's one more option you can try. The *Recovery Console* is designed for administrators and advanced users. It allows you limited access to FAT16, FAT32, and NTFS volumes without starting the Windows XP Professional graphical interface.

Through the Recovery Console, you can perform the following tasks:

- Copy, replace, or rename operating system files and folders. You might have to do this if your boot failure is caused by missing or corrupt files.
- Enable or disable the loading of services when the computer is restarted. If a particular service may be keeping the operating system from booting, you could disable the service. If a particular service is required for successful booting, you want to make sure that the service is configured to start automatically.
- Repair the file system boot sector or the Master Boot Record (MBR). You might use this option if a virus may have damaged the system boot sector or the MBR.
- Create and format partitions on the drives. You might use this option if your disk utilities will not delete or create Windows XP partitions. Normally, you use a disk-partitioning utility for these functions.

In the following sections, you will learn how to access and use the Recovery Console.

Starting the Recovery Console

You can add the Recovery Console to your computer from the Windows XP Professional CD or as a startup option. These options are covered in the following sections.

STARTING THE RECOVERY CONSOLE WITH THE WINDOWS XP CD

To use the Recovery Console from the Windows XP CD, follow these steps:

1. Restart your computer using the Windows XP Professional distribution CD.
2. When prompted, press any key to boot from the CD.
3. In the Welcome to Setup dialog box, press the R key to repair a Windows XP installation.
4. From the Windows XP Repair Options menu, press 1 to repair Windows XP using the Recovery Console. You will then be prompted to supply the Administrator password. The Windows XP Recovery Console will start.

ADDING THE RECOVERY CONSOLE TO WINDOWS XP STARTUP

You can add the Recovery Console to the Windows XP Professional startup options so that it will be available in the event of a system failure. This configuration takes about 7MB of disk space to hold the `CMDCONS` folder and files. To set up this configuration, follow these steps:

1. Insert the Windows XP Professional CD into your CD-ROM drive. You can disable autoplay by pressing the Shift key as the CD is read. From the command prompt, type **cd I386** and press Enter. Then type **`WINNT32 /CMDCONS`**.
2. The Windows XP Setup dialog box appears, asking you to confirm that you want to install the Recovery Console. Click the Yes button.
3. The installation files will be copied to your computer. Then you will see a dialog box letting you know that the Recovery Console has been successfully installed. Click the OK button to continue.

The next time you restart your computer, you will see an option for the Microsoft Windows XP Recovery Console. You will learn how to use the Recovery Console in the next section.

Working with the Recovery Console

After you add the Recovery Console, you can access it by restarting your computer. In the Boot Loader menu, you will see an option for Microsoft Windows XP Recovery Console. Select this option to start the Recovery Console.

Use the Recovery Console with extreme caution. Improper use may cause even more damage than the problems you are trying to fix—such as the computer not booting, requiring a complete reinstallation of the Windows XP Professional operating system.

The Recovery Console presents you with a command prompt and very limited access to system resources. This keeps unauthorized users from using the Recovery Console to access sensitive data. The following are the only folders you can access through the Recovery Console:

- The root folder
- The *`\Windir`* folder and the subfolders of the Windows XP Professional installation
- The `\CMDCONS` folder
- Removable media drives such as CD-ROM drives

If you try to access any other folders besides the ones listed above, you will receive an "access denied" error message.

In the Recovery Console, you cannot copy files from a local hard disk to a floppy disk. You can only copy files from a floppy disk or CD to a hard disk, or from one hard disk to another hard disk. This is for security purposes.

The first option you must specify is which Windows XP operating system you will log on to. Next, you must specify the Administrator password for the system you are logging on to. When

the Recovery Console starts, you can use the commands defined in Table 4.7 (you can see a full list of supported commands by typing Help at the console prompt):

TABLE 4.7 Commands Available with the Recovery Console

Command	Description
ATTRIB	Used to set file attributes. You can set file attributes for Read-only (R), System (S), Hidden (H), or Compressed (C).
BATCH	Used to execute commands in a specified input file.
BOOTCFG	Used to view or configure BOOT.INI settings.
CHDIR (or you can use CD)	Used to navigate the directory structure. If executed without a directory name, the current directory is displayed. (CHDIR and CD work the same way.)
CLS	Used to clear any text that is currently displayed on the console.
CHKDSK	Used to check the disk and display a disk status report.
COPY	Used to copy a single file from one location to another. COPY does not support wildcards and does not copy files to removable media (such as floppy disks).
DELETE (DEL)	Used to delete a single file. Wildcards are not supported. (DELETE and DEL work the same way.)
DIR	Used to display lists of files and subdirectories in the current directory.
DISABLE	Used to disable Windows XP Professional system services and drivers.
DISKPART	Used to manage disk partitions. If executed without a command-line argument, a user interface is displayed.
ENABLE	Used to enable Windows XP Professional system services and drivers.
EXIT	Used to quit the Recovery Console and restart the computer.
EXPAND	Used to expand compressed files.
FIXBOOT	Used to write a new boot sector onto the computer's system partition.
FIXMBR	Used to repair the MBR of the computer's boot partition.

TABLE 4.7 Commands Available with the Recovery Console *(continued)*

Command	Description
FORMAT	Used to prepare a disk for use with Windows XP Professional by formatting the disk as FAT16, FAT32, or NTFS.
HELP	Used to display help information for Recovery Console commands.
LISTSVC	Used to list all available services and drivers on the computer, as well as the current status of each service and driver.
LOGON	If the computer is configured for dual-booting or multi-booting, used to log on to other installations as the local administrator.
MAP	Used to display the current drive letter mappings.
MKDIR (MD)	Used to create new directories. (MKDIR and MD work the same way.)
MORE	Used to display a text file on the console screen. (Same as TYPE.)
NET	Used to access a net services command, for example Net Use or Net Share.
RENAME (REN)	Used to rename a single file. (RENAME and REN work the same way.)
RMDIR (RD)	Used to delete directories. (RMDIR and RD work the same way.)
SYSTEMROOT	Used to specify that the current directory is the system root.
TYPE	Used to display a text file on the console screen. (Same as MORE.)

Exam Essentials

Know how to use the Backup and Restore options of Windows Backup. Know all of the options associated with Windows Backup and how to use Windows Backup and Restore. Know how to use the Automated System Recovery Wizard and why you would use it.

Review Questions

1. You need to be able to save all of the settings (including the Windows configuration and Registry settings) for your Windows XP computer. Which of the following options should you use?
   - **A.** Use Windows Backup to back up the computer's System State data.
   - **B.** Use Windows Backup to back up System Configuration data.
   - **C.** Use Device Manager to back up the computer's System State data.
   - **D.** Use Device Manager to back up the computer's System Configuration data.

2. Your Windows XP Professional has two processors installed. You run several applications and notice that one of your applications takes up a significant amount of processing. When you run the processor-intensive application, the second processor is idle. How can you configure the application to use the second processor?
   - **A.** Configure processor affinity through Task Manager.
   - **B.** Configure the application through the `start` command and use the `/processor= switch`.
   - **C.** Reduce the priority that the application runs at through the `start` command.
   - **D.** Configure processor affinity through Device Manager for the application.

3. You recently purchased a new scanner and installed a driver for it on your Windows XP Professional computer. After you rebooted the computer and logged on, the new driver causes Windows to freeze after a few minutes. What course of action should you take to get the computer up and running as quickly as possible?
   - **A.** Use the Roll Back driver option.
   - **B.** Boot the computer to Safe mode and then disable the device.
   - **C.** Use Recovery Console to disable the device.
   - **D.** Use the Last Known Good Configuration option.

4. You run several applications on your Windows XP Professional computer. One of your applications is an accounting application that runs as a background application. You notice when you process reports that all of your other applications run very slowly. You want to make the other applications more responsive; even if that means that the accounting application will take longer to process reports. What should you do?
   - **A.** Increase the priority for the accounting application.
   - **B.** Decrease the priority for the accounting application.
   - **C.** Increase the priority of the other applications.
   - **D.** Decrease the priority of the other applications.

5. You have a Windows XP Professional computer that won't boot. You suspect that the master boot record has been infected with a virus and the boot files are corrupt. What course of action should you take?

   A. Use the Last Known Good configuration.

   B. Boot Windows XP Professional to Safe Mode.

   C. Use the Recovery Console.

   D. Use Windows Backup to restore the MBR.

6. Your computer is running very slowly. You are running several applications and suspect one of them is processor or memory intensive. What is the quickest way to determine if one of your applications is causing the bottleneck?

   A. Use Dr. Watson.

   B. Use Performance Logs and Alerts.

   C. Use System Monitor.

   D. Use Task Manager.

7. You run Windows XP Professional on a laptop computer with a 20GB hard drive. You use a database program that stores a large file called `data.dat`. You notice that it is taking more time to load than it did a month ago. You want to optimize your disk subsystem. You note that you have plenty of free disk space. The Physical Disk > Disk Read/sec counter is increasing even though you are monitoring the same files over time. What should you do?

   A. Run the Disk Defragmenter utility.

   B. Increase the size of the paging file.

   C. Format your partition as FAT32.

   D. Use DFS to manage your files.

8. You use a Windows XP Professional computer that runs an accounting application. You've noticed when you run the application that your computer runs very slowly. You need the application, so you are trying to determine what the bottleneck is. You run System Monitor and discover that the paging activity is very high. What should you do?

   A. Increase the size of the paging file.

   B. Spread the paging file over two disks.

   C. Upgrade your processor.

   D. Add memory.

9. You are planning a disaster recovery plan for your Windows XP Professional computer. You will create a full backup weekly, but you want to use a backup scheme for the other days of the week that will allow you to back up the files that have changed daily as quickly as possible. You are willing to trade off for a longer recovery process in the event that you need to restore the backup. Which of the following backup options should you use?

   A. Incremental backups

   B. Differential backups

   C. Full backups

   D. Archive-only backups

10. You are required to use two Windows 16-bit legacy applications for your job. One of the Windows 16-bit applications periodically crashes and causes the other application to crash as well. What course of action should you take?

   A. Use processor affinity to configure each application to run on a separate processor.

   B. Upgrade the memory on your computer.

   C. Configure each Windows 16-bit application to run in a separate memory space.

   D. Upgrade the processor on the computer.

Answers to Review Questions

1. A. The Windows XP Backup utility allows you to create and restore backups. Backups protect your data in the event of system failure by storing the data on another medium, such as another hard disk or a tape. If your original data is lost due to corruption, deletion, or media failure, you can restore the data using your backup. System State data includes the Registry, the COM_ registration database, and the system boot files.

2. A. If your computer has multiple processors installed, you can also set processor affinity (the process of associating a specific process with a specific processor) for a process. You can do this from Task Manager through the Processes tab by right-clicking the process and selecting Processor Affinity.

3. B. If Windows XP Professional will not load, you can attempt to load the operating system through Safe Mode. When you run Windows XP in Safe Mode, you are simplifying your Windows configuration as much as possible. Safe Mode loads only the drivers needed to get the computer up and running.

4. B. You can manage process priority through the Task Manager utility or through the `start` command-line utility. To change the priority of a process that is already running, use the Processes tab of Task Manager. Right-click the process you want to manage and select Set Priority from the pop-up menu. You can select from Realtime, High, Abovenormal, Normal, Belownormal, and Low priorities. Running a process-intensive application in a higher priority class can significantly impact Windows XP Professional performance, so you should reduce the priority of the accounting application in this situation.

5. C. The Recovery Console is designed for administrators and advanced users. It allows you limited access to FAT16, FAT32, and NTFS volumes without starting the Windows XP Professional graphical interface. It allows you to copy, replace, or rename operating system files and folders. You might have to do this if your boot failure is caused by missing or corrupt files.

6. D. The Task Manager utility shows the applications and processes that are currently running on your computer, as well as CPU and memory usage information. Task Manager is easier to use than System Monitor or Performance Logs and Alerts since it doesn't require any configuration.

7. A. If you have files that are heavily fragmented, use Disk Defragmenter to consolidate files so that disk space and data access are optimized.

8. D. The page file is logical memory that exists on the hard drive. If you are using excessive paging (swapping between the page file and physical RAM), it's a clear sign that you need to add more memory.

9. A. Incremental backups only back up the files that have not been marked as archived, and they set the archive bit for each file that is backed up. For the restore process, incremental backup requires the last normal backup and all the incremental tapes that have been created since the last normal backup.

10. C. The `start /separate` command line utility runs Windows 16-bit applications in a separate memory spaces. By default, Windows 16-bit applications run in a shared memory space called the NT Virtual DOS Machine (NTVDM).

Chapter 5

Configuring and Troubleshooting the Desktop Environment

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configure and manage user profiles and desktop settings.**
- ✓ **Configure support for multiple languages or multiple locations.**
  - Enable multiple-language support.
  - Configure multiple-language support for users.
  - Configure local settings.
  - Configure Windows XP Professional for multiple locations.
- ✓ **Manage applications by using Windows Installer packages.**

This chapter covers configuring, managing, and troubleshooting the user desktop environment. You will learn about user profiles and desktop settings, how to support multiple language environments, and how to manage applications through Windows Installer packages.

Configure and Manage User Profiles and Desktop Settings

User profiles contain information about the Windows XP environment for a specific user. For example, profile settings include the *desktop* arrangement, program groups, and screen colors that users see when they log on.

Each time you log on to a Windows XP Professional computer, the system checks to see if you have a local user profile in the Documents and Settings folder, which was created on the boot partition when you installed Windows XP Professional.

The first time users log on, they receive a default user profile. A folder that matches the user's logon name is created for the user in the Documents and Settings folder. The user profile folder that is created holds a file called *NTUSER.DAT*, as well as subfolders that contain directory links to the user's desktop items. The default location of a local users profile is `systemdrive:\Documents and Settings\UserName`.

Critical Information

The drawback of local user profiles is that they are available only on the computer where they were created. For example, suppose all of your Windows XP Professional computers are a part of a domain and you use only local user profiles. User Kevin logs on at Computer A and creates a customized user profile. When he logs on to Computer B for the first time, he will receive the default user profile rather than the customized user profile he created on Computer A. In order for users to access their user profile from any computer they log on to, you need to supply them with roaming profiles; however, these profiles need to be able to use a network server and can't be stored on a local Windows XP Professional computer.

In the next sections, you will learn about how roaming profiles and mandatory profiles can be used. In order to have a roaming profile or a mandatory profile, your computer must be a part of a network with server access.

As noted, each user's unique settings are stored in the *systemdrive*:\Documents and Settings*UserName* folder. Settings that are common to all users are stored in the *systemdrive*:\Documents and Settings\All Users folder. If multiple users share a computer, and you don't want any user to affect other users' settings, you should remove permissions for each individual user who accesses the computer from the *systemdrive*:\Documents and Settings\All Users folder.

Roaming Profiles

A *roaming profile* is stored on a network server and allows users to access their user profile, regardless of the client computer to which they're logged on. Roaming profiles provide a consistent desktop for users who move around, no matter which computer they access. Even if the server that stores the roaming profile is unavailable, the user can still log on using a local profile.

Normally you would configure roaming profiles for users who are part of an Active Directory domain. In this case, you would use the Active Directory Users and Computers utility to specify the location of a user's roaming profile.

If you are using roaming profiles, the contents of the user's profile folder will be copied to the local computer each time the roaming profile is accessed. If you have stored large files in any subfolders of your user profile folder, you may notice a significant delay when accessing your profile remotely as opposed to locally. If this problem occurs, you can reduce the amount of time the roaming profile takes to load by moving the subfolder to another location (for example moving the user's My Documents folder to a network share, which is called folder redirection) or you can use Group Policy objects (GPOs) within the Active Directory to specify that specific folders should be excluded when the roaming profile is loaded.

Using Mandatory Profiles

A *mandatory profile* is a profile that can't be modified by the user. Only members of the Administrators group can manage mandatory profiles. You might consider creating mandatory profiles for users who should maintain consistent desktops. For example, suppose that you have a group of 20 salespeople who know enough about system configuration to make changes, but not enough to fix any problems they create. For ease of support, you could use mandatory profiles. This way, all of the salespeople will always have the same profile and will not be able to change their profiles.

You can create mandatory profiles for a single user or a group of users. The mandatory profile is stored in a file named *NTUSER.MAN* (which is created by renaming the NTUSER.DAT file to NTUSER.MAN). A user with a mandatory profile can set different desktop preferences while logged on, but those settings will not be saved when the user logs off.

Only roaming profiles can be used as mandatory profiles. Mandatory profiles do not work for local user profiles.

Managing Desktop Settings

Windows XP Professional can be viewed using the Windows XP theme, the Windows Classic theme (the interface from Windows 2000 Professional), or any customized theme you would like to use. The Windows XP Professional desktop appears after a user has logged on to a Windows XP Professional computer. Users can configure their desktops to suit their personal preferences and to work more efficiently.

You can configure the desktop by customizing the Taskbar and Start menu, adding shortcuts, and setting display properties. These configurations are described in the following sections.

Customizing the Taskbar and Start Menu

Users can customize the Taskbar and Start menu through the Taskbar and Start Menu Properties dialog box, shown in Figure 5.1. The easiest way to access this dialog box is to right-click a blank area in the Taskbar and choose Properties from the pop-up menu.

The Taskbar and Start Menu Properties dialog box has two tabs, Taskbar and Start Menu, containing the options described in the following sections.

FIGURE 5.1 The Taskbar tab of the Taskbar and Start Menu Properties dialog box

CONFIGURING TASKBAR PROPERTIES

Through the Taskbar tab of the Taskbar and Start Menu Properties dialog box (shown in Figure 5.1), you can specify Taskbar and Start menu features, such as whether the Taskbar is always visible and whether the clock is shown on the Start menu. Table 5.1 lists the properties on the Taskbar tab.

TABLE 5.1 Taskbar Properties

Property	Description
Lock the taskbar	Locks the Taskbar into the current position and size so it cannot be moved around the desktop. This option is enabled by default.
Auto-hide the taskbar	Hides the Taskbar. This option is disabled by default. When it is enabled, you show the Taskbar by clicking the area of the screen where the Taskbar appears.
Keep the taskbar on top of other windows	Keeps the Taskbar visible, even if you open full-screen applications. This option is enabled by default.
Group similar taskbar buttons	Keeps all Taskbar buttons for the same program in the same location. Also specifies that if you have many applications open and the Taskbar becomes crowded, all the buttons for a single application should be collapsed into a single button. This option is enabled by default.
Show Quick Launch	Shows the Quick Launch icon on the Taskbar. Quick Launch is used to get back to the Windows desktop with a single click. This option is enabled by default.
Show the clock	Displays a digital clock in the right corner of the Taskbar. By right-clicking the clock, you can adjust the computer's date and time. This option is enabled by default.
Hide inactive icons	Hides icons that have not been recently used. You can access the hidden icons by clicking the double arrow on the left side of the system tray on the Taskbar. This option is enabled by default.

The Customize button in the lower right-hand corner of the dialog box is used to list the icons and notifications for your computer. All current items are listed, and you can define each item's status—for example, you can choose from hide icon when inactive, always hide icon, and always show icon.

CONFIGURING START MENU PROPERTIES

The Start Menu tab of the Taskbar and Start Menu Properties dialog box allows you to customize your Start menu. By selecting Start menu, you edit the Windows XP Professional theme, and by selecting Classic Start menu, you edit the standard Windows 2000 theme.

You can add or remove items from the Start menu, remove records of recently accessed items, and specify which options are displayed by clicking the Customize button for the theme you want to use. Figure 5.2 shows the options for customizing the Start menu for the Windows XP Professional theme.

Using Shortcuts

Shortcuts are links to items that are accessible from your computer or network. You can use a shortcut to quickly access a file, program, folder, printer, or computer from your desktop. Shortcuts can exist in various locations, including on the desktop, on the Start menu, and within folders.

To create a shortcut from Windows Explorer, just right-click the item for which you want to create a shortcut and select Create Shortcut from the pop-up menu. Then you can click the shortcut and drag it to where you want it to appear.

Setting Display Properties

The options in the Display Properties dialog box, shown in Figure 5.3, allow you to customize the appearance of your desktop. You can access this dialog box by right-clicking an empty area on the desktop and selecting Properties from the pop-up menu. Alternatively, you can select Start ➢ Control Panel ➢ Appearance and Themes ➢ Display.

The Display Properties dialog box has five tabs with options that control various aspects of your display:

Themes tab This allows you to customize the background used by your desktop, including the sounds, icons, and other desktop elements that personalize your desktop.

Desktop tab This lets you pick your desktop background, which uses a picture or an HTML document as wallpaper.

FIGURE 5.2 Customize Start Menu dialog box

FIGURE 5.3 The Display Properties dialog box

Screen Saver tab This lets you select a screen saver that will start after the system has been idle for a specified amount of time. You can also specify a password that must be used to re-access the system after it has been idle. When the idle time has been reached, the computer will be locked, and the password of the user who is currently logged on must be entered to access the computer. You can also adjust monitor power settings.

Appearance tab This lets you choose which Windows interface, buttons, color scheme, and font size will be used for the Desktop.

Exam Essentials

Know how to manage user profiles. Be able to create and manage local, roaming, and mandatory user profiles. Be able to implement a roaming mandatory profile.

Be able to manage desktop settings. Know what options are available through the Windows XP Start menu and how to customize the Start menu.

Configure Support for Multiple Languages or Multiple Locations

Windows XP Professional includes support for multiple languages and regional settings. The support that comes with localized versions of Windows XP Professional allows users to view, edit, and print multilingual documents, which are documents that are written in almost any language. You can also specify locale settings for the Desktop to customize items such as the date format and currency for your geographical location.

Critical Information

In addition to configuring your desktop, you can also configure the language and regional settings that are used on your computer desktop. Windows XP Professional supports multiple languages through the use of multilanguage technology. Multilanguage technology is designed to meet the following needs:

- Provide support for multilingual editing of documents
- Provide support for various language interfaces in your environment
- Allow users who speak various languages to share the same computer

Using Multilingual Technology

Windows XP Professional supports user options to view, edit, and process documents in a variety of different languages. These options are provided through Unicode support, National Language Support API, Multilingual API, Resource Files, and Multilingual developer support. Each is discussed here:

Unicode This is an international standard that allows character support for the common characters used in the world's most common languages.

National Language Support API This is used to provide information for locale, character mapping, and keyboard layout. Locale settings are used to set local information such as date and time format, currency format, and country names. Character mapping arranges the mapping of local character encodings to Unicode. Keyboard layout settings include character typing information and sorting information.

Multilingual API This is used to set up applications to support keyboard input and fonts from various language versions of applications. For example, Japanese users will see vertical text, and Arabic users will see right-to-left ligatures. This technology allows users to create mixed-language documents.

Resource files These are files in which Windows XP Professional stores all language-specific information, such as text for help files and dialog boxes. They are separate from the operating system files. System code can thus be shared by all language versions of Windows XP Professional, which allows modular support for different languages.

Multilingual developer support This is a special set of APIs that enables developers to create generic code and then provide support for multiple languages.

Choosing Windows XP Multiple-Language Support

Multilanguage support consists of two technologies:

- Multilingual editing and viewing, which support multiple languages while a user is viewing, editing, and printing documents
- Multilanguage user interfaces, which allow the Windows XP Professional user interface to be presented in different languages

Depending on the level of language support required by your environment, you may use either a localized version of Window XP Professional or the Multilanguage Version of Windows XP Professional. The following sections describe these versions and how to configure multilanguage support.

Using Localized Windows XP

Microsoft provides localized editions of Windows XP Professional. For example, users in the United States will most likely use the English version, and users in Japan will most likely use the Japanese version. Localized versions of Windows XP Professional include fully localized user interfaces for the language that was selected. In addition, localized versions allow users to view, edit, and print documents in more than 60 different languages. However, localized versions do not support multilanguage user interfaces.

Using Windows XP Multilanguage Version

Windows XP Multilanguage Version provides user interfaces in several different languages. This version is useful in multinational corporations where users speak several languages and must share computers. It is also appropriate when administrators want to deploy a single version of Windows XP Professional worldwide. You can manage multiple users who share a single computer and speak different languages through user profiles or through group policies.

Two sets of files are necessary to support Windows XP Multilanguage Version:

- Language groups, which contain the fonts and files required to process and display the specific languages
- Windows XP Professional Multilanguage Version files, which contain the language content required by the user interface and help files

When you install Windows XP Multilanguage Version, you select the initial language that will be installed on the computer. For each language that you wish to use, you must also have the appropriate language group installed. For example, if you want to use the Japanese user interface, you must also install the Japanese language group. If you want to install other language support after installation, you can install and remove Windows XP Multilanguage Version files and language groups through Date, Time, Language and Regional Options in Control Panel. Each instance of Multilanguage Version files will use approximately 45MB of disk space. You can set the default user interface (UI) language, or add/remove UI languages through the `Muisetup.exe` file.

Windows XP Multilanguage Version is not available through retail stores. You order this version of Windows XP Professional through Microsoft Volume Licensing Programs. For more information about the Multilanguage Version, go to `www.microsoft.com/licensing`.

Enabling and Configuring Multilingual Support

On a localized version of Windows XP Professional, you enable and configure multilingual editing and viewing through Start ➢ Control Panel ➢ Date, Time, Language and Regional Options ➢ Regional Options. This allows access to the Regional and Language Options dialog box, shown in Figure 5.4.

FIGURE 5.4 The Regional and Language Options dialog box

Through Regional and Language Options you can configure Regional Options, Languages, and Advanced Settings. We will look at each of these in the following sections.

Configuring Local Settings

For localized Windows XP Professional as well as the Multilanguage Version, you can also configure locale settings for numbers, currency, time, and date formats, and for input locales (which allows you to select the input language you will use). Like multilingual support, these settings are made through the Regional Options dialog box. Simply select the locale (location) for the regional settings that you want to use from the drop-down list at the top of the dialog box in the Standards and format section.

In the list box at the bottom of the Regional Options dialog box under the Location section, check the language settings that you wish to support on the computer. After you click OK, you may be prompted to insert the Windows XP Professional CD to copy the distribution files required for multiple-language support. Then you will need to restart your computer for the new changes to take effect. After the restart, you will notice a new icon on the Taskbar that shows the current locale and keyboard inputs that are being used. You can switch to another supported language by clicking this icon and selecting the locale input you wish to use.

You should only install these options if you will use them. The option to install East Asian language support requires 230MB of disk space.

Configuring Languages

The Languages tab is used to provide supplemental language support. The options that can be configured include the following:

- Install Files for Complex Script and Right-to-Left Languages (Including Thai), which is used to support languages such as Arabic, Armenian, Georgian, Hebrew, Indic languages, Thai, and Vietnamese.
- Install Files for East Asian Languages, which is used to support Chinese, Japanese, and Korean languages.

Configuring Advanced Settings

The Advanced settings tab allows you to support languages for non-Unicode programs. This enables non-Unicode programs to display menus and dialog boxes in the users' native language (for example, East Asian languages support characters for Japanese, Chinese, and Korean languages).

The following steps are used to configure the locale settings on your computer:

1. Select Start ➢ Control Panel ➢ Date, Time, Language, and Regional Options ➢ Regional and Language Options. On the Regional Options tab, configure your current locale.
2. One by one, click the Regional Options, Languages, and Advanced tabs and note the configurations in each tab.
3. Click the Regional Options tab, and select the Danish locale (location) from the drop-down list at the top of the dialog box in the Standards and formats section. Then click the Apply button.
4. In the Number, Currency, Time, and Date fields, note the changed configurations.
5. Return to the General tab, reset your locale to the original configuration, and click the Apply button.

Configuring Windows XP Professional for Multiple Locations

In order to support multiple languages, you must use Windows XP Multilanguage Version. For each location, create a separate user profile and select the preferred UI and locale information. When you log on as a specific user, you see the linguistic and locale information that has been configured.

Exam Essentials

Know how to configure Windows XP for multiple languages. Be able to read and edit documents using multiple languages. Be able to add the support for non-Unicode characters.

Be able to set locale settings for different environments. Know what options can be configured for locale settings. Be able to change back and forth for different languages.

Know how to change the user interface (UI) to support different languages. Know what is required to change the UI to a different language. Be able to use the `Muisetup.exe` utility.

Manage Applications by Using Windows Installer Packages

With Windows XP, you can easily distribute new applications through Windows Installer packages, which are special application distribution files. To use Windows Installer packages, you must have a Windows Server 2003 or a Windows 2000 Server configured as a domain controller (so that Active Directory is running). You can distribute applications to users (for example, everyone in the accounting department) or to specific computers (for example, a Service Pack being distributed to all Windows XP Professional computers).

Critical Information

Windows Installer packages work with applications that are one of the following file types:

- Microsoft Installer (MSI) format files, which are usually provided by the software vendor. They support components such as on-demand installation of features as they are accessed by users.
- Repackaged applications (MSI files) that do not include the native Windows Installer packages. Repackaged applications are used to provide users with applications that can be cleanly installed, are easily deployed, and can perform self-diagnosis and repair.
- ZAP files, which are used if you do not have MSI files. ZAP files are used to install applications using their native Setup program. ZAP files are needed when the setup program requires an .INI file to install (usually for older programs).

If your application includes a modification tool, you can create customized application installations that include specific features of the application through the use of modification (`.mst`) files. These files can only be used during initial deployment of the package.

Windows Installer packages work as published applications or assigned applications. When you publish an application, users can choose to install the application through the Control Panel Add or Remove Programs icon, or can choose not to install it. When you assign an application to users or computers, the package is automatically installed when the user selects the application on the Start ➢ All Programs menu or via document invocation (by the document extension, which means if a user clicks on a file with a specified extension and does not have the associated application installed, it will be automatically installed for them).

The primary steps for using Windows Installer packages to distribute applications are as follows, and are discussed in the sections coming up:

1. Copy the MSI application to a network share.
2. Create a GPO) for the application.

3. Filter the GPO so only authorized users can access the application.
4. Add the package to the GPO.
5. If it is a published application, install it through the Control Panel Add or Remove Programs icon.

Copying the MSI Application to a Share

As noted earlier, Windows Installer works with MSI applications. Applications that use the MSI standard will include a file with an `.msi` extension on the application's distribution media. Create a network share that will be used to store the application, and copy the `.msi` file to the network share.

Creating a Group Policy Object

Your next step in preparing an application for distribution is to create a GPO on a Windows Sever 2003 domain controller. To create a GPO on a Windows Server 2003, take the following steps:

1. Select Start ➢ Administrative Tools ➢ Active Directory Users and Computers.
2. Right-click your domain name and select Properties from the pop-up menu. Click the Group Policy tab.
3. In the Group Policy tab (Figure 5.5), click the New button.
4. A new GPO will be created. Specify the new GPO name.

FIGURE 5.5 The Group Policy tab of the domain Properties dialog box

Filtering the Group Policy Object

After you've created the GPO, you must filter it so that only authorized users will be able to install the application. To filter a GPO on a Windows Server 2003, take the following steps:

1. In the Group Policy tab of the domain Properties dialog box, highlight the GPO you created and click the Properties button.
2. The GPO's Properties dialog box appears. Click the Security tab (see Figure 5.6) and set the appropriate permissions.
3. Click the OK button to close the GPO's Properties dialog box.

Adding the Package to the Group Policy Object

The next step in preparing to use a Windows Installer is to add the package (MSI) to the GPO you created for it. You can configure the package so that it is published or assigned to a user or a computer. Published applications are advertised through the Add/Remove Programs utility. Assigned applications are advertised through the Programs menu.

If you are configuring the package for a user, you add the package to the User Configuration\Software Settings\Software installation. If the package is for a computer, you add it to the Computer Configuration\Software Settings\Software installation. The following steps are used to add a package to a group policy:

1. In the Group Policy tab of the domain Properties dialog box, highlight the GPO and click the Edit button.

FIGURE 5.6 The Security tab of the GPO's Properties dialog box, with default settings

2. The Group Policy window appears, as shown in Figure 5.7. Expand User Configuration, then Software Settings.
3. Right-click Software Installation and select New ➢ Package. Specify the location of the software package and click the Open button.
4. The Deploy Software dialog box appears next, as shown in Figure 5.8. Here, you'll specify the deployment method. The options are Published, Assigned, and Advanced Published or Assigned. Make your selection and click the OK button.

Installing a Published Application

After the application (package) has been published, users who have permission to access the application can install it on a Windows XP Professional computer that is a part of the same domain that contains the application. The published application is available through the Add/Remove Programs icon in Control Panel. In the Add/Remove Programs utility, click the Add New Programs option, and you will see the published application listed in the dialog box. Select the application and click the Add button to install it.

In the event that the network connection fails during the installation, Windows Installer will automatically roll back the application and restart the installation when the network connection is restored.

FIGURE 5.7 The Group Policy window

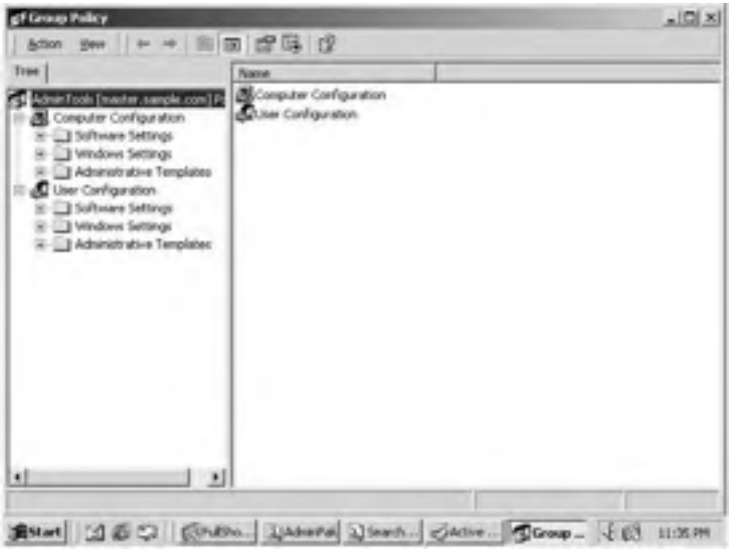
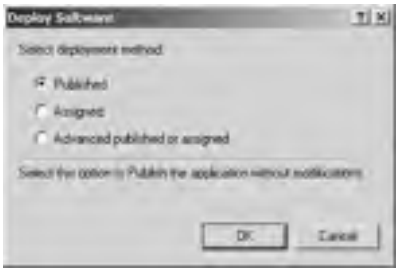


FIGURE 5.8 Specifying the deployment method



Exam Essentials

Be able to use Windows Installer packages to deploy applications. Know what types of files are used to deploy Windows Installer packages. Understand the difference between deploying applications to users or computers. Be able to use Active Directory to create deployment packages.

Review Questions

1. You want to deploy the XYZ application to users in the Sales and Accounting department. Each department needs the application deployed based on their specific configuration needs. What is the easiest way to automate the deployment of the applications?
   - **A.** Create an MSI file for both departments and a ZAP file with the customizations for each department.
   - **B.** Create an MST file for both departments and an MSI file with the customizations for each department.
   - **C.** Create an MSI file for both departments and an MST file with the customizations for each department.
   - **D.** Create a ZAP file for both departments and an MSI file with the customizations for each department.

2. You want to create a user profile for all of the sales users. Once the user profile is deployed, the users should not be able to make any changes to their profile. What should you configure?
   - **A.** Configure the `NTUSER.DAT` file as read only.
   - **B.** Configure the `\Documents` and `Settings\`*`username`* folder for each user with Read permissions.
   - **C.** Configure the registry setting for User Profiles to 1.
   - **D.** Rename the `NTUSER.DAT` file for each user to `NTUSER.MAN`.

3. You are using Windows Installer to install Microsoft Office on your laptop. During the installation, you disconnect your laptop from the network. You reconnect your laptop to the network. What is the next step you should take to get Microsoft Office installed on your laptop?
   - **A.** The installation will automatically restart when the network connection is restored.
   - **B.** Ask the administrator to re-create the package for deploying the application.
   - **C.** Refresh the GPO associated with the Installer package.
   - **D.** Ask the administrator to roll back the package for deploying the application.

4. You have a user who is fluent in English and Chinese. The user spends six months in New York and six months in Taiwan each year. When he switches between offices, he wants to configure Windows XP to use the local language for the Windows interface. The user's laptop is currently configured for a Chinese UI. He is currently in New York and wants the laptop reconfigured for English. What do you do?
   - **A.** Use Control Panel, Regional Options, Services tab to configure English as the user interface.
   - **B.** Use Control Panel, Regional Options, Advanced tab to select English services.
   - **C.** Set English as the preferred language through `Muisetup.exe`.
   - **D.** Reinstall Windows XP Professional using an English version.

5. You have two users who work different shifts and use the same Windows XP Professional computer. Both of the users are members of the Power Users group. You want to ensure that neither user can change options on the Start menu that could affect the other user. What should you configure?
   - **A.** Remove each individual user's write permission to the `\Documents and Settings\All Users` folder.
   - **B.** Configure the attribute on the `\Documents and Settings\All Users` folder to Read Only.
   - **C.** Delete the `\Documents and Settings\All Users` folder.
   - **D.** Copy the `\Documents and Settings\All Users` folder to a network server.

6. You have several sales users that frequently travel. When the users are in the office, they typically use the same computer, but sometimes they have to use different work spaces. You have configured roaming profiles for each sales user. Each user stores data in their home directory. When the users access their profile over the network, it takes a long time to load. What can you do to speed up this process?
   - **A.** Compress the files in the My Document folders.
   - **B.** Use DFS to host the My Documents folders.
   - **C.** Defragment the drives that host the My Documents folder on each computer.
   - **D.** Copy the users' My Documents folders to a network share.

7. You have a user who is fluent in Chinese and Japanese. Their Windows XP Professional computer is configured to use English. They need to install a Chinese application, but after the application is installed, the application interface does not display the Chinese characters properly. What should you do?
   - **A.** On the Advanced tab of Regional and Language options, install files for East Asian languages.
   - **B.** Apply the MUI Pack for Chinese to the computer.
   - **C.** In Control Panel, choose Services and add the Chinese language.
   - **D.** Add Chinese language support through Control Panel, Add Remove Programs, and specify Chinese language support.

8. You have just received a new laptop with Windows XP Professional installed on it. The Start menu shows several applications that were installed by the manufacturer. You want to leave these applications installed but you don't want the user who will be assigned the laptop to see the options from the Start menu. What should you do?
   - **A.** Access the Taskbar and choose Properties to edit what is displayed on the Start menu.
   - **B.** Select Control Panel, Start Menu Options.
   - **C.** Right-click My Computer, select Manage, then Start Menu Options.
   - **D.** Right-click My Computer, select Properties, then Start Menu Options.

9. What folder stores a user's local profile on a Windows XP Professional computer that was installed from scratch (not upgraded)?

   A. *systemdrive*:\Windows*UserName*

   B. *systemdrive*:\Documents and Settings*UserName*

   C. *systemdrive*:\Documents and Settings\Profiles*UserName*

   D. *systemdrive*:\Profiles*UserName*

10. You want to deploy an application using Windows Installer packages. Your application does not support Microsoft Installer format. You want to deploy the application using the native setup program. What kind of installer package should you create?

   A. ZAP

   B. MSI

   C. MST

   D. WIP

Answers to Review Questions

1. C. Microsoft Installer (MSI) format files are usually provided by the software vendor. They support components such as on-demand installation of features as they are accessed by users. If your application includes a modification tool, you can create customized application installations that include specific features of the application through the use of modification (`.mst`) files.

2. D. You can create mandatory profiles for a single user or a group of users. The mandatory profile is stored in a file named `NTUSER.MAN` (which is created by renaming the `NTUSER.DAT` file to `NTUSER.MAN`). A user with a mandatory profile can set different desktop preferences while logged on, but those settings will not be saved when the user logs off.

3. A. In the event that the network connection fails during the installation, Windows Installer will automatically roll back the application and restart the installation when the network connection is restored.

4. C. When you install Windows XP Multilanguage Version, you select the initial language that will be installed on the computer. For each language that you wish to use, you must also have the appropriate language group installed. You can set the default user interface (UI) language, or add/remove UI languages through the `Muisetup.exe` file.

5. A. Each user's unique settings are stored in the *`systemdrive`*`:\Documents and Settings\`*`UserName`* folder. Settings that are common to all users are stored in the *`systemdrive`*`:\Documents and Settings\All Users` folder. If multiple users share a computer, and you don't want any user to affect other users' settings, you should remove permissions for each individual user who accesses the computer from the *`systemdrive`*`:\Documents and Settings\All Users` folder.

6. D. If you are using roaming profiles, the contents of the user's profile folder will be copied to the local computer each time the roaming profile is accessed. If you have stored large files in any subfolders of your user profile folder, you may notice a significant delay when accessing your profile remotely as opposed to locally. If this problem occurs, you can reduce the amount of time the roaming profile takes to load by moving the subfolder to another location (for example, moving the user's My Documents folder to a network share) or you can use GPOs within the Active Directory to specify that specific folders should be excluded when the roaming profile is loaded.

7. A. The Advanced settings tab allows you to support languages for non-Unicode programs. This enables non-Unicode programs to display menus and dialog boxes in the users' native language (for example East Asian languages support characters for Japanese, Chinese, and Korean).

8. A. Users can customize the Taskbar and Start menu through the Taskbar and Start Menu Properties dialog box. The easiest way to access this dialog box is to right-click a blank area in the Taskbar and choose Properties from the pop-up menu.

9. B. The first time users log on, they receive a default user profile. A folder that matches the user's logon name is created for the user in the Documents and Settings folder. The user profile folder that is created holds a file called `NTUSER.DAT`, as well as subfolders that contain directory links to the user's desktop items. The default location of a local users profile is *`systemdrive`*`:\Documents and Settings\`*`UserName`*.

10. A. Microsoft Installer (MSI) format files are usually provided by the software vendor. They support components such as on-demand installation of features as they are accessed by users. Repackaged applications (MSI files) do not include the native Windows Installer packages. They are used to provide users with applications that can be cleanly installed, are easily deployed, and can perform self-diagnosis and repair. ZAP files are used if you do not have MSI files. These files are used to install applications using their native Setup program. If your application includes a modification tool, you can create customized application installations that include specific features of the application through the use of modification (`.mst`) files.

Chapter 6

Implementing, Managing, and Troubleshooting Network Protocols and Services

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configure and troubleshoot the TCP/IP protocol.**
- ✓ **Connect to computers by using dial-up networking.**
  - Connect to computers by using a virtual private network (VPN) connection.
  - Create a dial-up connection to connect to a remote access server.
  - Connect to the Internet by using dial-up networking.
  - Configure and troubleshoot Internet Connection Sharing (ICS)
- ✓ **Connect to resources by using Internet Explorer.**
- ✓ **Configure, manage, and implement Internet Information Services (IIS).**
- ✓ **Configure, manage, and troubleshoot Remote Desktop and Remote Assistance.**
- ✓ **Configure, manage, and troubleshoot an Internet Connection Firewall (ICF).**

In this chapter you will learn about configuring and troubleshooting the TCP/IP protocol, connecting computers through dial-up networking, using Internet Explorer, using Remote Desktop and Remote Assistance, and how to use the Internet Connection Firewall.

Configure and Troubleshoot the TCP/IP Protocol

In this section you will learn about IP addressing and configuration, the options for implementing TCP/IP, and additional IP configuration options which can be used for troubleshooting.

Critical Information

Before you can configure TCP/IP, you must have a basic understanding of TCP/IP configuration and addressing. To configure a TCP/IP client, you must specify an IP address and subnet mask. Depending on your network, optional settings might include the default gateway, DNS server settings, and WINS server settings.

In the following subsections, you will learn about these TCP/IP addressing and configuration options:

- IP address
- Subnet mask
- Default gateway
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS) servers
- Windows Internet Name Service (WINS) servers

IP Address

The *IP address* uniquely identifies your computer on the network. The IP address is a four-field, 32-bit address, separated by periods (an example would be 165.76.21.22). Part of the address is used to identify your network address, and part is used to identify the host (or local) computer's address.

If you use the Internet, then you should register your IP addresses with one of the Internet registration sites. There are three main classes of IP addresses. Depending on the class you use, different parts of the address show the network portion of the address and the host address.

Table 6.1 shows the three classes of network addresses and the number of networks and hosts that are available for each network class.

TABLE 6.1 IP Class Assignments

Network Class	Address Range of First Field	Number of Networks Available	Number of Host Nodes Supported
A	1–126	126	16,777,214
B	128–191	16,384	65,534
C	192–223	2,097,152	254

Subnet Mask

The *subnet mask* is used to specify which part of the IP address is the network address and which part of the address is the host address. By default, the following subnet masks are applied:

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

By using 255, you are selecting the octet or octets (or, in some cases, the piece of an octet) used to identify the network address. For example, in the Class B network address 191.200.2.1, if the subnet mask is 255.255.0.0, then 191.200 is the network address and 2.1 is the host address.

Default Gateway

You configure a *default gateway* if the network contains routers. A *router* is a device that connects two or more network segments together. You configure the computers on each segment to point to the IP address of the network card on the router that is attached to their network segment.

DHCP

Each device that will use TCP/IP on your network must have a valid, unique IP address. This address can be manually configured or can be automated through *Dynamic Host Configuration Protocol (DHCP)*. DHCP is implemented as a DHCP server and a DHCP client. The server is configured with a pool of IP addresses and their associated IP configurations. The client is configured to automatically access the DHCP server to obtain its IP configuration.

DHCP works in the following manner, all through the use of network broadcasts:

1. When the client computer starts up, it sends a broadcast DHCPDISCOVER message, requesting a DHCP server. The request includes the hardware address of the client computer.
2. Any DHCP server receiving the broadcast that has available IP addresses will send a DHCPOFFER message to the client. This message offers an IP address for a set period of time (called a lease), a subnet mask, and a server identifier (the IP address of the DHCP server). The address that is offered by the server is marked as unavailable and will not be offered to any other clients during the DHCP negotiation period.
3. The client selects one of the offers and broadcasts a DHCPREQUEST message, indicating its selection. This allows any DHCP offers that were not accepted to be returned to the pool of available IP addresses.
4. The DHCP server that was selected sends back a DHCPACK message as an acknowledgment, indicating the IP address, subnet mask, and duration of the lease that the client computer will use. It may also send additional configuration information, such as the address of the default gateway or the DNS server address.

If you want to use DHCP and there is no DHCP server on your network segment, you can use a DHCP server on another network segment—provided that the DHCP server is configured to support your network segment and a DHCP Relay Agent has been installed on your network router.

If you are not able to access a DHCP server installed on a Windows 2000 Server or Windows Server 2003 within Active Directory, make sure that the DHCP server has been authorized.

DNS Servers

Domain Name System (DNS) servers are used to resolve hostnames to IP addresses. This makes it easier for people to access domain hosts.

When you access the Internet and type in a URL, there are DNS servers within the infrastructure of the Internet that resolve the hostname to the proper IP address. If you did not have access to a properly configured DNS server, you could configure a `HOSTS` file for your computer that contains the mappings of IP addresses to the domain hosts that you need to access.

WINS Servers

Windows Internet Name Service (WINS) servers are used to resolve NetBIOS (Network Basic Input/Output System) names to IP addresses. Windows XP uses NetBIOS names in addition to hostnames to identify network computers. This is mainly for backward compatibility with Windows NT 4, which used this addressing scheme extensively. When you attempt to access a computer using the NetBIOS name, the computer must be able to resolve

the NetBIOS name to an IP address. This address resolution can be accomplished by using one of the following methods:

- Through a broadcast (if the computer you are trying to reach is on the same network segment)
- Through a WINS server
- Through an `LMHOSTS` file, which is a static mapping of IP addresses to NetBIOS computer names

Name resolution is covered in greater detail in the "Understanding TCP/IP Name Resolution" section of this chapter.

Using TCP/IP

Windows XP Professional offers four methods for configuring the TCP/IP protocol. You can use Dynamic Host Configuration Protocol (DHCP), Automatic Private IP Addressing (APIPA), Static IP Addressing, or Alternate IP Configuration. The following sections include a description of each option, as well as instructions for configuring each option.

Using DHCP

Dynamic IP configuration assumes that you have a DHCP server on your network. DHCP servers are configured to automatically provide DHCP clients with all their IP configuration information. For large networks, DHCP is the easiest and most reliable way of managing IP configurations. By default, when TCP/IP is installed on a Windows XP Professional computer, the computer is configured for dynamic IP configuration.

If your computer is configured for manual IP configuration and you want to use dynamic IP configuration, take the following steps:

1. Select Start ➢ Control Panel ➢ Network and Internet Connections.
2. From the Network and Internet Connections dialog box, click the Network Connections option. You will see your Local Area Connection as an icon.
3. Right-click Local Area Connection, and select Properties.
4. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click the Properties button.
5. The Internet Protocol (TCP/IP) Properties dialog box appears. Select the Obtain an IP Address Automatically radio button. Then click OK.

If your network adapter is a part of a network bridge, you will not be able to configure TCP/IP properties.

Using APIPA

Automatic Private IP Addressing (APIPA) is used to automatically assign private IP addresses for home or small business networks that contain a single subnet, have no DHCP server, and are not using static IP addressing. If APIPA is being used, then clients will only be able to communicate with other clients on the same subnet that are also using APIPA. The benefit of using APIPA in small networks is that it is less tedious and has less chance of configuration errors than statically assigning IP addresses and configuration.

APIPA is used with Windows XP Professional under the following conditions:

- The client is configured as a DHCP client, but no DHCP server is available to service the DHCP request.
- The client originally obtained a DHCP lease from a DHCP server, but when the client tried to renew the DHCP lease, the DHCP server was unavailable.

In the next sections you will learn how APIPA works, be able to determine if your computer is using APIPA, and learn how to disable APIPA.

HOW APIPA WORKS

By default, a range of Class B network addresses, 169.254.0.1–169.254.255.254, has been set aside as private Class B network addresses. Windows XP Professional uses this range of addresses to automatically assign IP addresses if APIPA is used.

The steps used by APIPA are as follows:

1. The client will select an address from the range of private Class B addresses that have been allocated, using the subnet mask of 255.255.0.0.
2. The client will use duplicate-address detection to verify that the address that was selected is not already in use.
3. If the address is already in use, the client will repeat steps 1 and 2, for a total of up to 10 retries. If the address is not already in use, the client will configure its interface with the address that was selected.
4. As a background process, the client will continue to search for a DHCP server every five minutes. If a DHCP server replies to the request, the APIPA configuration will be dropped and the client will receive new IP configuration settings from the DHCP server.

Using Static IP Addressing

You can manually configure IP if you know your IP address and subnet mask. If you are using optional components such as a default gateway or a DNS server, you need to know the IP addresses of the computers that host these services as well. This option is not typically used in large networks because it is time-consuming and prone to user errors.

The following steps are used to manually configure IP on a Windows XP computer:

1. Select Start ➢ Control Panel ➢ Network and Internet Connections.
2. From the Network and Internet Connections dialog box, click the Network Connections option. You will see your Local Area Connection as an icon.
3. Right-click Local Area Connection, and select Properties.

4. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click the Properties button.
5. The Internet Protocol (TCP/IP) Properties dialog box appears, as shown in Figure 6.1. Choose the Use the Following IP Address radio button.
6. In the appropriate text boxes, specify the IP address, subnet mask, and the default gateway option.
7. Click OK to save your settings and close the dialog box.

ADVANCED CONFIGURATION

Clicking the Advanced button in the Internet Protocol (TCP/IP) Properties dialog box opens the Advanced TCP/IP Settings dialog box, shown in Figure 6.2. In this dialog box, you can configure advanced DNS, WINS, and other Options settings. The other options that can be configured include the following:

- The IP address that will be used. You can add, edit, or remove IP addresses.
- The default gateways that will be used and the metric associated with each gateway. Metrics are used to calculate the path that should be used through a network.

ADVANCED DNS SETTINGS

You can configure additional DNS servers to be used for name resolution and other advanced DNS settings through the DNS tab of the Advanced TCP/IP Settings dialog box, shown in Figure 6.3. The options in this dialog box are described in Table 6.2.

FIGURE 6.1 Internet Protocol (TCP/IP) Properties dialog box

FIGURE 6.2 The Advanced TCP/IP Settings dialog box

FIGURE 6.3 The DNS tab of the Advanced TCP/IP Settings dialog box

TABLE 6.2 Advanced DNS TCP/IP Settings Options

Option	Description
DNS server addresses, in order of use	Specifies the DNS servers that are used to resolve DNS queries. Use the arrow buttons on the right side of the list box to move a server up or down in the list.
Append primary and connection-specific DNS suffixes	Specifies how unqualified domain names are resolved by DNS. For example, if your primary DNS suffix is `TestCorp.com` and you type **`ping computer1`**, DNS will try to resolve the address as `computer1.TestCorp.com`.
Append parent suffixes of the primary DNS suffix	Specifies whether name resolution includes the parent suffix for the primary domain DNS suffix, up to the second level of the domain name. For example, if your primary DNS suffix is `SanJose.TestCorp.com` and you type **`ping computer1`**, DNS will try to resolve the address as `computer1.SanJose.TestCorp.com`. If this doesn't work, DNS will try to resolve the address as `computer1.TestCorp.com`.
Append these DNS suffixes (in order)	Specifies the DNS suffixes that will be used to attempt to resolve unqualified name resolution. For example, if your primary DNS suffix is `TestCorp.com` and you type **`ping computer1`**, DNS will try to resolve the address as `computer1.TestCorp.com`. If you append the additional DNS suffix `MyCorp.com` and type **`ping computer1`**, DNS will try to resolve the address as `computer1.TestCorp.com` and `computer1.MyCorp.com`.
DNS suffix for this connection	Specifies the DNS suffix for the computer. If this value is configured by a DHCP server and you specify a DNS suffix, it will override the value set by DHCP.
Register this connection's addresses in DNS	Specifies that the connection will try to register its addresses dynamically using the computer name that was specified through the Network Identification tab of the System Properties dialog box (accessed through the System icon in Control Panel).
Use this connection's DNS suffix in DNS registration	Specifies that when the computer registers automatically with the DNS server, it should use the combination of the computer name and the DNS suffix.

ADVANCED WINS SETTINGS

You can configure advanced WINS options through the WINS tab of the Advanced TCP/IP Settings dialog box, shown in Figure 6.4. The options in this dialog box are described in Table 6.3.

FIGURE 6.4 The WINS tab of the Advanced TCP/IP Settings dialog box

TABLE 6.3 Advanced WINS TCP/IP Settings Options

Option	Description
WINS addresses, in order of use	Specifies the WINS servers that are used to resolve WINS queries. You can use the arrow buttons on the right side of the list box to move a server up or down in the list.
Enable LMHOSTS lookup	Specifies whether an `LMHOSTS` file can be used for name resolution. If you configure this option, you can use the Import LMHOSTS button to import an `LMHOSTS` file to the computer.
Use NetBIOS setting from the DHCP server	Specifies that the computer should obtain its NetBIOS-over-TCP/IP and WINS settings from the DHCP server.
Enable NetBIOS over TCP/IP	Allows you to use statically configured IP addresses so that the computer is able to communicate with pre–Windows XP computers.
Disable NetBIOS over TCP/IP	Allows you to disable NetBIOS over TCP/IP. Use this option only if your network includes only Windows XP clients or DNS-enabled clients.

OPTIONS

The Options tab, shown in Figure 6.5, allows you to configure TCP/IP filtering options. By clicking the Properties button, you access the TCP/IP Filtering dialog box shown in Figure 6.6.

Through TCP/IP filtering, you can specify the following:

- Which TCP ports are permitted for your computer
- Which UDP ports are permitted for your computer
- Which IP protocols are permitted for your computer

FIGURE 6.5 The Options tab of the Advanced TCP/IP Settings dialog box

FIGURE 6.6 The TCP/IP Filtering dialog box

Using Alternate IP Configuration

Windows XP Professional includes a new feature called Alternate IP Configuration. This feature is designed to be used by laptops and other mobile computers to manage IP configurations when the computer is used in multiple locations and one location requires a static IP address and the other location(s) require dynamic IP addressing. For example, a user with a laptop might need a static IP address to connect to their broadband ISP at home and then use DHCP when connected to the corporate network.

Alternate IP Configuration works by allowing the user to configure the computer so that it will initially try to connect to a network using DHCP; if the DHCP attempt fails (for example, when the user is at home), the alternate static IP configuration is used. The alternate static IP address can be an automatic private IP address (which would use APIPA) or a specifically configured IP address.

To configure Alternate IP Configuration, you would take the following steps:

1. Select Start ➢ Control Panel ➢ Network and Internet Connections.
2. From the Network and Internet Connections dialog box, click the Network Connection option. You will see your Local Area Connection as an icon.
3. Right-click Local Area Connection, and select Properties.
4. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click the Properties button.
5. The Internet Protocol (TCP/IP) Properties dialog box appears. From the General tab, verify that the Obtain an IP Address Automatically radio button is selected. Click the Alternate Configuration tab.
6. If you want to use APIPA to assign the alternate address, select the Automatic Private IP Address option. If you want to manually configure a static address, select the User Configured option. You would then need to supply the IP address, the subnet mask, and, if needed, the default gateway, preferred and alternate DNS servers, and preferred and alternate WINS servers. Finally, click the OK button.

Additional TCP/IP Features and Options

The TCP/IP protocol is complex and offers many features. In addition to having a basic understanding of the TCP/IP protocol and being able to configure and manage basic IP configurations on a Windows XP Professional computer, you should be aware of some other key features and options of TCP/IP. The TCP/IP features and options that will be covered in greater detail in the following subsections include the following:

- Understanding TCP/IP name resolution
- Using multiple IP addresses
- Testing and verifying TCP/IP connectivity

Understanding TCP/IP Name Resolution

When users try to access a network resource, it is unusual for them to access the resource via an IP address. In Windows environments, users typically access resources using a hostname or a NetBIOS name. The methods used to manage TCP/IP name resolution are:

- DNS
- NetBIOS over TCP/IP (NBT)
- WINS
- `HOSTS` or `LMHOSTS` files
- Subnet broadcasts

DNS is a global, distributed database that is based on a hierarchical naming system. DNS name resolution is used to name DNS-based names (friendly usernames such as `Sybex.com`) to IP addresses and vice versa. Windows 2000 and Windows 2003 domains inherently use DNS services, and DNS is the default name resolution method used.

Microsoft clients that are using Windows 9*x*, Windows Me, or other early implementations of Windows operating systems rely on NetBIOS names to identify computers on the network. Windows 2000 Server and Windows Server 2003 use a service called Windows Internet Name Service (WINS) for compatibility with applications and services that use NetBIOS services to map the NetBIOS name to an IP address.

`HOSTS` and `LMHOSTS` files are local files that must be maintained manually, to provide hostname-to-IP address resolution. This is not a common method of resolving IP addresses, as it is administrator intensive and prone to configuration errors.

If no name resolution method is configured for NetBIOS, the final way that address resolution is attempted is through the use of subnet broadcasts. You typically want to avoid these broadcasts since they are directed to all computers on the subnet as opposed to being sent only to the specified computer as a unicast transmission.

Using Multiple IP Addresses

Windows XP Professional allows you to configure more than one network adapter in a single computer, which is referred to as multihoming. Windows XP Professional also supports logical multihoming, which is when multiple IP addresses are configured for a single network adapter. You would use logical multihoming if you had a single physical network that was logically divided into subnets and you wanted your computer to logically be associated with more than one subnet.

To configure multiple IP addresses for a single network adapter, you would take the following steps:

1. Select Start ➢ Control Panel ➢ Network and Internet Connections.
2. From the Network and Internet Connections dialog box, click the Network Connections option. You will see your Local Area Connection as an icon.
3. Right-click Local Area Connection and select Properties.

4. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click the Properties button.
5. From the Internet Protocol (TCP/IP) Properties dialog box, verify that Use the Following IP Address is selected and configured for the first configuration you want to use.
6. From the Internet Protocol (TCP/IP) Properties dialog box, click the Advanced button to access the Advanced TCP/IP Settings dialog box. From the IP Settings tab, under IP Addresses, click the Add button. You will then be able to assign multiple IP addresses and subnet mask settings. Click the Add button again to add any additional addresses.
7. If you need to assign more than one default gateway to your IP configuration, use the Default Gateways section of Advanced IP Settings.

Testing IP Configuration

After you have installed and configured the TCP/IP settings, you can test the IP configuration using the `IPCONFIG`, `PING`, and `NBTSTAT` command-line utilities. These commands are also very useful in troubleshooting IP configuration errors. You can also graphically view connection details through Local Area Connection Status. Each command is covered in detail in the following subsections.

THE *IPCONFIG* COMMAND

The *IPCONFIG* command displays your IP configuration. Table 6.4 lists the command switches that can be used with the `IPCONFIG` command.

TABLE 6.4 **IPCONFIG** Switches

Switch	Description
`/?`	Shows all of the help options for `IPCONFIG`
`/all`	Shows verbose information about your IP configuration, including your computer's physical address, the DNS server you are using, and whether you are using DHCP
`/release`	Releases an address that has been assigned through DHCP
`/renew`	Renews an address through DHCP
`/flushdns`	Purges the DNS Resolver cache
`/registerdns`	Shows the contents of the DNS Resolver cache
`/showclassid`	Lists the DHCP class IDs allowed by the computer
`/setclassID`	Allows you to modify the DHCP class ID

THE *PING* COMMAND

The *PING* command is used to send an ICMP (Internet Control Message Protocol) echo request and echo reply to verify whether the remote computer is available. You can `PING` a computer based on the computer's IP address or the DNS name. If you were using an IP address, the `PING` command has the following syntax:

```
PING IP address
```

For example, if your IP address is 131.200.2.30, you would type the following command:

```
PING 131.200.2.30
```

If you were using a DNS name, the `PING` command has the following syntax:

```
PING DNS name
```

For example, if your DNS name was `Example.Sybex.com`, you would type the following command:

```
PING Example.Sybex.com
```

`PING` is useful for verifying connectivity between two hosts. For example, if you were having trouble connecting to a host on another network, `PING` would help you verify that a valid communication path existed. You would ping the following addresses:

- The loopback address, 127.0.0.1
- The local computer's IP address (you can verify this with `IPCONFIG`)
- The local router's (default gateway's) IP address
- The remote computer's IP address

If `PING` failed to get a reply from any of these addresses, you would have a starting point for troubleshooting the connection error. The error messages that can be returned from a `PING` request include the following:

- **TTL Expired in Transit**, which means that the packet exceeded the number of hops specified to reach the destination host computer. Each time a packet passes through a router, the Time To Live (TTL) counter reflects the pass through the router as a hop. You can use the `ping -i` parameter to increase TTL. This error can also be due to a routing configuration error, which has resulted in a routing loop. The `tracert` command can be used to identify routing loops.
- **Destination Host Unreachable**, which is generated when a local or remote route path does not exist between the sending host and the specified destination computer. This error could occur because the router is misconfigured or the target computer is not available.
- **Request Timed Out**, which means that the echo reply message was not received from the destination computer within the time allotted. By default, destination computers have four seconds to respond. You can increase the timeout value with the `ping -w` parameter.

- **Ping Request Could Not Find Host**, which indicates that the destination hostname couldn't be resolved. Verify that the destination hostname was properly specified, that all DNS and WINS settings are correct, and that the DNS and WINS servers are available.

THE *NBTSTAT* COMMAND

NBT is NetBIOS over TCP/IP, and the `NBTSTAT` command is used to display TCP/IP connection protocol statistics over NBT. Table 6.5 lists the command-line options that can be used.

TABLE 6.5 **NBTSTAT** Command-Line Options

Switch	Option	Description
`/?`	Help	Shows all of the help options for `NBTSTAT`
`-a`	Adapter Status	Shows adapter status and lists the remote computer's name, based on the hostname you specify
`-A`	Adapter Status	Shows adapter status and lists the remote computer's name, based on the IP address you specify
`-c`	Cache	Displays the NBT's cache of remote computers through their names and IP addresses
`-n`	Names	Shows a list of the local computer's NetBIOS names
`-r`	Resolved	Shows a list of computer names that have been resolved either through broadcast or WINS
`-R`	Reload	Causes the remote cache name table to be purged and reloaded
`-S`	Sessions	Shows the current sessions table with the destination IP addresses
`-s`	Sessions	Shows the current sessions table and the converted destination IP address to the computer's NetBIOS name
`-RR`	ReleaseRefresh	Sends a Name Release packet to the WINS server, then starts a refresh

LOCAL AREA CONNECTION STATUS

To use a graphical interface to access local area connection status, you access the main windows of Network Connections (from Control Panel ➢ Network and Internet Connections), then right-click Local Area Connection and select Status.

From the Local Area Connection Status dialog box, shown in Figure 6.7, you can view connection information including status, duration, and the speed at which you connected. You can

also see the activity that has been generated for the current session through all packets that have been sent and received through the network adapter.

If you click the Support tab on the Local Area Connection dialog box, you will see the support status, as shown in Figure 6.8. This will display the general configuration for your connection.

Exam Essentials

Know how to configure IP. Be able to configure IP with static addresses or with DHCP. Understand how automatic configuration works.

Know the command-line utilities that can be used to configure and troubleshoot IP. Be familiar with the `IPCONFIG`, `PING`, and `NBTSTAT` command-line utilities. Know the options associated with each.

FIGURE 6.7 The Local Area Connection Status dialog box

FIGURE 6.8 The Support tab of the Local Area Connection Status dialog box

Connect to Computers by Using Dial-Up Networking

In this section, you will learn how to connect computers by using dial-up networking. You can connect computers in a variety of ways: through the Internet, through dial-up networking, through virtual private networks (VPNs), or through direct connections.

Critical Information

The New Connection Wizard is used to guide you through the process of implementing all of the remote connections that can be used with Windows XP Professional. You access the New Connection Wizard through Start ➢ Control Panel ➢ Network and Internet Connections ➢ Network Connections. In the Network Connections dialog box, under Network Tasks, click Create a New Connection. The New Connection Wizard will start. From the Welcome screen, click the Next button to continue, and you will see the Network Connection Type dialog box, as shown in Figure 6.9.

The options that can be configured through the Network Connection Wizard include the following:

- Internet connections
- Dial-up connections to private networks
- VPN connections to private networks
- Networks for small office or home networks
- Direct connections to other computers through serial, parallel, or infrared connections

FIGURE 6.9 The Network Connection Type dialog box

Connecting to Computers by Using a Virtual Private Network (VPN) Connection

A VPN is a private network that uses links across private or public networks (such as the Internet). When data is sent over the remote link, it is encapsulated and encrypted and requires authentication services. You must use Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP) to support a VPN connection, both of which are automatically installed on Windows XP Professional computers. To have a VPN, you must also have a Windows 2000 Server or a Windows Server 2003 computer that has been configured as a VPN server.

The main advantage of using a VPN rather than a Remote Access Server (RAS) connection is that with a RAS connection, a long-distance call might be required to dial into the RAS server. With a VPN connection, all you need is access to a network such as the Internet.

Creating a RAS Connection

To configure a RAS client, take the following steps:

1. Select Start ➢ Control Panel ➢ Network and Internet Connections, then select the option Create a Connection to the Network at Your Workplace.
2. The Network Connection dialog box appears. Select the Dial-Up Connection option and click the Next button.
3. The Connection Name dialog box will appear. Type in the name that you want to use for the connection, which will be the descriptive name that will be used when you access the connection, and click the Next button.
4. Next up is the Phone Number to Dial dialog box. Enter the telephone number you wish to dial. If the telephone number is in a different country, enter the associated country code in the Country/Region Code field (for example, the Czech Republic's country code is 420 when you are calling internationally). After you enter the information, click Next.
5. The Completing the New Connection Wizard dialog box will appear. By default, the connection will be saved in the Network Connections folder. From the Completing the New Connection Wizard, you can also specify that a shortcut will be added for the connection on the desktop. Verify the new connection information, and click the Finish button. The Connect Dialup dialog box will automatically launch.
6. If you have access to a RAS server, you would connect to it through Control Panel ➢ Network and Internet Connections, and then select Network Connections.
7. The RAS connection will be listed under Dial-Up, as shown in Figure 6.10.
8. The Connect dialog box will appear as shown in Figure 6.11. Type in your username and password. You can also specify whether the username and password will be saved on the computer for you only or for anyone who uses the computer. Select the number you want to dial (if multiple options have been configured—for example, if the RAS server has five incoming lines)—and click the Dial button.

FIGURE 6.10 Network Connections dialog box

FIGURE 6.11 RAS Connect dialog box

Managing the Properties of a RAS Connection

The Connection Properties dialog box has five tabs: General, Options, Security, Networking, and Advanced. The options on these tabs are covered in the following sections.

Configuring General RAS Connection Properties

The General tab includes options for configuring the connection you will use and the telephone number you are dialing. You can also specify whether an icon will be displayed on the Taskbar when a connection is in use.

Within the General tab, the Phone Number section has text boxes for the area code and telephone number of the connection. To specify alternate telephone numbers to make a connection, if a RAS server has multiple phone lines that are supported, click the Alternates button. If you choose to use dialing rules, you can click the Dialing Rules button, which brings up the Dialing Rules dialog box. To modify dialing rules for an existing location, you select the location and click the Edit button. The Edit Location dialog box allows you to configure General, Area Code Rules, or Calling Card information for the location. Examples of general properties include specifying a number that must be dialed before accessing an outside line or the number that must be specified for dialing a long distance number. Area code rules specify how numbers will be dialed based on the area code you are dialing from. Calling card is used to specify dialing rules if you access the remote connection using a calling card.

The options for Area Code and Country/Region Code are grayed out unless you have checked the Use Dialing Rules check box on the General tab of the Connection Properties dialog box.

Configuring RAS Connection Options

The Options tab, shown in Figure 6.12, contains dialing options and redialing options. You can configure the following options for dialing:

- The Display Progress while Connecting option displays the progress of the connection attempt.
- The Prompt for Name and Password, Certificate, Etc. option specifies that before a connection is attempted, the user will be prompted for a username, password, or (if *smart card* authentication is being used) a certificate.

Smart cards are hardware devices used to provide additional security. They store public and private keys, passwords, and other personal information securely.

- The Include Windows Logon Domain option works in conjunction with the Prompt for Name and Password, Certificate, Etc. option. This option specifies that Windows logon-domain information should be requested prior to initiating a connection.
- The Prompt for Phone Number option allows the telephone number to be viewed, selected, or modified prior to initiating a connection.

The options for redialing let you specify the number of redial attempts if the connection is not established, and the time between the redial attempts. You can also designate how long a connection will remain idle before the computer hangs up. If you want the computer to redial the connection number should the connection be dropped, check the Redial if Line Is Dropped check box.

The X.25 button at the bottom of this dialog box can be used to configure an X.25 connection. This requires you to know which X.25 provider you are using and the X.121 address of the remote server to which you wish to connect.

Configuring RAS Connection Security

Security settings are among the most important options to be configured for dial-up connections. You can set typical or advanced (custom settings) security options in the Security tab of the Connection Properties dialog box, as shown in Figure 6.13. This tab also has options for interactive logon and scripting.

FIGURE 6.12 The Options tab of the Connection Properties dialog box

FIGURE 6.13 The Security tab of the Connection Properties dialog box

Connections that are more secure require more overhead and are usually slower. Less-secure connections require less overhead and are typically faster.

TYPICAL SECURITY SETTINGS

You generally will configure typical security settings unless you need to use specific security protocols. When you select the Typical radio button, you can then choose to validate the user's identity, to automatically use the Windows logon name and password (and domain, if specified), and whether data encryption is required. For validating the user's identity, you can select from the following options:

Allow Unsecured Password Specifies that the password can be transmitted without any encryption.

Require Secured Password Specifies that the password must be encrypted prior to transmission.

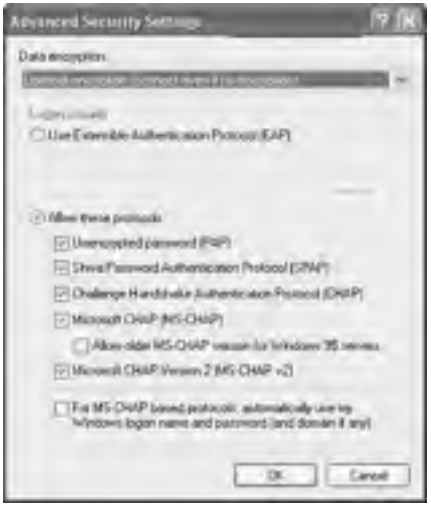
Use Smart Card Specifies that you must use a smart card.

The options for configuring Automatically Use My Windows Logon Name and Password (and Domain if Any) and Require Data Encryption (Disconnect if None) are enabled based on the validation method you select and whether the options are supported by the selected validation option.

ADVANCED SECURITY SETTINGS

If you need to configure specific security protocols, select the Advanced (Custom Settings) radio button in the Security tab and then click the Settings button. This brings up the Advanced Security Settings dialog box, as shown in Figure 6.14.

FIGURE 6.14 Connection Properties, Security tab, Advanced Settings dialog box



This dialog box allows you to configure the type of data encryption that will be employed. You also specify whether logon security will use the Extensible Authentication Protocol (EAP), which is used in conjunction with other security devices, including smart cards and certificates. You can select from the following protocols for logon security:

- Password Authentication Prococol (PAP) Unencrypted Password
- Shiva Password Authentication Protocol (SPAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP (MS-CHAP), if you select this option, you can also specify that you want to support older MS-CHAP for Windows 95 servers
- Microsoft CHAP Version 2 (MS-CHAPv2)

If you are using MS-CHAP-based protocols, you can also specify that you want to automatically use your Windows logon name and password (and domain, if any).

INTERACTIVE LOGON AND SCRIPTING

The Interactive Logon and Scripting options on the Security tab are provided for users who use terminal services for remote access. These options allow you to display a terminal window after dialing, and run a script after dialing.

Configuring Networking Options for RAS Connections

The Networking tab, shown in Figure 6.15, contains networking options for the dial-up connection. You can configure the wide area network (WAN) protocol you will use and the network components that will be employed by the network connection.

FIGURE 6.15 The Networking tab of the Connection Properties dialog box

Your choices for the WAN protocol are the *Point-to-Point Protocol (PPP)* or *Serial Line Internet Protocol (SLIP)*. PPP offers more features and is the WAN protocol used by Windows 9*x*, Windows NT (all versions), Windows 2000 (all versions), Windows XP, Windows Server 2003, and most Internet servers. SLIP is an older protocol that is used with some Unix servers. If you click the Settings button for PPP, you can configure options for Enable LCP Extensions, Enable Software Compression, and Negotiate Multi-link for Single Link Connections. You typically leave PPP settings at default values.

The network components used by the connection might include the protocols (such as Internet Protocol (IP) and NWLink IPX/SPX/NetBIOS Compatible Transport Protocol) and the client software (such as File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks). By clicking the Install button, you can install additional connections. The Properties button allows you to configure the properties of whatever connection you have highlighted.

Configuring Advanced Options

The Advanced tab, shown in Figure 6.16, is used to configure an Internet Connection Firewall and Internet Connection Sharing. The Internet Connection Firewall is used to limit access to your computer through the Internet and is implemented as a security feature. Internet Connection Sharing is used to allow more than one Internet connection through a single computer.

Troubleshooting Remote Access Connections

If your remote access connection is not working properly, there are many possible causes. The following list categorizes common problems and the options that can be used to troubleshoot, identify, and resolve configuration errors:

FIGURE 6.16 The Advanced tab of the Connection Properties dialog box

If you suspect the problem is with your modem

- Verify that the modem you are using is on the Hardware Compatibility List (HCL) and that you have the most current driver.
- If you are using an external modem, verify that it is turned on and connected to the proper port and that the modem cable is not defective. If you require a 9-to-25-pin serial connector, do not use one that came with a mouse, as most are not manufactured to support modem signals.
- Use modem logging and modem diagnostics to test the modem.

If you suspect the problem is with your access line

- If you are using an unknown line type (for example, in a hotel), verify the line type you are using. Analog modems only use analog phone lines, and digital modems only use digital lines. The remote client and the server that is being accessed must also use a common access method, analog or digital.
- Verify that you dialed the correct number for the remote server. If you need to dial an external line-access number (usually 9), verify that it is properly configured.
- If the modem is having problems connecting, there may be excessive static on the phone line that is preventing the modem from connecting at the configured speed. Attempt to connect using lower speed and call the phone company to have the quality of the line checked.

If you suspect the problem is with the RAS server

- Verify that you are using a valid user account and password. Make sure the user account has been granted remote access permission on the RAS server.
- Make sure the RAS server is properly configured and is running. If no remote clients can connect, the problem is most likely the RAS server. If other remote clients can connect, the RAS server is most likely properly configured.

If connections to the RAS server are being dropped

- Verify that the connection is not being dropped due to inactivity. Check with the RAS server administrator to find out what the inactivity settings are.
- If your phone line uses call waiting, an incoming call may be disrupting your connection; verify that call waiting has been disabled.

Connecting to the Internet by Using Dial-Up Networking

The most common option for remote access to the Internet is through a valid *Internet service provider (ISP)*. There are many ISPs to choose from, and they usually supply software to facilitate your Internet connection through their service. If you do not have software from your ISP, you can set up an Internet connection the first time you access Internet Explorer or through New Connection Wizard. Common options for accessing the Internet include analog modem and phone line, ISDN adapter and ISDN phone line, cable modem, and DSL.

Configuring and Troubleshooting Internet Connection Sharing (ICS)

Internet Connection Sharing (ICS) allows you to connect a small network (typically a home network) to the Internet through a single connection. The computer that provides ICS services is usually the one with the fastest outgoing connection—for example, the one using DSL.

The ICS host computer must have two connections. One of the connections is used to connect the computer to the local area network (LAN). The second connection—for example, a modem, ISDN adapter, DSL, or cable modem—is used to connect the computer to the Internet.

The ICS computer that accesses the Internet provides network address translation, IP addressing, and DNS name resolution services for all the computers on the network. Through Internet connection sharing, the other computers on the network can use Internet applications such as Internet Explorer and Outlook Express, as well as access Internet resources.

There are three main steps for using ICS:

1. The ICS host computer is configured to access the Internet through whatever connection method is appropriate (dial-up, cable modem, ISDN, etc.).
2. The ICS host computer has ICS enabled.
3. The client computers that will access the Internet through the ICS connection must be configured to use dynamic IP addressing.

When you enable ICS on a host computer, the following configuration changes will occur:

- When Internet connection sharing is enabled, the Internet host computer's address becomes 192.168.0.1 with a subnet mask of 255.255.255.0. The host also becomes the DHCP allocator, which acts as a "baby" DHCP server.
- All of the network clients must get their IP addresses automatically through the DHCP allocator, which gives out addresses randomly to the clients, in the range 192.168.0.2 through 192.168.0.254 with a subnet mask of 255.255.255.0.
- The autodial feature is enabled on the ICS host computer.
- DNS Proxy is enabled on the ICS host computer.

Configuring Internet Connection Sharing on the Host Computer

The computer that will act as the host computer for Internet connection sharing must be configured to support this option. Following are the options that can be configured:

Whether Internet connection sharing is enabled If it is, watch out—local network access may be momentarily disrupted because the IP address will automatically be reassigned to the computers that use Internet connection sharing.

Whether on-demand dialing is enabled When it is, if you do not have a permanent connection on the computer that hosts Internet connection sharing, the host computer will automatically dial out whenever a client tries to access the Internet. Enabling Internet Connection Sharing automatically enables on-demand dialing.

Which applications and services can be used through the shared connection For example, you could specify that only FTP requests on port 21, Telnet requests on port 23, and HTTP requests on port 80 can be passed through the shared Internet connection.

To configure Internet connection sharing on the host computer, take the following steps:

1. Create an Internet connection or a VPN connection.
2. Verify that the host computer is configured as a DHCP client and that each client (Internet Sharing) computer is also configured as a DHCP client. If the host has a static address, it will be changed to 192.168.0.1 automatically.
3. Select Start ➢ Control Panel ➢ Network and Internet Connections, then select Network Connections.
4. Right-click the connection you want to share, and select Properties from the pop-up menu.
5. The Properties dialog box for the selected connection appears. Click the Advanced tab and under Internet Connection Sharing, check the option for Allow Other Network Users to Connect through This Computer's Internet Connection.

   Enabling Internet Connection Sharing automatically enables on-demand dialing. When on-demand dialing is enabled, if the Internet connection is not active and another computer tries to access Internet resources, a connection will be automatically established.
6. Click the Settings button to access the Advanced Settings dialog box. This dialog box allows you to specify which applications and services can be serviced through the shared Internet connection. If you leave the blank default settings as is, then all applications and services are supported. However, you may want to limit access to one application—for example, HTTP. If so, you could configure HTTP requests to only be serviced by limited access to HTTP on port 80 (which is the default port that is used by HTTP requests). When you are done, click the OK button twice to close both open dialog boxes.

Configuring Internet Connection Sharing on the Network Computers

To configure Internet connection sharing on the network computers, take the following steps:

1. Right-click the Internet Explorer icon on the Desktop and select Properties from the pop-up menu.
2. In the Internet Properties dialog box, click the Connections tab and click the Never Dial a Connection option.
3. Click the LAN Settings button, and in Automatic Configuration, clear the Automatically Detect Settings and Use Automatic Configuration Script boxes. In Proxy Server, clear the Use a Proxy Server check box.

Do not configure Internet connection sharing on corporate networks with domain controllers, DNS servers, WINS servers, DHCP servers, routers, or other computers that use static IP addresses. When Internet connection sharing is configured, it causes computers that use the shared Internet connection to lose their IP configuration and generates a new IP configuration. Normal network connections then have to be reset manually to access local network resources.

Exam Essentials

Be able to configure dial-up networking. Know how to configure dial-up networking and manage security on dial-up networking. Be able to troubleshoot connectivity problems.

Know ho to configure and use Internet Connection Sharing. Be able to set up Internet Connection Sharing. Be aware of the special configuration required for manual IP configuration.

Connect to Resources by Using Internet Explorer

Internet Explorer (IE) is a web browser used to search and view information on the World Wide Web (WWW) via the Internet, or information that is stored on local intranets. You can access resources by typing in the address of the web page you wish to access or by selecting an address from your Favorites list. In this section, you will learn about accessing resources through IE and how to configure IE.

When you access a resource through IE, you use a Uniform Resource Locator (URL) address. A URL address is typically composed of four parts—for example: `http://www.sybex.com`.

- The first part of the address is the protocol that is being used. Examples of protocols include HTTP and FTP.
- The second part of the address is the location of the site—for example, the World Wide Web (`www`).
- The third part of the address is who maintains the site—for example, Sybex.
- The fourth part of the address identifies the kind of organization. Examples of defined suffixes include `.com`, `.gov`, `.org`, and `.edu`.

Critical Information

HTTP is the main protocol for making WWW requests. HTTP defines how messages are formatted and transmitted and the actions that will be executed by web servers and browsers based on the requests you make. The main standard that is used with HTTP is Hypertext Markup Language (HTML), which defines how web pages are formatted and displayed.

If the web server you are trying to access is using Secure Sockets Layer (SSL) services, then instead of using `http://` requests, you use secure HTTP—in other words, your request uses `https://` instead.

FTP is mainly used to transfer files between computers on the Internet. Access to FTP servers is based on permissions that have been set on the FTP server you are trying to access. Access can be granted to anonymous users or users can be required to have a valid username and password.

Once you access a FTP site, you can

- Work with files and folders in the same manner that would be used on a local computer
- View, download, upload, rename, and delete files and folders (based on your permissions)

When you use FTP for file transfer with IE, the syntax looks different than a typical HTTP request. FTP requests are made through the address bar on IE. For example, if you were trying to access Microsoft's FTP site, you would type

```
ftp://ftp.microsoft.com
```

If the FTP site required user and password authentication services, you could use the File menu and select the Login As option.

If you need to provide logon credentials as a part of the FTP request, then the syntax you would use would be

```
ftp://username:password@ftp.microsoft.com
```

Exam Essentials

Know how to use Internet Explorer to access web resources. Know what options can be used with Internet Explorer. Be able to access secure websites.

Configure, Manage, and Implement Internet Information Services (IIS)

Windows XP Professional comes with *Internet Information Services (IIS)*, which allows you to create and manage websites. This software provides a wide range of options for configuring the content, performance, and access controls for your websites. IIS can be used to publish resources on the Internet or a private intranet.

The IIS software that is included with Windows XP Professional is designed for small-scale use, mainly for users who are developing web services for home or office use. IIS Professional version can support only 10 incoming client connections. IIS Professional version also does not support all of the features of IIS that are included with the server versions of IIS. In previous versions of Windows client operating systems, the scaled-down version of IIS was called Peer Web Services (PWS). Windows XP Professional does not ship with PWS, and if you upgraded to Windows XP Professional, then PWS can't be upgraded. The IIS Professional version software is included with Windows XP Professional but is not installed by default.

In this section, you will learn how to install IIS and how to configure and manage website properties. The final section includes tips for troubleshooting problems with website access.

IIS is not included with Windows XP Home Edition.

Critical Information

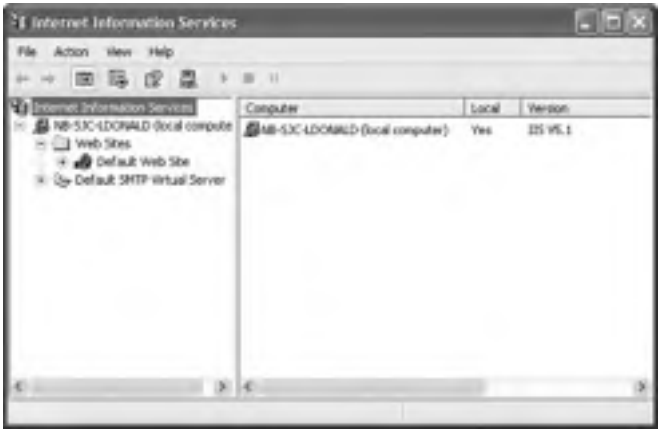
IIS is installed on a Windows XP computer through the Add or Remove Programs option in Control Panel. Before you can install IIS, your computer must have TCP/IP installed and configured. To install IIS on a Windows XP Professional computer, you take the following steps:

1. Select Start ➢ Control Panel ➢ Add or Remove Programs.
2. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.
3. In the Windows Components dialog box, check the Internet Information Services box and click the Next button.
4. Configuration changes will be made to your computer and files will be copied. You may be prompted to provide the Windows XP Professional CD.
5. The Completing the Windows Components Wizard dialog box will appear. Click the Finish button.

Using IIS

To access Internet Information Services, select Start ➢ Administrative Tools ➢ Internet Information Services. When you start Internet Information Services, you will see that items are defined by default for Web Sites and Default SMTP Virtual Server, as shown in Figure 6.17.

FIGURE 6.17 Internet Information Services dialog box



Through Internet Information Services, you can configure many options for your website, such as website identification and connection settings, performance settings, and access controls. To access a website's properties, right-click the website you want to manage in the Internet Information Services window and select Properties from the pop-up menu. This brings up the website Properties dialog box, as shown in Figure 6.18.

The website Properties dialog box has eight tabs with options for configuring and managing your website. The options on these tabs are described briefly in Table 6.6 and in more detail in the following sections.

TABLE 6.6 The Website Properties Dialog Box Tabs

Tab	Description
Web Site	Allows you to configure website identification, connections, and logging
ISAPI Filters	Allows you to set ISAPI (Internet Server Application Programming Interface) filters
Home Directory	Allows you to configure the content location, access permissions, content control, and application settings
Documents	Allows you to specify the default document that users will see if they access your website without specifying a specific document
Directory Security	Allows you to configure anonymous access and authentication control, IP address and domain name restrictions, and secure communications
HTTP Headers	Allows you to configure values that will be returned to web browsers in the HTML headers of the web pages
Custom Errors	Allows you to present a customized error message that will appear when there is a web browser error
Server Extensions	Allows you to configure publishing controls for FrontPage options

Setting Website Properties

The Web Site tab (see Figure 6.18) includes options for identifying the website, controlling connections, and enabling logging.

WEBSITE IDENTIFICATION

The description of the website appears in the Internet Information Services window. By default, the website description is the same as the name of the website. You can enter another description in the Description text box.

FIGURE 6.18 The website Properties dialog box

You also configure the IP address that is associated with the site. The IP address must already be configured for the computer. If you leave the IP address at the default setting of All Unassigned, all of the IP addresses that are assigned to the computer and that have not been assigned to other websites will be used.

The TCP port specifies the port that will be used to respond to HTTP requests by default. The default TCP port that is used is TCP port 80. If you change this value, clients attempting to connect to the website must specify the correct port value. This option can be used for additional security.

Common ports that are used by IIS and can be modified for additional security include FTP on port 21, Telnet on port 23, and HTTP on port 80.

CONNECTIONS

The Connection Timeout is used to specify how long an inactive user can remain connected to the website before the connection is automatically terminated.

If you select the HTTP Keep-Alives Enabled option, the client will maintain an open connection with the server, as opposed to opening a new connection for each client request. This enhances client performance, but may degrade server performance.

LOGGING

Logging is used to enable logging features, which record details of website access. If logging is enabled, you can select from several log formats that collect information in a specified format. If you want to log user access to the website, the Log Visits check box on the Home Directory tab must also be checked (which is the default setting).

Setting ISAPI Filters

ISAPI filters direct web browser requests for specific URLs to specific ISAPI applications, which are then run. ISAPI filters are commonly used to manage customized logon authentication. These filters work by monitoring HTTP requests and responding to specific events that are defined through the filter. The filters are loaded into the website's memory.

Through the ISAPI Filters tab, shown in Figure 6.19, you can add ISAPI filters for your website. The filters are applied in the order they are listed in the list box. You can use the up and down arrow buttons to the left of the list box to change the order of the filters.

Configuring Home Directory Options

The Home Directory tab, shown in Figure 6.20, includes options for the content location, access permissions, content control, and application settings.

CONTENT LOCATION

The home directory is used to provide web content. The default directory is called `inetpub\wwwroot`. You have three choices for the location of the home directory:

- A directory on the local computer
- A share on another computer (stored on the local network and identified by a Universal Naming Convention [UNC] name)
- A redirection to a resource using a URL

FIGURE 6.19 The ISAPI Filters tab of the website Properties dialog box

FIGURE 6.20 The Home Directory tab of the website Properties dialog box

ACCESS PERMISSIONS AND CONTENT CONTROL

Access permissions define what access users have to the website. Content control specifies whether logging and indexing are enabled. By default, users have only Read access, and logging and indexing are enabled. The access permissions and content control options are described in Table 6.7.

TABLE 6.7 Access Permissions and Content Control Options

Option	Description
Script Source Access	Allows users to access source code for scripts, such as ASP (Active Server Pages) applications, if the user has either Read or Write permissions.
Read	Allows users to read or download files located in your home folder. This is used if your folder contains HTML files. If your home folder contains CGI applications or ISAPI applications, you should uncheck this option so that users can't download your application files.
Write	Allows users to modify or add to your web content. This access should be granted with extreme caution.

TABLE 6.7 Access Permissions and Content Control Options *(continued)*

Option	Description
Directory Browsing	Allows users to view website directories. This option is not commonly used because it exposes your directory structure to users who access your website without specifying a specific HTML file.
Log Visits	Allows you to log access to your website. In order to log access, the Enable Logging box in the Web Site tab of the Properties dialog box also must be checked.
Index This Resource	Allows you to index your home folder for use with the Microsoft Indexing Service.

Web service access permissions and NTFS permissions work together. The more restrictive of the two permissions will be the effective permission.

APPLICATION SETTINGS

Application, in this context, is defined as the starting point of a specific folder (and its subfolder and files) that has been defined as an application. For example, if you specify that your home folder is an application, every folder in your content location can participate in the application.

The Execute Permissions setting specifies how applications can be accessed within this folder. If you select None, no applications or scripts can be executed from this folder. The Scripts Only setting allows you to run script engines, even if no execute permissions have been set. This permission is used for folders that contain ASP scripts. The other option is Scripts and Executables, which allows all file types (including binary files with `.exe` and `.dll` extensions) to be executed.

The Application Protection setting specifies how applications will be run. There are three choices:

- Low (IIS Process) means that the application runs in the same process as the web service.
- Medium (Pooled) means that the application is run in an isolated pooled process with other applications.
- High (Isolated) means that each application runs as a separate isolated application.

Setting a Default Document

The Documents tab, shown in Figure 6.21, allows you to specify the default document users will see if they access your website without specifying a specific document. You normally set your default document as your website's home page.

FIGURE 6.21 The Documents tab of the website Properties dialog box

You can specify multiple documents in the order you prefer. This way, if a document is unavailable, the web server will access the next default document that has been defined.

You can also specify document footers. A document footer is an HTML document that will appear at the bottom of each web page that is sent to web clients.

Setting Directory Security

The Directory Security tab, shown in Figure 6.22, includes options for anonymous access and authentication control, IP address and domain name restrictions, and secure communications.

FIGURE 6.22 The Directory Security tab of website Properties dialog box

ANONYMOUS ACCESS AND AUTHENTICATION CONTROL

To enable anonymous access and specify authentication control methods, click the Edit button in the Anonymous Access and Authentication Control section of the dialog box. This brings up the Authentication Methods dialog box, as shown in Figure 6.23.

If your website is available for public use, you will most likely allow anonymous access. If you enable anonymous access, by default, your computer will use the `IUSR_`*`computername`* user account. You can limit the access the Anonymous user account has by applying NTFS permissions to your web content.

There are three choices in the Authenticated Access section of the Authentication Methods dialog box:

- The Digest Authentication for Windows Domain Servers option works only for Windows 2000 and Windows Server 2003 domain accounts. This method requires accounts to store passwords as encrypted clear text.
- The Basic Authentication option requires a Windows 2000 or Windows 2003 domain user account. If anonymous access is disabled or the anonymous account tries to access data that the account does not have permission to access, the system will prompt the user for a valid Windows 2000 or Windows 2003 domain user account. With this method, all passwords are sent as clear text. You should use this option with caution since it poses a security risk.
- The Integrated Windows Authentication option uses secure authentication to transmit the Windows 2000 or Windows Server 2003 username and password.

IP ADDRESS AND DOMAIN NAME RESTRICTIONS

This feature is not accessible and is only available with server versions of IIS.

FIGURE 6.23 The Authentication Methods dialog box

SECURE COMMUNICATIONS

You can increase the security of your website by using secure communications. With secure communications, you are able to create and manage key requests and key certificates. These options are used in conjunction with Certificate Server. This allows you to specify that you will require secure channel services (using certificates) when accessing your website.

Configuring HTTP Headers

The HTTP Headers tab, shown in Figure 6.24, allows you to configure values that will be returned to web browsers in the HTML headers of the web pages.

You can configure four options:

- If your website contains information that is time-sensitive, you can specify that you want to use content expiration. You can set content to expire immediately, after a specified number of minutes, or on a specific date. This helps the web browser determine whether it should use a cached copy of a requested page or whether it should request an updated copy of the web page from the website.
- Custom HTTP headers are used to replace the default HTTP headers that are normally used with customized HTTP headers from your web server to the client browser. For example, you may want to specify a custom HTTP header to send instructions that may not be supported by the HTML specification that is currently in use.
- Content ratings allow you to specify appropriate restrictions if a site contains violence, sex, nudity, or adult language. Most web browsers can then be configured to block objectionable material based on how the content rating has been defined.
- MIME (Multipurpose Internet Mail Extensions) maps are used to configure web browsers so that they can view files that have been configured with different formats.

FIGURE 6.24 The HTTP Headers tab of the website Properties dialog box

Specifying Custom Error Messages

If the web browser encounters an error, it will display an error message. By default, predefined error messages are displayed. Through the Custom Errors tab, shown in Figure 6.25, you can customize the error message that the user will see. To generate a custom error message, you create an `.htm` file, which can then be mapped to a specific HTML error.

Setting Server Extensions

By default, Server Extensions are not enabled on IIS Professional version. You can enable Server Extensions by right-clicking your website and selecting All Tasks, then Configure Server Extensions, which will run the Server Extensions Wizard. Before you enable this option, you should have a good understanding of IIS security. Enabling Server Extensions can create security risks for IIS.

Once Server Extensions are enabled, the Server Extensions tab, shown in Figure 6.26, allows you to configure publishing controls for FrontPage options. FrontPage is used to create and edit HTML pages for your website through a What You See Is What You Get (WYSIWYG) editor.

This tab includes the following options:

- The Enable Authoring option specifies whether authors can modify the content of the website. If this option is selected, you can specify version control, performance based on how many pages the website hosts, and the client scripting method that will be used.
- The Options section includes Settings and Administer buttons, which allow you to specify how mail should be sent and Office Collaboration features (this option is enabled only if Microsoft Office is configured).
- The Don't Inherit Security Settings option overrides the global security settings for the website.

FIGURE 6.25 The Custom Errors tab of the website Properties dialog box

FIGURE 6.26 The Server Extensions tab of the website Properties dialog box

Troubleshooting Website Access

If users are unable to access your website, the problem may be caused by improper access permissions, an improperly configured home folder or default document, or use of the wrong TCP port. Here are some tips for troubleshooting website access problems:

- Determine whether anonymous access is allowed. If so, verify that the username and password that have been configured through IIS match the name of the user account and password that are in the Windows XP, Windows 2000 domain, or Windows 2003 domain user database.
- Confirm that access has not been denied based on the IP address or domain name.
- Make sure that the proper access permissions have been configured.
- Confirm that the home folder is properly configured and that the default document has been properly configured.
- Make sure that the TCP port is set to port 80 or that you are accessing the website using the proper TCP port number.
- Make sure that the NTFS permissions have not been set on the home folder so that they deny access to website users.

Exam Essentials

Know how to install and configure IIS. Be able to install, configure, and troubleshoot IIS. Be able to manage your web servers.

Configure, Manage, and Troubleshoot Remote Desktop and Remote Assistance

Remote Desktop and Remote Assistance are new features of Windows XP Professional. *Remote Desktop* is a service that allows you to remotely take control of your computer from another location. For example, you could access your work computer from home or while traveling on business. *Remote Assistance* is used to request assistance from another Windows XP user.

You will learn more about Remote Desktop and Remote Assistance in the following sections.

Critical Information

Remote Desktop is a new tool of Windows XP Professional that allows you to take control of a remote computer's keyboard, video, and mouse. This tool does not require that someone collaborate with you on the remote computer. While the remote computer is being accessed, it remains locked and any actions that are performed remotely will not be visible to the monitor that is attached to the remote computer. Remote Desktop was designed to be used in the following situations:

- For troubleshooting computers within an organization that may be in a remote location, but are connected to the central network through a direct network connection, secure Virtual Private Network (VPN), or remote access
- To allow Help Desk administrators within a network to remotely troubleshoot organizational computers
- To allow remote access to organizational computers without security concerns that unauthorized users are viewing the remote computer's monitor and watching what actions are being performed remotely

In the following sections, you will learn:

- The Remote Desktop restrictions
- The minimum set of requirements for Remote Desktop
- How to configure the computer that will be accessed remotely
- How to configure the computer that will be used to access the remote computer
- How to start a remote desktop session
- How to customize a remote desktop session
- How to end a remote desktop session

Remote Desktop Restrictions

Remote Desktop uses all of the inherent security features of Windows XP Professional. In addition, Remote Desktop imposes the following additional security features:

- Remote Desktop is designed to be used to access internal domain computers. If the computer that you want to access is outside your organization's firewall, then you will need to use Internet proxy software or Microsoft Internet Security and Acceleration Server client software.

- If you want to establish a session from a computer via the Internet to your company's internal network, you must first establish a secure VPN connection to the internal network you wish to access.
- Remote Desktop can't be used to create a connection between two computers directly connected to the Internet.
- There is no option for simultaneous remote and local access to the Windows XP Professional Desktop. If a computer will be accessed remotely, Windows XP will prompt the local user that they need to be logged off before the computer can be accessed remotely.

Remote Desktop Requirements

To use Remote Desktop, the following requirements must be met:

- Windows XP Professional must be running on the computer that will be accessed remotely.
- The computer that will access the remote computer must be running Windows 95 or higher and have Remote Desktop client software installed and configured.
- There must be an IP connection between the two computers that will be used to establish a Remote Desktop session.

Configuring a Computer for Remote Access

You enable a computer to be accessed remotely through Control Panel. To enable remote access, select Start ➢ Control Panel ➢ Performance and Maintenance ➢ System. Click the Remote tab. Within the Remote tab of System Properties, check Allow Users to Connect Remotely to This Computer, as shown in Figure 6.27. To enable Remote Desktop, you must be logged on to the computer as an administrator or as a member of the Administrators group.

FIGURE 6.27 The Remote tab of the System Properties dialog box

By default, only members of the Administrators group can access a computer that has been configured to use Remote Desktop. To enable other users to access the computer remotely, click the Select Remote Users button shown in Figure 6.27. This brings up the Remote Desktop Users dialog box, as shown in Figure 6.28, and allows you to specify which users can access the remote computer by selecting users through the Add or Remove buttons.

When you enable remote access to a computer, the changes will take effect immediately. By default, members of the local or domain Administrators group will have Remote Desktop permissions. Members of the Administrators groups can end a local user's session without permission. Non-administrative users who are granted Remote Desktop permissions can't end a local user's session if the local user refuses the session.

Installing the Remote Desktop Connection Client Software

The Remote Desktop Connection client software is used to control a Windows XP Professional computer remotely. This software is installed by default on computers running Windows XP Home Edition and Windows XP Professional. The Remote Desktop Communications client software is used for remote desktop support on pre–Windows XP clients, which are listed within this section.

To install the Remote Desktop Connection client software on a Windows XP computer, take the following steps:

1. Insert the Windows XP Professional CD in the computer that will be used for remote access.
2. The Welcome Page will appear. Select Perform Additional Tasks, then click the Setup Remote Desktop option.
3. Follow the prompts that appear.

FIGURE 6.28 The Remote Desktop Users dialog box

You can also install the Remote Desktop Communications client software on the following computers:

- Windows 95
- Windows 98
- Windows Me
- Windows NT 4
- Windows 2000

Starting a Remote Desktop Session

Once you have configured the computer that will be accessed remotely and have installed the Remote Desktop Connection client software, you are ready to start a Remote Desktop session. You start a session through the following steps:

1. Start ➢ All Programs ➢ Accessories ➢ Communications ➢ Remote Desktop Connection. You could also use the command-line utility `MSTSC` to start the Remote Desktop connection. This will bring up the dialog box shown in Figure 6.29.
2. In the Computer name field, type in the name of the computer you wish to access. Remote Desktop must be enabled on this computer and you must have permissions to access the computer remotely.
3. Click the Connect button.
4. The Logon to Windows dialog box will appear. Type in your username, password, and domain name, and click OK.
5. The Remote Desktop Connection window will open, and you will now have remote access.

Once a computer has been accessed remotely, it will be locked. No one at the local site will be able to use the local computer without a password. In addition, no one at the local site will be able to see the work that is being done on the computer remotely.

Customizing a Remote Desktop Connection

You can manage your Remote Desktop connection settings by clicking the Options button that was shown in Figure 6.29. This brings up the dialog box shown in Figure 6.30. Through this dialog box you can configure the following:

General Contains logon settings.

Display Is used to set the size of the remote Desktop and the colors used by the remote Desktop.

Local Resources Are used to specify whether you hear remote computer sounds, the Windows keyboard combinations that will be applied, and which local devices you will automatically connect to on the local computer.

Programs Allows you to start a program on connection.

Experience Is used to select your connection speed, so performance can be optimized based on it.

FIGURE 6.29 The Remote Desktop Connection dialog box

FIGURE 6.30 The Remote Desktop Connection options

The General tab contains a Connection Settings button. This allows you to save your settings. By default, settings are saved in the `My Documents\Remote Desktop` folder. The default extension for Remote Desktop files is `.rdp`.

Ending a Remote Desktop Session

To end a Remote Desktop Session, take the following steps:

1. In the Remote Desktop Connection window, select Start ➢ Shutdown.
2. The Shut Down Windows dialog box appears. In the drop-down menu, select Log Off and click the OK button.

Using Remote Assistance

Remote Assistance provides a mechanism for requesting help for *x*86-based computers through Windows Messenger and e-mail, or by sending a file. To use Remote Assistance, the computer

requesting help and the computer providing help must be using Windows XP Professional and both computers must have interconnectivity. Common examples of when you would use Remote Assistance include the following:

- When you are diagnosing problems that are difficult to explain or reproduce. By using Remote Assistance, you can remotely view the computer and the remote user can show you what the error is or step you through the processes that are used to cause the error to occur.
- When you need an inexperienced user to perform a complex set of instructions. Instead of asking the inexperienced user to complete the task, you can use Remote Assistance to take control of the computer and complete the tasks yourself.

In the following sections, you will learn more about:

- Differences between Remote Desktop and Remote Assistance
- Options for establishing remote connections
- Enabling Remote Assistance
- How users request remote assistance
- How administrators respond to remote assistance requests
- Administrator-initiated remote assistance
- Limitations of Remote Assistance invitations
- Security and Remote Assistance

Differences Between Remote Desktop and Remote Assistance

The following are the key differences between the Remote Desktop utility and the Remote Assistance utility:

- With Remote Desktop, there is only one connection at a time. With Remote Assistance, the expert is able to establish a concurrent session with the user at the remote computer.
- Remote Assistance requires the user at the remote computer to authorize access. Remote Desktop does not require administrators to seek permission before they establish a remote session.
- With Remote Assistance, both computers have to be running Windows XP Professional.

Options for Establishing Remote Assistance

The following options can be used to establish remote connections:

- A LAN connection between the expert's computer and the novice's computer
- An Internet connection between the expert's computer and the novice's computer
- Connection via the Internet when the expert computer is behind a firewall and the novice computer is just connected to the Internet
- Connection via the Internet when the expert computer is behind a firewall and the novice computer is also behind a firewall

If the Remote Assistance connections are made through a firewall, the firewall may need to be configured to open TCP Port 3389.

Enabling Remote Assistance

You can enable Remote Assistance through the following steps:

1. Select Start ➢ Control Panel ➢ Performance and Maintenance ➢ System.
2. Click the Remote tab and select the Allow Remote Assistance Invitations to Be Sent from This Computer check box, as shown in Figure 6.31.

If you click the Advanced button from the Remote tab, you can set configuration options for the maximum number of days that invitations will remain open, as shown in Figure 6.32.

FIGURE 6.31 The Remote Tab of the System Properties dialog box

FIGURE 6.32 The Remote Assistance Settings dialog box

Requesting Remote Assistance

If a user requires remote assistance, they send an invitation. The following steps are used to request remote assistance:

1. Notify the person providing assistance that you will be sending a Remote Assistance invitation. Notification methods might include e-mail, instant messaging, or a telephone call. Give the person providing assistance the password that will be used for the Remote Assistance session.
2. Select Start ➢ Help and Support.
3. From the Help and Support Center window, under Ask for Assistance, click the Invite a Friend to Connect to Your Computer with Remote Assistance option, as shown in Figure 6.33.
4. From the Remote Assistance window, shown in Figure 6.34, select Invite Someone to Help You.
5. You will be asked to specify how you want to contact the person providing assistance. You can specify Windows Messenger or e-mail (for example using Outlook or Outlook Express).
6. Click Send Invitation to send the invitation. You can specify the invitation delivery method, the length of time until the invitation expires, and whether to use the optional password protection feature.

FIGURE 6.33 Help and Support Center window

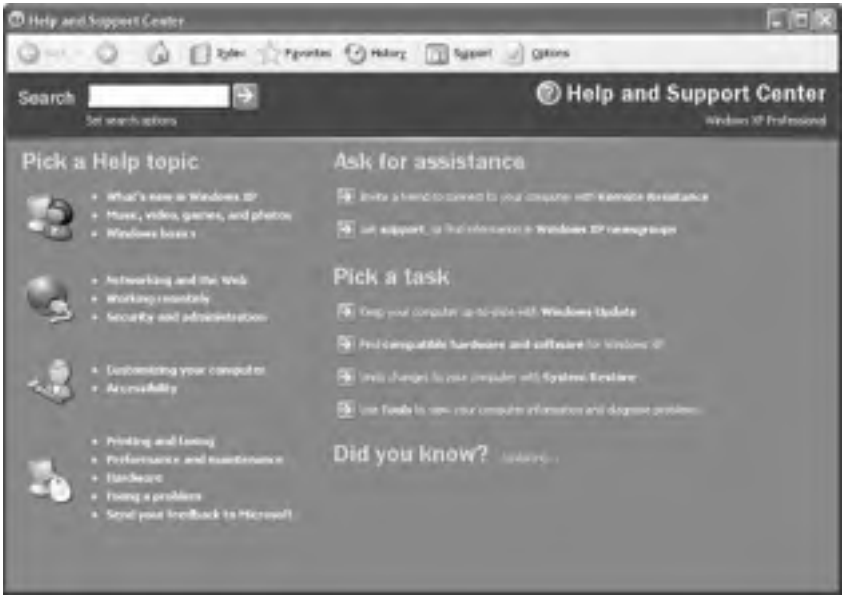


FIGURE 6.34 Remote Assistance window

Responding to Remote Assistance Requests

When you receive a Remote Assistance invitation, you would use the following steps to respond:

1. Receive the Remote Assistance invitation via e-mail or Instant Messenger.
2. Open the invitation and double-click the attachment that is used to start the session. If a password has been configured, provide the appropriate password.
3. The user seeking assistance will see an acceptance message on their screen and be prompted to verify that you be allowed to view the remote screen and chat with them.
4. The user seeking assistance should confirm the acceptance message and a terminal window will appear on the your monitor, displaying the user's computer desktop.
5. You will then be able to manipulate remotely the user's computer by using the Take Control option, after the user approves the interaction by clicking the Allow Expert Interaction button that they see in the Remote Assistance window.

The person who requested remote assistance can terminate the session at any time by clicking the Stop Control button in the Remote Assistance window.

Initiating a Remote Assistance Session

Administrators can also initiate a remote assistance session through the Offer Remote Assistance feature. By default, this option is disabled, but it can be enabled through Group Policy by taking the following actions:

1. Select Start ➢ Run and in the Run dialog box, type **`gpedit.msc`**.
2. Expand Local Computer Policy ➢ Computer Configuration ➢ Administrative Templates.
3. Expand System, then Remote Assistance.
4. In the details pane, double-click Offer Remote Assistance, click Enabled, then the OK button.

Once Offer Remote Assistance is enabled, you can offer remote assistance to a user through the following steps:

1. Inform the user that you will be offering remote assistance.
2. From the Help and Support Center dialog box, under the Pick a Task list, select Tools, then Offer Remote Assistance.
3. Follow the instructions for providing the name or IP address of the user's computer.
4. The user will see a prompt that you—the network administrator—would like to view the screen, chat with them in real time, and work on their computer. The user then accepts your assistance request.

Reuse of Remote Assistance Invitations

If both of the following conditions are met, a Remote Assistance ticket can be used more than once:

- The invitation ticket can't be expired.
- The IP address of the computer cannot have changed since the ticket was issued. Such a change can occur if a user connects to the Internet through an ISP that assigns dynamic IP addresses each time the user connects to the Internet.

Security and Remote Assistance

The following list includes a security concern and a security configuration concern tied to using Remote Assistance:

- If a user clicks the Allow Expert Interaction button, then the person providing expert assistance will have all of the security privileges that the local user has.
- If you allow a user outside of your organization to access your computer, you should have them connect via a VPN account. If they connect through the network firewall, then TCP Port 3389 must be opened.

Exam Essentials

Know what Remote Desktop and Remote Assistance are. Be able to configure and manage Remote Desktop and Remote Assistance. Be able to troubleshoot any access problems.

Configure, Manage, and Troubleshoot an Internet Connection Firewall (ICF)

If you have a computer that attaches to the Internet through a dial-up modem, cable modem, or DSL connection, you can use an *Internet Connection Firewall (ICF)* to protect your connection from passive or active Internet security threats. *Firewalls* are security systems that act as a boundary between your computer or network and the outside world. ICF works by acting as a protective mechanism by restricting what access is allowed to your computer through the Internet.

Critical Information

You would use ICF only if your computer was directly connected to the Internet. If your network already uses a firewall or a proxy server, it doesn't need ICF. ICF should also not be installed on computers that use VPN services. ICF can't be enabled on private connections for host computers of ICS.

ICF is a stateful firewall, which means that it monitors all communications by defining the source and destination traffic of all messages that are sent to the computer. ICF works by using a flow table, which defines protected networks. The only incoming traffic that is allowed is traffic that can be validated through an entry in the flow table. If unauthorized traffic is detected, ICF automatically discards the unauthorized packets. If you originate traffic from an ICF computer, then that traffic is logged in a table, so that if you receive inbound traffic from a site you have contacted, that traffic is allowed to pass through.

To configure and manage ICF, you take the following steps:

1. Select Start ➢ Control Panel and click Network and Internet Connections. Click Network Connections and right-click the dial-up connection on which you want to enable ICF. Select Properties.
2. Click the Advanced tab. Check the Protect My Computer and Network by Limiting or Preventing Access to This Computer from the Internet option.
3. To configure ICF logging, click the Settings button. In the Advanced Settings dialog box, click the Security Logging tab (Figure 6.35). This allows you to configure ICF logging options such as whether dropped packets are logged and whether successful connections are logged. You can also specify the log file that will be used and the maximum log file size.

Exam Essentials

Know what the purpose and use of ICF is. Be able to configure your computer to use ICF.

FIGURE 6.35 The Security Logging tab of the Advanced Settings dialog box

Review Questions

1. You are attempting to access the Internet from your Windows XP Professional computer. You normally access the Internet with no problems using DHCP. When you type **`ipconfig /all`**, you see that you are configured to use the IP address 169.254.0.10. What should you do?

   A. Use `ipconfig /renew`.

   B. Configure your computer to use a manual IP address.

   C. Confirm that your default gateway is configured properly.

   D. Confirm that your subnet mask is configured properly.

2. You are configuring a Windows XP Professional computer. The computer is having connectivity problems. You want to manually configure an IP address and want to keep the configuration as simple as possible. Which of the following options represent a minimal IP configuration? Choose all that apply.

   A. IP address

   B. Subnet mask

   C. Default gateway

   D. DNS server

3. You recently changed the configuration on your computer for the DNS server it is using. The new DNS server has some incorrect settings that are causing problems. You configure your computer to use the original DNS server. What additional step do you need to take to purge the DNS Resolver cache?

   A. `Nbtstat /clear`

   B. `Nbtstat /flush`

   C. `Ipconfig /flushdns`

   D. `Ipconfig /clear`

4. Which of the following protocols would you use if you were using dial-up networking to connect to a RAS server using smart card authentication?

   A. PAP

   B. SPAP

   C. MS-CHAP 2

   D. EAP

5. Which of the following options is *not* configured on the computer that hosts Internet Connection Sharing when it is enabled?

   A. The Internet host computer's address becomes 192.168.0.1 with a subnet mask of 255.255.255.0. The host also becomes the DHCP allocator, which acts as a "baby" DHCP server.

   B. All of the network clients must get their IP addresses automatically through the DHCP allocator, which gives out addresses randomly to the clients, in the range 192.168.0.2 through 192.168.0.254 with a subnet mask of 255.255.255.0.

   C. The autodial feature is enabled on the ICS host computer.

   D. DNS Proxy is disabled on the ICS host computer.

6. You are trying to access a website that uses Secure Socket Layer (SSL) services. Which of the following requests should you make through Internet Explorer?

   A. `http://`

   B. `shhtp://`

   C. `https://`

   D. `sechttp://`

7. You have installed IIS on your Windows XP Professional computer. What port needs to be opened on your firewall to allow HTTP requests to be processed?

   A. 21

   B. 40

   C. 80

   D. 96

8. You are using IIS to host a website on your Windows XP Professional computer. Which of the following accounts is used by default to provide access for anonymous users?

   A. `IUSR_`*`computername`*

   B. `IIS_`*`computername`*

   C. `Internet_User`

   D. `Anonymous`

9. You are the network administrator of a large network. You want to verify the configuration of a Windows XP Professional computer by taking control of the computer remotely. What needs to be configured on the Windows XP Professional computer so that you can use Remote Desktop?

   A. From Control Panel ➢ Remote Desktop, configure Remote Desktop.

   B. From Control Panel ➢ System, click the Remote tab and check Allow Users to Connect Remotely to This Computer.

   C. From Device Manager ➢ Remote Options, check Allow Remote Access.

   D. From Support, click the Remote tab and check Allow Users to Connect Remotely to This Computer.

10. You use a cable modem to connect to the Internet. You are concerned with security and want to protect your computer from malicious attacks. What Windows XP Professional service should you use?

A. ICS

B. ICF

C. WINS

D. Proxy Server

Answers to Review Questions

1. A. By default, a range of Class B network addresses, 169.254.0.1–169.254.255.254, has been set aside as private Class B network addresses. Windows XP Professional uses this range of addresses to automatically assign IP addresses if Automatic Private IP Addressing (APIPA) is used. In this case, your computer needs to get its address from a DHCP server. You can force this process through `ipconfig /renew`.

2. A, B. To configure a TCP/IP client, you must specify an IP address and a subnet mask. Depending on your network, optional settings might include the default gateway, DNS server settings, and WINS server settings.

3. C. The `Ipconfig /flushdns` command is used to purge the DNS Resolver cache.

4. D. Extensible Authentication Protocol (EAP) is used in conjunction with other security devices, including smart cards and certificates.

5. D. DNS Proxy is enabled on the ICS host computer.

6. C. If the web server you are trying to access is using SSL services, then instead of using an `http://` requests, you use secure HTTP, and the request would use `https://`.

7. C. Make sure that the TCP port is set to port 80 or that you are accessing the website using the proper TCP port number.

8. A. If your website is available for public use, you will most likely allow anonymous access. If you enable anonymous access, by default, your computer will use the `IUSR_`*`computername`* user account. You can limit the access that the Anonymous user account has by applying NTFS permissions to your web content.

9. B. You enable a computer to be accessed remotely through Control Panel. To enable remote access, select Start ➢ Control Panel ➢ Performance and Maintenance ➢ System. Click the Remote tab. Within the Remote tab of System Properties, check Allow Users to Connect Remotely to This Computer. To enable Remote Desktop, you must be logged on to the computer as an administrator or a member of the Administrators group.

10. B. Internet Connection Firewall (ICF) is a stateful firewall, which means that it monitors all communications by defining the source and destination traffic of all messages that are sent to the computer. ICF works by using a flow table, which defines protected networks. The only incoming traffic that is allowed is traffic that can be validated through an entry in the flow table. If unauthorized traffic is detected, ICF automatically discards the unauthorized packets. If you originate traffic from an ICF computer, then that traffic is logged in a table so that if you receive inbound traffic from a site you have contacted, that traffic is allowed to pass through.

Chapter 7

Configuring, Managing, and Troubleshooting Security

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configure, manage, and troubleshoot Encrypting File System (EFS).**
- ✓ **Configure, manage, and troubleshoot a security configuration and local security policy.**
- ✓ **Configure, manage, and troubleshoot local user and group accounts.**
  - Configure, manage, and troubleshoot auditing.
  - Configure, manage, and troubleshoot account settings.
  - Configure, manage, and troubleshoot account policy.
  - Configure, manage, and troubleshoot user and group rights.
  - Troubleshoot cache credentials.
- ✓ **Configure, manage, and troubleshoot Internet Explorer security settings.**

This chapter covers using Encrypting File System (EFS), managing security configuration and local security policy, managing user and group accounts, and configuring and managing Internet Explorer.

Configure, Manage, and Troubleshoot Encrypting File System (EFS)

Data encryption is a way to increase data security. Encryption is the process of translating data into code that is not easily accessible. Once data has been encrypted, you must have a password or key to decrypt it. Unencrypted data is known as plain text, and encrypted data is known as cipher text.

The *Encrypting File System (EFS)* is the Windows XP technology that is used to store encrypted files on NTFS partitions. Encrypted files add an extra layer of security to your file system. A user with the proper key can transparently access encrypted files. A user without the proper key is denied access. If the user who encrypted the files is unavailable, you can use the *data recovery agent (DRA)* to provide the proper key to decrypt folders or files.

In the following sections, you will learn about the new features for EFS for Windows XP and Windows Server 2003, how to create and manage DRAs, how to recover encrypted files, how to share encrypted files, and how to use the `Cipher` utility.

Critical Information

To use EFS, a user specifies that a folder or file on an NTFS partition should be encrypted. The encryption is transparent to that user, who has access to the file. However, when other users try to access the file, they will not be able to unencrypt the file—even if those users have Full Control NTFS permissions. Instead, they will receive an error message.

To encrypt a folder or a file, take the following steps:

1. Select Start ➢ Run and type **`Explorer`**.
2. In Windows Explorer, find and select the folder or file you wish to encrypt.
3. Right-click the folder or file and select Properties from the pop-up menu.
4. In the General tab of the folder or file Properties dialog box, click the Advanced button.
5. The Advanced Attributes dialog box appears. Check the Encrypt Contents to Secure Data check box. Then click the OK button.

6. The Confirm Attribute Changes dialog box appears. Specify whether you want to apply encryption only to this folder (Apply Changes to This Folder Only) or to the subfolders and files in the folder, as well (Apply Changes to This Folder, Subfolders and Files). Then click the OK button.

To decrypt folders and files, repeat these steps, but uncheck the Encrypt Contents to Secure Data option in the Advanced Attributes dialog box.

Managing EFS File Sharing

In Windows 2000 and Windows XP Professional, only one user can use or access a folder that has been encrypted. However, Windows XP Professional does allow you to support EFS file sharing at the file level (as opposed to the folder level). By implementing EFS file sharing, you provide an additional level of recovery in the event that the person who encrypted the files is unavailable.

To implement EFS file sharing, you would take the following steps:

1. Encrypt the file if it is not already encrypted (see previous section for instructions).
2. Through Windows Explorer, access the encrypted file's properties, as shown in Figure 7.1. At the bottom of the dialog box, click the Advanced button.
3. The Advanced Attributes dialog box will appear, as shown in Figure 7.2.

   In the Compress or Encrypt Attributes section of the Advanced Attributes dialog box, click the Details button, which brings up the Encryption Details dialog box shown in Figure 7.3.

FIGURE 7.1 An encrypted file's Properties dialog box

FIGURE 7.2 Advanced Attributes dialog box

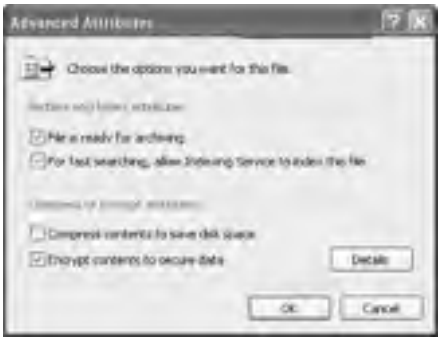


FIGURE 7.3 Encryption Details dialog box

4. In the Encryption Details dialog box, click the Add button to add any additional users (provided they have a valid certificate for EFS in the Active Directory) who should have access to the encrypted file.

Using the DRA to Recover Encrypted Files

If the user who encrypted the folders or files is unavailable to decrypt the folders or files when they're needed, you can use the DRA to access the encrypted files. DRAs are

implemented differently depending on the version of your operating system and the configuration of your computer.

- For Windows 2000 Professional and Windows 2000 Server computers, a DRA was mandatory, and EFS could not be used if a DRA was not in place. For Windows 2000 Professional computers that were installed as a part of the Active Directory, the domain Administrator user account is automatically assigned the role of the DRA. If the Windows 2000 Professional computer was not a part of the Active Directory, then the local administrator user account is automatically assigned the role of DRA.
- For Windows XP Professional computers that are a part of a Windows 2000 or Windows 2003 Active Directory domain, the domain Administrator user account is automatically assigned the role of DRA.
- For Windows XP Professional computers that are installed as stand-alone computers or if the computer is a part of a workgroup, no default DRA is assigned.

You should use extreme caution when using EFS on a stand-alone Windows XP Professional computer. If the user who encrypts the files is unavailable, there is no default recovery process, and all access to the files will be lost.

Creating a DRA on a Stand-Alone Windows XP Professional Computer

If Windows XP Professional is installed as a stand-alone computer or on a computer that is part of a workgroup, then no DRA is created by default. To manually create a DRA, you use the `Cipher` command-line utility as follows (this is covered in greater detail in the following section):

```
Cipher /R:filename
```

The `/R` switch is used to generate two files, one with a `.pfx` extension and one with a `.cer` extension. The `.pfx` file is used for data recovery and the `.cer` file includes a self-signed EFS recovery agent certificate. The `.cer` file (self-signed public key certificate) can then be imported into the local security policy and the `.pfx` file (private key) can be stored in a secure location.

Once you have created the public and private keys to be used with EFS, you can specify the DRA through Local Security Policy, using the following steps:

1. Through Local Security Policy, which can be accessed through Administrative eTools or the Local Computer Policy Microsoft Management Console (MMC) snap-in, expand Public Key Policies ➢ Encrypting File System, as shown in Figure 7.4.
2. Right-click Encrypting File System and select Add Data Recovery Agent.
3. The Add Recovery Agent Wizard will start. Click the Next button to continue.
4. The Select Recovery Agents dialog box will appear as shown in Figure 7.5. Click the Browse Folders button to access the `.cer` file you created with the `Cipher /R:filename` command. Select the certificate and click the Next button.
5. The Completing the Add Recovery Agent Wizard dialog box will appear. Confirm the settings are correct and click the Finish button.
6. You will see the Data Recovery Agent listed in the Local Security Settings dialog box, under Encrypting File System.

FIGURE 7.4 Local Security Settings dialog box

FIGURE 7.5 Add Recovery Agent Wizard dialog box

Recovering Encrypted Files

If DRA has the private key to the DRA certificate (that was created through `Cipher /R:`*`filename`*), the DRA can decrypt files in the same manner as the user who originally encrypted the file. Once the encrypted files are opened by a DRA, they are available as unencrypted files, and can be stored as either encrypted or unencrypted files.

In Windows 2000, encrypted files could be accessed by changing the password of the user who encrypted the files, and then logging in as that user. On a Windows XP Professional computer, if a user's local password is changed by an administrator or any method other than the local user changing their own password, all access to previously encrypted files will be blocked to the local user.

Using the *Cipher* Utility

Cipher is a command-line utility that can be used to encrypt files on NTFS volumes. The syntax for the `Cipher` command is as follows:

`Cipher /[command parameter] [filename]`

Table 7.1 lists the command parameters associated with the `Cipher` command.

TABLE 7.1 **Cipher** Command Parameters

Parameter	Description
`/e`	Specifies that files or folders should be encrypted. Any files that are subsequently added to the folder will be encrypted.
`/d`	Specifies that files or folders should be decrypted. Any files that are subsequently added to the folder will not be encrypted.
`/s:dir`	Specifies that subfolders of the target folder should also be encrypted or decrypted based on the option specified.
`/I`	Causes any errors that occur to be ignored. By default, the `CIPHER` utility stops whenever an error occurs.
`/f`	Forces all files and folders to be encrypted or decrypted, regardless of their current state. Normally, if a file is already in the specified state, it is skipped.
`/q`	Runs `CIPHER` in quiet mode and displays only the most important information.
`/a`	Specifies that you want the operation you are executing to be applied to all files and folders.
`/h`	By default, files with hidden or system attributes are omitted from display. This option specifies that hidden and system files should be displayed.
`/r`	Used to generate a recovery agent key and certificate for use with EFS.

Exam Essentials

Be able to encrypt and decrypt files and folders. Know how to use Windows Explorer or the `Cipher` command-line utility to encrypt and decrypt files and folders.

Be able to recover encrypted files. If the person who encrypts a file is unable to decrypt a file, know how to use the DRA to recover an encrypted file.

Configure, Manage, and Troubleshoot a Security Configuration and Local Security Policy

Windows XP Professional offers a wide variety of security options. If the Windows XP Professional computer is a part of a Windows 2000 or Windows 2003 domain, then security can be applied through a group policy within Active Directory. If the Windows XP Professional computer is not a part of a Window 2000 or Windows 2003 domain, then you use Local Group Policy objects to manage local security.

Critical Information

The tools that are used to manage Windows XP Professional computer security configurations are dependent on whether the Windows XP Professional computer is a part of a Windows 2000 or Windows 2003 domain environment.

If the Windows XP Professional client is not a part of a Windows 2000 or Windows 2003 domain—for example, if the computer is installed as a stand-alone computer or part of a Windows workgroup, Windows NT 4 domain, Unix network, or NetWare network—then you apply security settings through *Local Group Policy objects (LGPOs)*. LGPOs are a set of security configuration settings that are applied to users and computers. LGPOs are created and stored on the Windows XP Professional computer.

If your Windows XP Professional computer is a part of a Windows 2000 Server or Windows Server 2003 domain, both of which use the services of *Active Directory*, then you typically manage and configure security through *Group Policy Objects (GPOs)*. Group Policy is an MMC snap-in that is used to define security (called group policies) for users, groups, and computers via the Active Directory. Windows XP Professional computers that are a part of a Windows 2000 or Windows 2003 domain still have an LGPO, and the LGPO can be used in conjunction with the Active Directory group policies.

The settings that can be applied through the Group Policy utility within Active Directory are more comprehensive than the settings that can be applied through LGPOs. By default, the LGPO is stored in `\systemroot\System32\GroupPolicy`. Table 7.2 lists all of the options that can be set for GPOs within the Active Directory and which of those options can be applied through LGPOs.

TABLE 7.2 Group Policy and LGPO Setting Options

Group Policy Setting	Available for LGPO?
Software installation	No
Scripts	Yes

TABLE 7.2 Group Policy and LGPO Setting Options *(continued)*

Group Policy Setting	Available for LGPO?
Security settings	Yes
Administrative templates	Yes
Folder redirection	No
RIS options	No
Internet Explorer configuration management	No

Group Policy Objects and Active Directory

Most Windows XP Professional computers reside within Windows 2000 domains or Windows 2003 domains. Typically, GPOs are applied through the Active Directory, as this is much easier to globally manage than applying LGPOs at local levels. To help you understand how GPOs and LGPOs work together, this section will first overview the Active Directory and then show you how GPOs and LGPOs are applied based on predefined inheritance rules.

Active Directory Overview

Within Active Directory, you have several levels of hierarchical structure. A typical structure will consist of domains and *Organizational Units (OUs)*. Other levels exist within Active Directory, but this overview focuses on domains and OUs in the context of using GPOs.

The domain is the main unit of organization within Active Directory. Within a domain are many domain objects (including users, groups, and GPOs). Each domain object can have security applied that specifies who can access the object and the level of access they have.

Within a domain, you can further subdivide and organize domain objects through the use of OUs. This is one of the key differences between Windows NT 3.51 and Windows NT 4 domains, and Windows 2000 Server and Windows Server 2003 domains. The NT domains were not able to store information hierarchically. Windows 2000 Server and Windows Server 2003 domains, through the use of OUs, allow you to store objects hierarchically, typically based on function or geography.

For example, assume that your company is called ABCCORP. You have locations in New York, San Jose, and Belfast. You might create a domain called ABCCORP.COM with OUs called NY, SJ, and Belfast. In a very large corporation, you might also organize the OUs based on function. For example, the domain could be ABCCORP.COM and the OUs might be SALES, ACCT, and TECHSUPP. Based on the size and security needs of your organization, you might also have OUs nested within OUs. As a general rule, however, you will want to keep your Active Directory structure as simple as possible.

GPO Inheritance

When GPOs are created within Active Directory, there is a specific order of inheritance. That is, the policies are applied in a specific order within the hierarchical structure of Active Directory. When a user logs on to Active Directory, depending on where within the hierarchy GPOs have been applied, the order of application is as follows:

1. Local computer
2. Site (group of domains)
3. Domain
4. OU

What this means is that the local policy is, by default, applied first when a user logs on. Then the site policies are applied, and if the site policy contains settings that the local policy doesn't have, they are added to the local policy. If there are any conflicts, the site policy overrides the local policy. Then the domain policies are defined. Again, if the domain policy contains additional settings, they are incorporated. When settings conflict, the domain policy overrides the site policy. Next, the OU policies are applied. Additional settings are incorporated; for conflicts, the OU policy overrides the domain policy. If conflicts occur between computer and user policy settings, the computer policy setting is applied.

The following options are available for overriding the default behavior of GPO execution:

No Override The No Override option is used to specify that child containers can't override the policy settings of higher-level GPOs. In this case, the order of precedence would be that site settings override domain settings, and domain settings override OU settings. The No Override option would be used if you wanted to set corporate-wide policies without allowing administrators of lower-level containers to override your settings. This option can be set per-container, as needed.

Block Inheritance The Block Inheritance option is used to allow the child container to block GPO inheritance from parent containers. This option would be used if you did not want to inherit GPO settings from parent containers and wanted only the GPO you had set for your container to be applied.

If a conflict exists between the No Override and the Block Inheritance settings, then the No Override option would be applied.

Using the Group Policy Result Tool

When a user logs on to a computer or domain, a resulting set of policies to be applied is generated based on the LGPO, site GPO, domain GPO, and OU GPO. The overlapping nature of group policies can make it difficult to determine what group policies will actually be applied to a computer or user.

To help determine what policies will actually be applied, Windows XP includes a tool called the Windows XP Operating System *Group Policy Result Tool*. This tool is accessed through the `GPResult.exe` command-line utility. The `GPResult.exe` command displays the resulting set of policies that were enforced on the computer and the specified user during the logon process.

You can use this utility by accessing a command prompt and typing `GPResult`. This will display the Resultant Set of Policy (RSOP) for the computer and user who is currently logged on. Several options can be used with this command. Use `GPResult /?` to get verbose help on each command switch option.

Understanding GPO Application

When you use an LGPO on a Windows XP Professional computer, there is only one GPO, which applies to all of the computer's users. Policies that have been linked though Active Directory will take precedence over any established local group policies. Local group policies are typically applied to computers that are not part of a network or are in a network that does not have a domain controller, and thus do not use Active Directory.

You apply an LGPO to a Windows XP Professional computer through the Local Computer Policy snap-in within the MMC. On a Windows XP Professional computer, the Local Group Policy snap-in will be displayed within the MMC as Local Computer Policy, as shown in Figure 7.6.

Through local group policies, you can set a wide range of security options. At the top levels, they are managed as Computer Configuration and User Configuration. The following sections describe in detail how to apply security settings through local group policy. The two main areas of security configuration are:

- Account policies, which are used to configure password and account lockout features
- Local policies, which are used to configure auditing, user rights, and security options

You can also access the account policies and local policies by opening the Control Panel and selecting Performance and Maintenance ➢ Administrative Tools ➢ Local Security Policy.

FIGURE 7.6 Accessing the Account Policies folders

Configuring Security Policies

Security option policies are used to configure security for the computer. Unlike user right policies, which are applied to a user or group, security option policies apply to the computer. Figure 7.7 shows the security option policies, which are described briefly in Table 7.3.

FIGURE 7.7 The security option policies

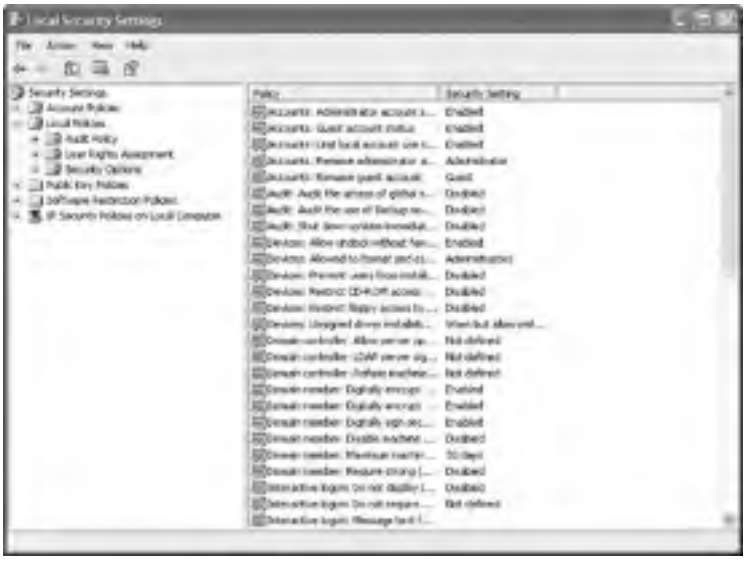


TABLE 7.3 Security Options

Option	Description	Default
Accounts: Administrator Account Status	Specifies whether the Administrator account is enabled or disabled under normal operation. Booting under Safe Mode, the Administrator account is enabled, regardless of this setting.	Enabled.
Accounts: Guest Account Status	Determines whether the Guest account is enabled or disabled.	Disabled.
Accounts: Limit Local Account Use of Blank Passwords to Console Logon Only	Means that if a user has a blank password, and this option is enabled, users can't use a blank password to log on from network logons. This setting does not apply to domain logon accounts.	Enabled.

TABLE 7.3 Security Options *(continued)*

Option	Description	Default
Accounts: Rename Administrator Account	Allows the Administrator account to be renamed.	Administrator account is named Administrator.
Accounts: Rename Guest Account	Allows the Guest account to be renamed.	Guest account is named Guest.
Audit: Audit the Access of Global System Objects	Allows access of global system objects to be audited.	Disabled.
Audit: Audit the use of Backup and Restore privilege	Allows the use of backup and restore privileges to be audited.	Disabled.
Audit: Shut Down System Immediately if Unable to Log Security Audits	Specifies that the system shuts down immediately if it is unable to log security audits.	Disabled.
Devices: Allow Undock without Having to Log On	Allows a user to undock a laptop computer from a docking station by pushing the computer's eject button without first having to log on.	Enabled.
Devices: Allowed to Format and Eject Removable Media	Specifies who can format and eject removable NTFS media.	Administrators.
Devices: Prevent Users from Installing Printer Drivers	If enabled, allows only Administrators and Power Users to install network print drivers.	Disabled on workstations and enabled on servers.
Devices: Restrict CD-ROM Access to Locally Logged-On User Only	Specifies whether the CD-ROM is accessible to local users and network users.	Disabled.
Devices: Restrict Floppy Access to Locally Logged-On User Only	Specifies whether the floppy drive is accessible to local users and network users.	Disabled.
Devices: Unsigned Driver Installation Behavior	Controls the behavior of the unsigned driver installation.	Warn but allow installation.
Domain Controller: Allow Server Operators to Schedule Tasks	Allows server operators to schedule specific tasks to occur at specific times or intervals. Only applies to tasks scheduled through the AT command and does not affect tasks scheduled through Task Scheduler.	Not defined.

TABLE 7.3 Security Options *(continued)*

Option	Description	Default
Domain Controller: LDAP server signing requirements	Specifies that the domain controller should use the Lightweight Directory Access Protocol for server signing.	Not defined.
Domain Controller: Refuse Machine Account Password Changes	Specifies whether a domain controller will accept password changes for computer accounts.	Disabled.
Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)	Specifies whether a secure channel must be created with the domain controller before secure channel traffic is generated.	Enabled.
Domain Member: Digitally Encrypt Secure Channel Data (when Possible)	Specifies that if a secure channel can be created between the domain controller and the domain controller partner, it will be.	Enabled.
Domain Member: Digitally Sign Secure Channel Data (when Possible)	Specifies that all secure channel traffic be signed if both domain controller partners who are transferring data are capable of signing secure data.	Enabled.
Domain Member: Disable Machine Account Password Changes	Specifies whether a domain member must periodically change its computer account password as defined in the "Domain Member: Maximum Age for Machine Account Password" setting.	Disabled.
Domain Member: Maximum Machine Account Password Age	Specifies the maximum age of a computer account password.	30 days.
Domain Member: Require Strong (Windows 2000 or Later) Session Key	If enabled, the domain controller must encrypt data with a 128-bit session key; if not enabled, 64-bit session keys can be used.	Disabled.
Interactive Logon: Do Not Display Last User Name	Prevents the last username in the logon screen from being displayed.	Disabled.

TABLE 7.3 Security Options *(continued)*

Option	Description	Default
Interactive Logon: Do Not Require Ctrl+Alt+Del	Allows the Ctrl+Alt+Delete requirement for logon to be disabled.	Not defined, but it is automatically used on standalone workstations. This means that users who log on to the workstation see a start screen with icons for all users who have been created on the computer.
Interactive Logon: Message Text for Users Attempting to Log On	Displays message text for users trying to log on, usually configured for displaying legal text messages.	Text space is blank.
Interactive Logon: Message Title for Users Attempting to Log On	Displays a message title for users trying to log on.	Not defined.
Interactive Logon: Number of Previous Logon Attempts to Cache (in Case Domain Controller Is Not Available)	Specifies the number of previous logon attempts stored in the cache. This option is useful if a domain controller is not available.	10.
Interactive Logon: Prompt User to Change Password before Expiration	Prompts the user to change the password before expiration.	14 days before password expiration.
Interactive Logon: Require Domain Controller Authentication to Unlock	Specifies that a username and password be required to unlock a locked computer. When this is disabled, a user can unlock a computer with cached credentials. When this is enabled, a user can only unlock the computer using a domain controller for authentication.	Disabled.
Interactive Logon: Smart Card Removal Behavior	Specifies what happens if a user who is logged on with a smart card removes the smart card.	No action.
Microsoft Network Client: Digitally Sign Communications (Always)	Specifies that the server should always digitally sign client communication.	Disabled.

TABLE 7.3 Security Options *(continued)*

Option	Description	Default
Microsoft Network Client: Digitally Sign Client Communication (if Server Agrees)	Specifies that the server should digitally sign client communication when possible.	Enabled.
Microsoft Network Client: Send Unencrypted Password to Connect to Third-Party SMB Servers	Allows third-party Server Message Block servers to use unencrypted passwords for authentication.	Disabled.
Microsoft Network Client: Amount of Idle Time Required before Idle before Suspending Session	Allows sessions to be disconnected when they are idle.	15 minutes for servers and undefined for workstations.
Microsoft Network Server: Digitally Sign Communications (Always)	Ensures that server communications will always be digitally signed.	Disabled.
Microsoft Network Server: Digitally Sign Communications (if Client Agrees)	Specifies that server communications should be signed when possible.	Disabled on workstations and enabled on servers.
Microsoft Network Server: Disconnect Clients when Logon Hours Expire	If a user logs on and then their logon hours expire, specifies whether an existing connection will remain connected or be disconnected.	Undefined.
Network Access: Allow Anonymous SID/Name Translation	Specifies whether an anonymous user can request the security identifier (SID) attributes for another user.	Disabled on workstations and enabled on servers.
Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts	If enabled, prevents an anonymous connection from enumerating Security Account Manager (SAM) accounts.	Enabled on workstations and disabled on servers.
Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts and Shares	If enabled, prevents an anonymous connection from enumerating Security Account Manager (SAM) accounts and network shares.	Disabled.
Network Access: Let Everyone Permission Apply to Anonymous Users	Specifies whether Everyone permissions will apply to anonymous users.	Disabled.

TABLE 7.3 Security Options *(continued)*

Option	Description	Default
Network Access: Named Pipes that Can Be Accessed Anonymously	Specifies which communication sessions will have anonymous access.	Defined.
Network Access: Remotely Accessible Registry Paths	Determines which Registry paths will be accessible when the winreg key is accessed for remote Registry access.	Defined.
Network Access: Shares that Can Be Accessed Anonymously	Specifies which network shares can be accessed by anonymous users.	Defined.
Network Access: Sharing and Security Model for Local Accounts	Specifies how network models that use local accounts will be authenticated.	Guest only—local users authenticate as Guest.
Network Security: Do Not Store LAN Manager Hash Value on Next Password Change	Specifies whether LAN Manager will store hash values from password changes.	Disabled.
Network Security: Force Logoff when Logon Hours Expire	Specifies whether a user with a current connection will be automatically logged off when their logon hours expire.	Disabled.
Network Security: LAN Manager Authentication Level	Specifies the LAN Manager Authentication Level.	Send LAN Manager and NTLM (NT LAN Manager) responses
Network Security: LDAP Client Signing Requirements	Specifies the client signing requirements that will be enforced for LDAP clients.	Negotiate signing.
Network Security: Minimum Session Security for NTLM SSP Based (Including Secure RPC) Clients	Specifies the minimum security standards for application-to-application client communications.	No minimum.
Network Security: Minimum Session Security for NTLM SSP Based (Including Secure RPC) Servers	Specifies the minimum security standards for application-to-application server communications.	No minimum.

TABLE 7.3 Security Options *(continued)*

Option	Description	Default
Recovery Console: Allow Automatic Administrative Logon	Specifies that when the Recovery Console is loaded, Administrative logon should be automatic, as opposed to a manual process.	Disabled.
Recovery Console: Allow Floppy Copy and Access to All Drives and Folders	Allows you to copy files from all drives and folders when the Recovery Console is loaded.	Disabled.
Shutdown: Allow System to Be Shut Down without Having to Log On	Allows the user to shut down the system without logging on.	Enabled on workstations and disabled on servers.
Shutdown: Clear Virtual Memory Pagefile	Specifies whether the virtual memory pagefile will be cleared when the system is shut down.	Disabled.
System Cryptography: Use FIPS Compliant Algorithms for Encryption	Specifies which encryption algorithms should be supported for encrypting file data.	Disabled.
System Objects: Default Owner for Objects Created by Members of the Administrators Group	Determines whether, when an object is created by a member of the Administrators group, the owner will be the Administrators group or user who created the object.	Object creator.
System Objects: Require Case Insensitivity to Non-Windows Subsystems	By default, Windows XP does not specify case insensitivity for file subsystems. However, subsystems such as POSIX use case-sensitive file systems, so this option allows you to configure case sensitivity.	Enabled.
System Objects: Strengthen Default Permissions of Internal System Objects (e.g. Symbolic Links)	Specifies the default discretionary access control list for objects.	Enabled.

The `Gpupdate /force` command can be used to force the group policies to be updated without waiting for the group policy refresh interval.

Analyzing and Troubleshooting Security Policies

You can analyze your system security by comparing your current configuration to a predefined template or through a customized template based on your organization's needs. This is accomplished through the `Secedit.exe` command-line utility or the *Security Configuration and Analysis tool*, which is a GUI interface implemented as an MMC snap-in.

The `Secedit` command-line utility can be used to perform the following options:

- Analyze security.
- Set security configuration options.
- Export a database of existing security configurations.
- Validate security settings based on predefined security templates.

The Security Configuration and Analysis utility works by comparing your actual security configuration to a security template configured with your desired settings.

The following steps are involved in the security analysis process:

1. Using the Security Configuration and Analysis tool, specify a working security database that will be used during the security analysis.
2. Import a security template that can be used as a basis for how you would like your security to be configured.
3. Perform the security analysis. This will compare your configuration against the template that you specified in step 2.
4. Review the results of the security analysis, and resolve any discrepancies that have been identified through the security analysis results.

The Security Configuration and Analysis tool is accessed as an MMC snap-in. After you add this utility to the MMC, you can use it to run the security analysis process, as described in the following sections.

To add the Security Configuration and Analysis tool, follow these steps:

1. Select Start ➢ Run ➢ MMC. The MMC will open and you will see a dialog box called Console1.
2. Select File ➢ Add/Remove Snap-In.
3. In the Add/Remove Snap-In dialog box, click the Add button. Highlight the Security Configuration and Analysis snap-in and click the Add button. Then click the Close button.
4. In the Add/Remove Snap-In dialog box, click the OK button.

Specifying a Security Database

The security database is used to store the results of your security analysis. To specify a security database, take the following steps:

1. In the MMC, right-click the Security Configuration and Analysis snap-in and select the Open Database option.

2. The Open Database dialog box appears. In the File Name text box, type the name of the database you will create. By default, this file will have an `.sdb` (for security database) extension. Then click the Open button.
3. The Import Template dialog box appears. Select the template that you want to import. You can select a predefined template through this dialog box. In the next section, you will learn how to create and use a customized template file. Make your selection and click the Open button.

Importing a Security Template

The next step in the security analysis process is to import a security template. The security template is used as a comparison tool. The Security Configuration and Analysis tool compares the security settings in the security template to your current security settings. You do not set security through the security template. Rather, the security template is where you organize all of your security attributes in a single location.

As an administrator, you can define a base security template on a single Windows XP Professional computer and then export the security template to other Windows XP Professional computers in your network.

The template you use can be one of the predefined user templates, a predefined template you have customized for your own needs, or a template you have defined from scratch. In the following sections, you will learn about the default templates that are provided with Windows XP Professional and how the templates can be modified.

CREATING A SECURITY TEMPLATE

By default, Windows XP Professional ships with a variety of predefined security templates. Each of the templates defines a standard set of security values based on the requirements of your environment. The template groups that are included by default are defined in Table 7.4.

TABLE 7.4 Default Security Templates

Template	Filename	Description
Default Security	`Setup security.inf`	Default security settings that are applied by default when a new computer is installed.
Compatible	`Compatws.inf`	Used for backward compatibility. This template relaxes the security used by Windows XP so applications that are not certified to work with Windows XP can still run. This template is typically associated with computers that have been upgraded and are having problems running applications that have run in the past.

TABLE 7.4 Default Security Templates *(continued)*

Template	Filename	Description
Secure	`Secure*.inf`	Implements recommended security settings for XP Professional in all security areas except for files, folders, and Registry keys.
High Secure	`Hisec*.inf`	Defines highly secure network communications for Windows XP computers. If you apply this security template, Windows XP computers can only communicate with other Windows 2000 Professional and Server, Windows XP (all versions), and Windows Server 2003 computers.
System Root Security	`Rootsec.inf`	Specifies that the new root permissions introduced with Windows XP be applied.

You create security templates through the Security Templates snap-in in the MMC. You can configure security templates with the items listed in Table 7.5.

TABLE 7.5 Security Template Configuration Options

Security Template Item	Description
Account Policies	Specifies configurations that should be used for password policies, account lockout policies, and Kerberos policies
Local Policies	Specifies configurations that should be used for audit policies, user rights assignments, and security options
Event Log	Allows you to set configuration settings that apply to Event Viewer log files
Restricted Groups	Allows you to administer local group memberships
Registry	Specifies security for local Registry keys
File System	Specifies security for the local file system
System	Sets security for system services and the startup mode that local system services will use

After you add the Security Templates snap-in to the MMC, you can open a sample security template and modify it, as follows:

1. In the MMC, expand the Security Templates snap-in and then expand the folder for `\Windir\Security\Templates`.
2. Double-click the sample template that you want to edit. There are several sample templates, including `securews` (for secure workstation) and `compatws` (for workstations that need backward-compatibility settings).
3. Make any changes you want to the sample security template. Changes to the template are not applied to the local system by default. They are simply a specification for how you would like the system to be configured.
4. Once you have made all of the changes to the sample template, save the template by highlighting the sample template file, right-clicking, and selecting the Save As option from the pop-up menu. Specify a location and a filename for the new template. By default, the security template will be saved with an `.inf` extension in the `\Windir\Security\Templates` folder.

OPENING A SECURITY TEMPLATE

Once you have configured a security template, you can import it for use with the Security Configuration and Analysis tool, assuming that a security database has already been configured. To import a security template, in the MMC, right-click the Security Configuration and Analysis tool and select the Import Template option from the pop-up menu. Then highlight the template file you wish to import and click the Open button.

Performing a Security Analysis

The next step is to perform a security analysis. To run the analysis, simply right-click the Security Configuration and Analysis tool and select the Analyze Computer Now option from the pop-up menu. You will see a Perform Analysis dialog box that allows you to specify the location and filename for the error log file path that will be created during the analysis. After this information is configured, click the OK button.

When the analysis is complete, you will be returned to the main MMC window. From there, you can review the results of the security analysis.

Reviewing the Security Analysis and Resolving Discrepancies

The results of the security analysis are stored in the Security Configuration and Analysis tool, under the configured security item. For example, to see the results for password policies, double-click the Security Configuration and Analysis tool, double-click Account Policies, and then double-click Password Policy.

The policies that have been analyzed will have an × or a √ next to each policy. An × indicates that the template specification and the actual policy do not match. A √ indicates that the template specification and the policy do match. If any security discrepancies are indicated, you should use the Group Policy snap-in to resolve the security violation.

Exam Essentials

Understand how group policies work within the Active Directory. Know the basics of Active Directory and how group policies are applied. Understand the difference between a GPO and a LGPO.

Know how to configure security policies. Know what security policies can be defined and what each security policy is used for.

Be able to analyze and troubleshoot security policies. Know the steps to perform a security analysis. Be able to use template files and know what templates are provided by default. Know what template is appropriate to use based on your security requirements.

Configure, Manage, and Troubleshoot Local User and Group Accounts

Windows XP supports two kinds of users: local users and domain users. A computer that is running Windows XP Professional has the ability to store its own user accounts database. The users stored at the local computer are known as *local user accounts*.

The *Active Directory* is a directory service that is available with the Windows Server 2003 and Windows 2000 Server platforms. It stores information in a central database that allows users to have a single user account for the network. The users stored in the Active Directory's central database are called *domain user accounts*.

If you use local user accounts, they must be configured on each computer that the user needs access to within the network. For this reason, domain user accounts are commonly used to manage users on large networks.

On Windows XP Professional computers and Windows Server 2003 and Windows 2000 Server member servers (a member server has a local accounts database and does not store the Active Directory), you create local users through the Local Users and Groups utility. On Windows Server 2003 and Windows 2000 Server domain controllers, you manage users with the Microsoft Active Directory Users and Computers utility.

Critical Information

To set up and manage users, you use the *Local Users and Groups* utility. With Local Users and Groups, you can create, disable, delete, and rename user accounts, as well as change user passwords.

The first step in working with Windows XP Professional user accounts is to access the Local Users and Groups utility. There are two common methods for doing so:

- You can load Local Users and Groups as an MMC snap-in.
- You can access the Local Users and Groups utility through the Computer Management utility.

Creating New Users

To create users on a Windows XP Professional computer, you must be logged on as a user with permissions to create a new user, or you must be a member of the Administrators group or Power Users group. Table 7.6 lists the options that are used when you create a new user.

TABLE 7.6 User Account Options Available in the New User Dialog Box

Option	Description
User Name	Defines the username for the new account. Choose a name that is consistent with your naming convention (e.g., WSmith). This is the only required field. Usernames are not case sensitive.
Full name	Allows you to provide more detailed name information. This is typically the user's first and last name (e.g., Wendy Smith). By default, this field contains the same name as the User Name field.
Description	Typically used to specify a title and/or location (e.g., Sales-Texas) for the account, but it can be used to provide any additional information about the user.
Password	Assigns the initial password for the user. For security purposes, avoid using readily available information about the user. Passwords can be up to 14 characters and are case sensitive.
Confirm password	Confirms that you typed the password the same way two times to verify that you entered the password correctly.
User must change password at next logon	If enabled, forces the user to change the password the first time they log on. This is done to increase security. By default, this option is selected.
User cannot change password	If enabled, prevents a user from changing their password. It is useful for accounts such as Guest and accounts that are shared by more than one user. By default, this option is not selected.
Password never expires	If enabled, specifies that the password will never expire, even if a password policy has been specified. For example, you might enable this option if this is a service account and you do not want the administrative overhead of managing password changes. By default, this option is not selected.
Account is disabled	If enabled, specifies that this account cannot be used for logon purposes. For example, you might select this option for template accounts or if an account is not currently being used. It helps keep inactive accounts from posing security threats. By default, this option is not selected.

Managing User Properties

For more control over user accounts, you can configure user properties. Through the user Properties dialog box, you can change the original password options, add the users to existing groups, and specify user profile information.

To open a user's Properties dialog box, access the Local Users and Groups utility, open the Users folder, and double-click the user account. The user Properties dialog box has tabs for the three main categories of properties: General, Member Of, and Profile.

The General tab, shown in Figure 7.8, contains the information that you supplied when you set up the new user account, including any Full Name and Description information, the password options you selected, and whether the account is disabled. If you want to modify any of these properties after you've created the user, simply open the user Properties dialog box and make the changes on the General tab.

The Member Of tab is used to manage the user's membership in groups. The Profile tab lets you set properties to customize the user's environment. These properties are discussed in detail in the following sections.

Managing User Group Membership

The Member Of tab of the user Properties dialog box displays all the groups that the user belongs to, as shown in Figure 7.9. From this tab, you can add the user to an existing group or remove that user from a group. To add a user to a group, click the Add button and select the group to which the user should belong. If you want to remove the user from a group, highlight the group and click the Remove button.

FIGURE 7.8 The General Of tab of the user Properties dialog box

Setting Up User Profiles, Logon Scripts, and Home Folders

The Profile tab of the user Properties dialog box, shown in Figure 7.10, allows you to customize the user's environment. Here, you can specify the following items for the user:

- User profile path
- Logon script
- Home folder

The following sections describe how these properties work and when you might want to use them.

FIGURE 7.9 The Member Of tab of the user Properties dialog box

FIGURE 7.10 The Profile tab of the user Properties dialog box

Setting a Profile Path

User profiles contain information about the Windows XP environment for a specific user. For example, profile settings include the desktop arrangement, program groups, and screen colors that users see when they log on.

Each time you log on to a Windows XP Professional computer, the system checks to see if you have a *local user profile* in the Documents and Settings folder, which was created on the boot partition when you installed Windows XP Professional.

The first time users log on, they receive a default user profile. A folder that matches the user's logon name is created for the user in the Documents and Settings folder. The user profile folder that is created holds a file called `NTUSER.DAT`, as well as subfolders that contain directory links to the user's desktop items.

Using Logon Scripts

Logon scripts are files that run every time a user logs on to the network. They are usually batch files, but they can be any type of executable file.

Setting Up Home Folders

Users normally store their personal files and information in a private folder called a *home folder*. In the Profile tab of the user Properties dialog box, you can specify the location of a home folder as a local folder or a network folder.

Troubleshooting User Accounts Authentication

When a user attempts to log on through Windows XP Professional and is unable to be authenticated, you will need to track down the reason for the problem. The following sections offer some suggestions that can help you troubleshoot logon authentication errors for local and domain user accounts.

Troubleshooting Local User Account Authentication

If a local user is having trouble logging on, the problem may be with the username, the password, or the user account itself. The following are some common causes of local logon errors:

Incorrect username You can verify that the username is correct by checking the Local Users and Groups utility. Verify that the name was spelled correctly.

Incorrect password Remember that passwords are case sensitive. Is the Caps Lock key on? If you see any messages relating to an expired password or locked-out account, the reason for the problem is obvious. If necessary, you can assign a new password through the Local Users and Groups utility.

Prohibitive user rights Does the user have permission to log on locally at the computer? By default, the Log On Locally user right is granted to the Users group, so all users can log on to Windows XP Professional computers. However, if this user right was modified, you will see an error message stating that the local policy of this computer does not allow interactive logon. The terms *interactive logon* and *local logon* are synonymous and mean that the user is logging on at the computer where the user account is stored on the computer's local database.

A disabled or deleted account You can verify whether an account has been disabled or deleted by checking the account properties through the Local Users and Groups utility.

A domain account logon at the local computer If a computer is a part of a domain, the logon dialog box has options for logging on to the domain or to the local computer. Make sure that the user has chosen the correct option.

Domain User Accounts Authentication

Troubleshooting a logon problem for a user with a domain account involves checking the same areas as you do for local account logon problems, as well as a few others.

The following are some common causes of domain logon errors:

Incorrect username You can verify that the username is correct by checking the Microsoft Active Directory Users and Computers utility to verify that the name was spelled correctly.

Incorrect password As with local accounts, check that the password was entered in the proper case (and make sure the Caps Lock key isn't on), the password hasn't expired, and the account has not been locked out. If the password still doesn't work, you can assign a new password through the Microsoft Active Directory Users and Computers utility.

Prohibitive user rights Does the user have permission to log on locally at the computer? This assumes that the user is attempting to log on to the domain controller. Regular users do not have permission to log on locally at the domain controller. The assumption is that users will log on to the domain from network workstations. If the user has a legitimate reason to log on locally at the domain controller, that user should be assigned the Log On Locally user right.

A disabled or deleted account You can verify whether an account has been disabled or deleted by checking the account properties through the Microsoft Active Directory Users and Computers utility.

A local account logon at a domain computer Is the user trying to log on with a local user account name instead of a domain account? Make sure that the user has selected to log on to a domain in the Logon dialog box.

The computer is not part of the domain. Is the user sitting at a computer that is a part of the domain to which the user is trying to log on? If the Windows XP Professional computer is not a part of the domain that contains the user account or does not have a trust relationship defined with the domain that contains the user account, the user will not be able to log on.

Unavailable domain controller, DNS Server, or Global Catalog Is the domain controller available to authenticate the user's request? If the domain controller is down for some reason, the user will not be able to log on until it comes back up (unless the user logs on using a local user account). A DNS Server and the Global Catalog for Active Directory are also required.

Creating and Managing Groups

Groups are an important part of network management. Many administrators are able to accomplish the majority of their management tasks through the use of groups; they rarely assign permissions to individual users. Windows XP Professional includes built-in local groups, such as Administrators and Backup Operators. These groups already have all the permissions needed to accomplish specific tasks. Windows XP Professional also uses default special groups, which

are managed by the system. Users become members of special groups based on their requirements for computer and network access.

You create and manage local groups through the Local Users and Groups utility. Through this utility, you can add groups, change group membership, rename groups, and delete groups.

To create a group, you must be logged on as a member of the Administrators group or the Power Users group. The Administrators group has full permissions to manage users and groups. The members of the Power Users group can manage only the users and groups that they create.

Creating groups is similar to creating users, and it is a fairly easy process. Access the Local Users and Groups utility, expand it to see the Users and Groups folders. Right-click the Groups folder and select New Group from the pop-up menu. This brings up the New Group dialog box.

The only required entry in the New Group dialog box is the group name. If appropriate, you can enter a description for the group, and you can add (or remove) group members. When you're ready to create the new group, click the Create button.

Configuring, Managing, and Troubleshooting Account Policy

Account policies are used to specify the user account properties that relate to the logon process. They allow you to configure computer security settings for passwords and account lockout specifications.

If security is not an issue—perhaps because you are using your Windows XP Professional computer at home—then you don't need to bother with account policies. If, on the other hand, security is important—for example, because your computer provides access to payroll information—then you should set very restrictive account policies.

To access the Account Policies folder from the MMC, follow this path: Local Computer Policy ➢ Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Account Policies. You will look at all these folders and how to use them throughout the rest of this chapter.

In the following sections, you will learn about the password policies and account lockout policies that define how security is applied to account policies.

Setting Password Policies

Password policies ensure that security requirements are enforced on the computer. It is important to understand that the password policy is set on a per-computer basis; it cannot be configured for specific users. Figure 7.11 shows the password policies, which are described in Table 7.7.

TABLE 7.7 Password Policy Options

Policy	Description	Default	Minimum	Maximum
Enforce Password History	Keeps track of user's password history	Remember 0 passwords	Same as default	Remember 24 passwords
Maximum Password Age	Determines maximum number of days user can keep valid password	Keep password for 42 days	Keep password for 1 day	Keep password for up to 999 days

TABLE 7.7 Password Policy Options *(continued)*

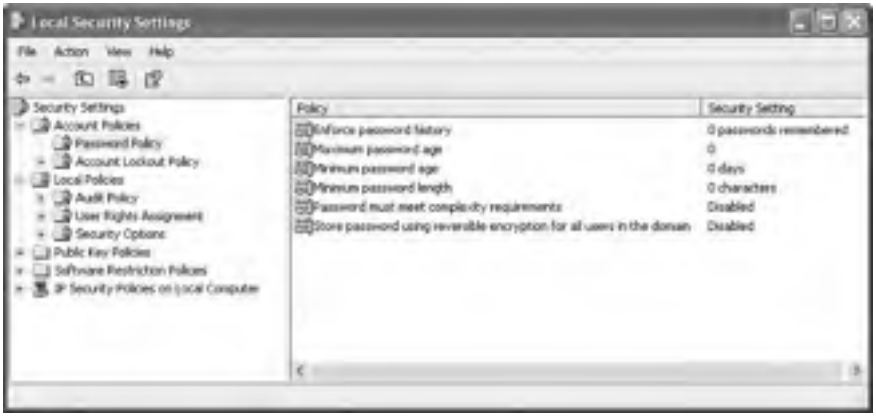
Policy	Description	Default	Minimum	Maximum
Minimum Password Age	Specifies how long password must be kept before it can be changed	0 days (password can be changed immediately)	Same as default	999 days
Minimum Password Length	Specifies minimum number of characters password must contain	0 characters (no password required)	Same as default	14 characters
Password Must Meet Complexity Requirements	Allows you to install password filter	Disabled		
Store Password Using Reversible Encryption for All Users in the Domain	Specifies higher level of encryption for stored user passwords	Disabled		

The password policies in Table 7.7 are used as follows:

Enforce Password History Prevents users from using the same password. Users must create a new password when their password expires or is changed.

Maximum Password Age Forces users to change their password after the maximum password age is exceeded.

FIGURE 7.11 The password policies



Minimum Password Age Prevents users from changing their password several times in rapid succession in order to defeat the purpose of the Enforce Password History policy.

Minimum Password Length Ensures that users create a password and specifies the length requirement for that password. If this option isn't set, users are not required to create a password at all.

Password Must Meet the Complexity Requirements of the Installed Password Filters Prevents users from using as passwords items found in a dictionary of common names.

Store Password Using Reversible Encryption for All Users in the Domain Provides a higher level of security for user passwords. This is required for Shiva Password Authentication Protocol (SPAP) authentication, which is used with remote access. This is primarily used with digest windows authentication through IIS.

Setting Account Lockout Policies

The *account lockout policies* are used to specify how many invalid logon attempts should be tolerated. You configure the account lockout policies so that after *x* number of unsuccessful logon attempts within *y* number of minutes, the account will be locked for a specified amount of time or until the Administrator unlocks the account.

Account lockout policies are similar to a bank's arrangements for ATM access code security. You have a certain number of chances to enter the correct PIN. That way, anyone who steals your card can't just keep guessing your access code until they get it right. Typically, after three unsuccessful attempts, the ATM takes the card. Then you need to request a new card from the bank.

Figure 7.12 shows the account lockout policies, which are described in Table 7.8.

FIGURE 7.12 The account lockout policies

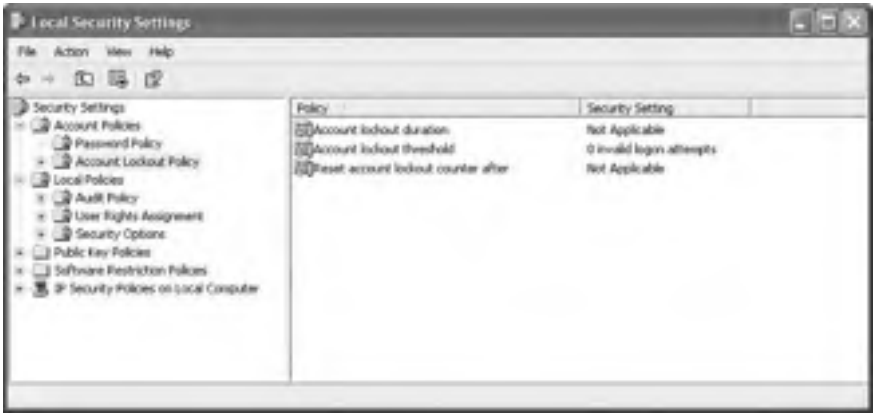


TABLE 7.8 Account Lockout Policy Options

Policy	Description	Default	Minimum	Maximum	Suggested
Account Lockout Duration	Specifies how long account will remain locked if Account Lockout Threshold is exceeded	0; but if Account Lockout Threshold is enabled, 30 minutes	Same as default	99,999 minutes	5 minutes
Account Lockout Threshold	Specifies number of invalid attempts allowed before account is locked out	0 (disabled, account will not be locked out)	Same as default	999 attempts	5 attempts
Reset Account Lockout Counter After	Specifies how long counter will remember unsuccessful logon attempts	0; but if Account Lockout Threshold is enabled, 5 minutes	Same as default	99,999 minutes	5 minutes

Using Local Policies

As you learned in the preceding section, account policies are used to control logon procedures. When you want to control what a user or group can do *after* logging on, you use *local policies*. With local policies, you can implement auditing, specify user rights, and set security options.

To use local policies, first add the Local Computer Policy snap-in to the MMC. Then, from the MMC, follow this path of folders to access the Local Policies folders: Local Computer Policy ➢ Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies.

Setting Audit Policies

Audit policies can be implemented to track success or failure of specified user actions. You audit events that pertain to user management through the audit policies. By tracking certain events, you can create a history of specific tasks, such as user creation and successful or unsuccessful logon attempts. You can also identify security violations that arise when users attempt to access system management tasks for which they do not have permission.

Users who try to go to areas for which they do not have permission usually fall into two categories: hackers and people who are just curious to see what they can get away with. Both are very dangerous.

When you define an audit policy, you can choose to audit success or failure of specific events. The success of an event means that the task was successfully accomplished. The failure of an event means that the task was not successfully accomplished.

By default, auditing is not enabled, and it must be manually configured. Once auditing has been configured, you can see the results of the audit through the Event Viewer utility, by selecting the Security log.

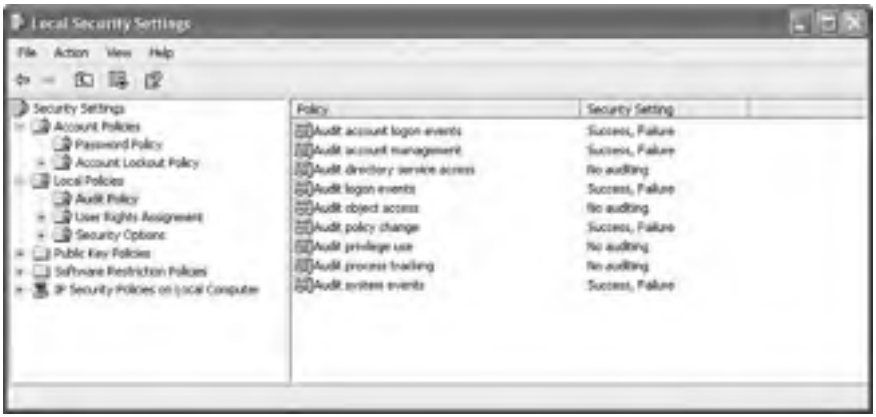
Figure 7.13 shows the audit policies, which are described in Table 7.9.

TABLE 7.9 Audit Policy Options

Policy	Description
Audit Account Logon Events	Tracks when a user logs on, logs off, or makes a network connection
Audit Account Management	Tracks user and group account creation, deletion, and management actions, such as password changes
Audit Directory Service Access	Tracks directory service accesses
Audit Logon Events	Audits events related to logon, such as running a logon script or accessing a roaming profile
Audit Object Access	Enables auditing of access to files, folders, and printers
Audit Policy Change	Tracks any changes to the audit policy
Audit Privilege Use	Tracks any changes to who can or cannot define or see the results of auditing
Audit Process Tracking	Tracks events such as activating a program, accessing an object, and exiting a process
Audit System Events	Tracks system events such as shutting down or restarting the computer, as well as events that relate to the Security log in Event Viewer

After you set the Audit Object Access policy to enable auditing of object access, you must enable file auditing through NTFS security or print auditing through printer security.

FIGURE 7.13 The audit policies



Assigning User Rights

The *user right policies* determine what rights a user or group has on the computer. User rights apply to the system. They are not the same as permissions, which apply to a specific object.

An example of a user right is the Back Up Files and Directories right. This right allows a user to back up files and folders, even if the user does not have permissions that have been defined through NTFS file system permissions. The other user rights are similar because they deal with system access as opposed to resource access.

Figure 7.14 shows the user right policies, which are described in Table 7.10.

TABLE 7.10 User Rights Assignment Policy Options

Right	Description
Access This Computer from the Network	Allows a user to access the computer from the network.
Act as Part of the Operating System	Allows low-level authentication services to authenticate as any user.
Add Workstations to Domain	Allows a user to create a computer account on the domain.
Adjust Memory Quotas for a Process	Allows you to configure how much memory can be used by a specific process. This is a new user right for Windows XP Professional.
Allow Logon through Terminal Services	Gives a user permission to log on through Terminal Services. This is a new user right for Windows XP Professional.

TABLE 7.10 User Rights Assignment Policy Options *(continued)*

Right	Description
Back Up Files and Directories	Allows a user to back up all files and directories, regardless of how the file and directory permissions have been set.
Bypass Traverse Checking	Allows a user to pass through and traverse the directory structure, even if that user does not have permissions to list the contents of the directory.
Change the System Time	Allows a user to change the internal time of the computer.
Create a Pagefile	Allows a user to create or change the size of a pagefile.
Create a Token Object	Allows a process to create a token if the process uses the NtCreateToken API.
Create Permanent Shared Objects	Allows a process to create directory objects through the Windows XP Object Manager.
Debug Programs	Allows a user to attach a debugging program to any process.
Deny Access to This Computer from the Network	Allows you to deny specific users or groups access to this computer from the network.
Deny Logon as a Batch Job	Allows you to prevent specific users or groups from logging on as a batch file.
Deny Logon as a Service	Allows you to prevent specific users or groups from logging on as a service.
Deny Logon Locally	Allows you to deny specific users or groups access to the computer locally.
Deny Logon through Terminal Services	Specifies that a user is not able to log on through Terminal Services. This is a new user right for Windows XP Professional.
Enable Computer and User Accounts to Be Trusted for Delegation	Allows a user or group to set the Trusted for Delegation setting for a user or computer object.
Force Shutdown from a Remote System	Allows the system to be shut down by a user at a remote location on the network.

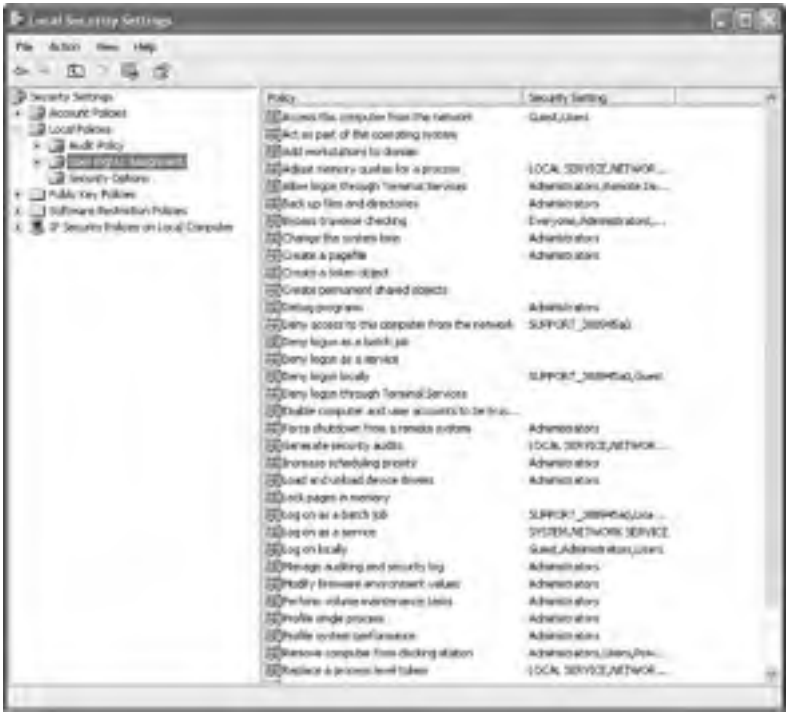
TABLE 7.10 User Rights Assignment Policy Options *(continued)*

Right	Description
Generate Security Audits	Allows a user, group, or process to make entries in the Security log.
Increase Scheduling Priority	Specifies that a process can increase or decrease the priority that is assigned to another process.
Load and Unload Device Drivers	Allows a user to dynamically unload and load Plug and Play device drivers.
Lock Pages in Memory	With this user right, an account can create a process that only runs in physical RAM and is not paged.
Log On as a Batch Job	Allows a process to log on to the system and run a file that contains one or more operating system commands.
Log On as a Service	Allows a service to log on in order to run the specific service.
Log On Locally	Allows a user to log on at the computer where the user account has been defined.
Manage Auditing and Security Log	Allows a user to manage the Security log.
Modify Firmware Environment Variables	Allows a user or process to modify the system environment variables.
Perform Volume Maintenance Tasks	Allows a user to perform volume maintenance tasks such as running Disk Cleanup and Disk Defragmenter. This is a new user right for Windows XP Professional.
Profile Single Process	Allows a user to monitor non-system processes through tools such as the Performance Logs and Alerts utility.
Profile System Performance	Allows a user to monitor system processes through tools such as the Performance Logs and Alerts utility.
Remove Computer from Docking Station	Allows a user to undock a laptop through the Windows XP user interface.

TABLE 7.10 User Rights Assignment Policy Options *(continued)*

Right	Description
Replace a Process Level Token	Allows a process to replace the default token that is created by the subprocess with the token that the process specifies.
Restore Files and Directories	Allows a user to restore files and directories, regardless of file and directory permissions.
Shut Down the System	Allows a user to shut down the local Windows XP computer.
Synchronize Directory Service Data	Allows a user to synchronize data associated with a directory service.
Take Ownership of Files or Other Objects	Allows a user to take ownership of system objects.

FIGURE 7.14 The user right policies



Troubleshooting Cache Credentials

When a user logon is successful, the logon credentials are saved to local cache. The next time the user attempts to log on, the cached credentials can be used to log on in the event that they can't be authenticated by a domain controller. By default, Windows XP will cache the credentials for the last 10 users that have logged on to the computer. If group policies have been updated and a user is using cached credentials, the new group policy updates will not be applied. If you want to force a user to log on using non-cached credentials you can set the number of cached credentials to 0 through group policy.

Exam Essentials

Know how to manage account settings. Be able to create users and groups and manage user properties.

Be able to manage account policies. Know what account polices can be defined for password and account lockout policies.

Be able to manage local policies. Know what local polices can be defined for audit policy and user right policies.

Configure, Manage, and Troubleshoot Internet Explorer Security Settings

Internet Explorer is used to access the Internet. Information is sent to websites and is sent back to the local computer. When you configure Internet Explorer settings you specify what can be accessed, what can be stored on your computer, and the level of security that is applied to the local computer.

Critical Information

Several options can be configured for Internet Explorer. You access Internet Properties by right-clicking Internet Explorer from the Start menu and selecting Internet Properties. This brings up the dialog box shown in Figure 7.15.

The options that can be configured are General, Security, Privacy, Content, Connections, Programs, and Advanced.

Configuring General Options

General properties are used to configure the home page, temporary Internet files, and history information. The Home Page section of this tab is used to configure the default home page that is displayed when you launch Internet Explorer. You can specify that you want to use the current home page for whatever is currently loaded, use the default home page that was preconfigured, or leave the option blank.

FIGURE 7.15 The Internet Options dialog box

The Temporary Internet Files options are used to manage cookies, files, and settings. Cookies are special files that are created by websites and they store information, such as the preferences you used when you visited the website. By choosing Delete Files, you delete any temporary Internet files that have been stored on your computer. This option is useful when you are low on disk space. The Settings button is used to configure options such as how your computer checks for newer versions of stored files and the location and amount of space that can be used by temporary Internet files.

The History options allow you to save all of the links to pages you have visited. By default, a history of all of the links you have accessed is kept for 20 days. You can customize how many days the history is stored or manually clear the history.

You can also set other options from the General tab that affect how Internet Explorer is customized, such as colors, fonts, languages, and accessibility options.

Configuring Security Options

The Security tab, as shown in Figure 7.16, allows you to configure the following options:

- The Internet content zones that can be used by the computer
- The local intranet zones that can be used by the computer
- The trusted sites that are allowed for the computer
- The restricted sites that are in effect for the computer

You set security zones by selecting the web content zone you want to configure, and then clicking the Sites button. The Custom Settings allow you to configure options such as whether you enable the downloading or use of signed or unsigned ActiveX controls. If you have configured your computer for security options and have specified security restrictions, you will receive an error message anytime you access a zone or site that is not configured for use with your computer.

Configuring Privacy Options

The Privacy tab, as shown in Figure 7.17, is used to configure privacy settings that relate to how third-party cookies are allowed to store information on your computer. You can select from different levels of security that range from blocking all cookies to allowing all cookies. When you click the Import button, you can import saved privacy settings from a predefined file. The Advanced button allows you to customize privacy settings. At the bottom of the screen, the Edit button for Web Sites allows you to customize privacy settings for specific websites.

FIGURE 7.16 The Security tab of the Internet Options dialog box

FIGURE 7.17 Internet Options, Privacy tab dialog box

Configuring Content-Related Options

The Content tab, as shown in Figure 7.18, is used to configure the options for Content Advisor, Certificates, and Personal Information.

Content Advisor

When you click the Enable button for Content Advisor, shown in Figure 7.19, you can set ratings of what can be viewed on the computer. This allows you to set flags to limit what is accessed based on language, nudity, sex, and violence on a sliding scale of acceptability. This option assumes that the website has been rated appropriately through the website configuration. The Approved Sites tab allows you to specifically define what sites are allowed or disallowed regardless of their content rating. The Content Advisor's General tab allows you to configure options to allow a supervisor to override content settings. The Advanced tab allows you to configure access for the ratings bureau you want to use for content ratings.

Certificates

Certificates are used to identify who you are based on a certificate that has been issued to you from a certification authority or certificate publisher. Through the Certificates section on the Content tab, you can Clear SSL State, configure Certificates, and configure Publishers.

With Secure Sockets Layer (SSL), any certificates that are used are automatically saved in SSL cache. The certificates are stored in SSL cache until the computer is restarted. If you need to use a new certificate, the Clear SSL Start button can be used to manually clear the SSL cache so that the new certificate can be used without restarting the computer.

FIGURE 7.18 The Content tab of the Internet Options dialog box

FIGURE 7.19 The Content Advisor dialog box

The Certificates option is used to require a trusted website to provide you, the client, with a valid certificate. This option is used to verify that the website being accessed can be authenticated through certificate services.

The Publishers button is used to configure all of the trusted publishers for the computer. You import a certificate from trusted publishers through the Import button in the Certificates dialog box.

Personal Information

The Personal Information section allows you to configure AutoComplete and use the Microsoft Profile Assistant. With AutoComplete, the entries you make are stored, and when you type in a few keystrokes of a new entry, AutoComplete will compare the new entry to the previous entries and try and make a match for you. Profile Assistant is used to store personal information about you.

Configuring Connections

The Connections tab, as shown in Figure 7.20, is used to configure what connection is used to access the Internet. This can be any connection you have created or a connection that is using Internet Connection Sharing. You can also configure proxy server settings and the LAN settings that are used by the Internet connection.

Dial-up settings include the following:

- Never Dial a Connection
- Dial Whenever a Network Connection Is Not Present
- Always Dial My Default Connection

FIGURE 7.20 The Connections tab of the Internet Options dialog box

LAN settings are used to define automatic configuration settings and proxy server settings (what the IP address for the proxy server is and the port that should be used). Proxy settings defined for the LAN do not apply to dial-up or VPN connections.

Configuring Program Options

The Programs tab, as shown in Figure 7.21, is used to configure what programs are associated with different Internet services. You can specify what programs are used for the following:

- HTML editor
- E-mail
- Newsgroups
- Internet call
- Calendar
- Contact list

When you click the Reset Web Settings button, Internet Explorer will default back to all of the default home and search page settings.

Configuring Advanced Options

The Advanced tab, as shown in Figure 7.22, is used to configure Internet Explorer options for accessibility, browsing, how links are underlined, HTTP settings, multimedia, printing, and security settings.

FIGURE 7.21 The Programs tab of the Internet Options dialog box

FIGURE 7.22 The Advanced tab of the Internet Options dialog box

Exam Essentials

Be able to configure Internet Explorer. Be able to configure and manage Internet Explorer settings, especially those related to security.

Review Questions

1. Who is created as the default data recovery agent (DRA) to recover encrypted files on a Windows XP Professional computer that is part of a Windows 2003 domain?
   - **A.** No default DRA is created
   - **B.** The local Administrator account
   - **C.** The user that created the encrypted file
   - **D.** The domain administrator
2. Which of the following commands is used to generate a recovery key agent that can be used to recover files that have been created through Encrypting File System (EFS)?
   - **A.** `Efs /r`
   - **B.** `Efs /k`
   - **C.** `Cipher /r`
   - **D.** `Ciper /k`
3. You are troubleshooting group policy inheritance. What is the order in which the GPOs will be applied?
   - **A.** Local computer, site, domain, OU
   - **B.** Site, local computer, domain, OU
   - **C.** Local computer, domain, OU, site
   - **D.** OU, domain, site, local computer
4. You are troubleshooting group policies. You want to see what policies have been applied to the current user. Which of the following command-line utilities should you use?
   - **A.** `GPO.exe`
   - **B.** `GPmanage.exe`
   - **C.** `GRP.exe`
   - **D.** `GPResult.exe`
5. You have just updated the group policy settings on your computer. The policies do not seem to be taking effect. Which of the following commands should you use to force the update?
   - **A.** `Gpupdate /force`
   - **B.** `GPResult /f`
   - **C.** `GPO /update`
   - **D.** `Secedit /refreshpolicy`

6. You have just upgraded your computer to Windows XP Professional. After the upgrade one of your applications will not work. You suspect that the problem is due to the new Group Policy settings. Which of the following templates should you apply for backward compatibility?
   - **A.** `Compatws.inf`
   - **B.** `Secure.inf`
   - **C.** `Hisec.inf`
   - **D.** `Rootsec.inf`

7. Which user right would you grant to a user who needs to be able to log on to the local computer where the user account is stored?
   - **A.** Log On at Current Computer
   - **B.** Log On Locally
   - **C.** Allow Private Logon
   - **D.** Allow Local Logon

8. You have a user who performs a local backup on your Windows XP Professional computer. The user needs to be able to eject the tapes when the backups are complete. Which security policy should you apply for this user?
   - **A.** Devices: Allowed to Format and Eject Removable Media
   - **B.** Backup: Allowed to Eject Backup Media
   - **C.** Backup: Allowed to Insert and Remove Media
   - **D.** Devices: Allowed to Insert and Eject All Media

9. You have a computer that is used to process payroll checks that should be configured with high security. You want to ensure that no users can access the computer from the network. Which of the following user rights should you configure?
   - **A.** Logon Locally
   - **B.** Access to This Computer from the Network
   - **C.** Logon from the Network
   - **D.** Network Access

10. You want to prevent employees from viewing offensive material on company computers. Which of the following options should you configure through Internet Explorer?
    - **A.** Privacy Settings
    - **B.** Content Advisor
    - **C.** Sites Allowed
    - **D.** Personal Information

Answers to Review Questions

1. D. For Windows XP Professional computers that are a part of a Windows 2000 or Windows 2003 Active Directory domain, the domain Administrator user account is automatically assigned the role of DRA.

2. C. The `Cipher /r` command is used to generate a recovery agent key and certificate for use with EFS. This is used to recover the data in the event that the person who encrypted the data is unavailable.

3. A. When GPOs are created within Active Directory, there is a specific order of inheritance. That is, the policies are applied in a specific order within the hierarchical structure of Active Directory. When a user logs on to Active Directory, depending on where within the hierarchy GPOs have been applied, the order of application is as follows: 1. Local computer, 2. Site (group of domains), 3. Domain, 4. OU.

4. D. To help determine what policies will actually be applied, Windows XP includes a tool called the Windows XP Operating System *Group Policy Result Tool*. This tool is accessed through the `GPResult.exe` command-line utility. The `GPResult.exe` command displays the resulting set of policies that were enforced on the computer and the specified user during the logon process.

5. A. The `Gpupdate /force` command can be used to force the group policies to be updated without waiting for the group policy refresh interval.

6. A. The `Compatws.inf` template is used for backward compatibility. This template relaxes the security used by Windows XP so applications that are not certified to work with Windows XP can still run. This template is typically associated with computers that have been upgraded and are having problems running applications that have run in the past.

7. B. The Log On Locally user right allows a user to log on at the computer where the user account has been defined.

8. A. The Devices: Allowed to Format and Eject Removable Media security policy specifies who can format and eject removable NTFS media.

9. B. The Access to This Computer from the Network user right specifies what users or groups can access a computer from the network.

10. B. Content Advisor allows you to set ratings of what can be viewed on the computer. This allows you to set flags to limit what is accessed based on language, nudity, sex, and violence on a sliding scale of acceptability. This option assumes that the website has been rated appropriately through the website configuration.

Index

Note to the reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z