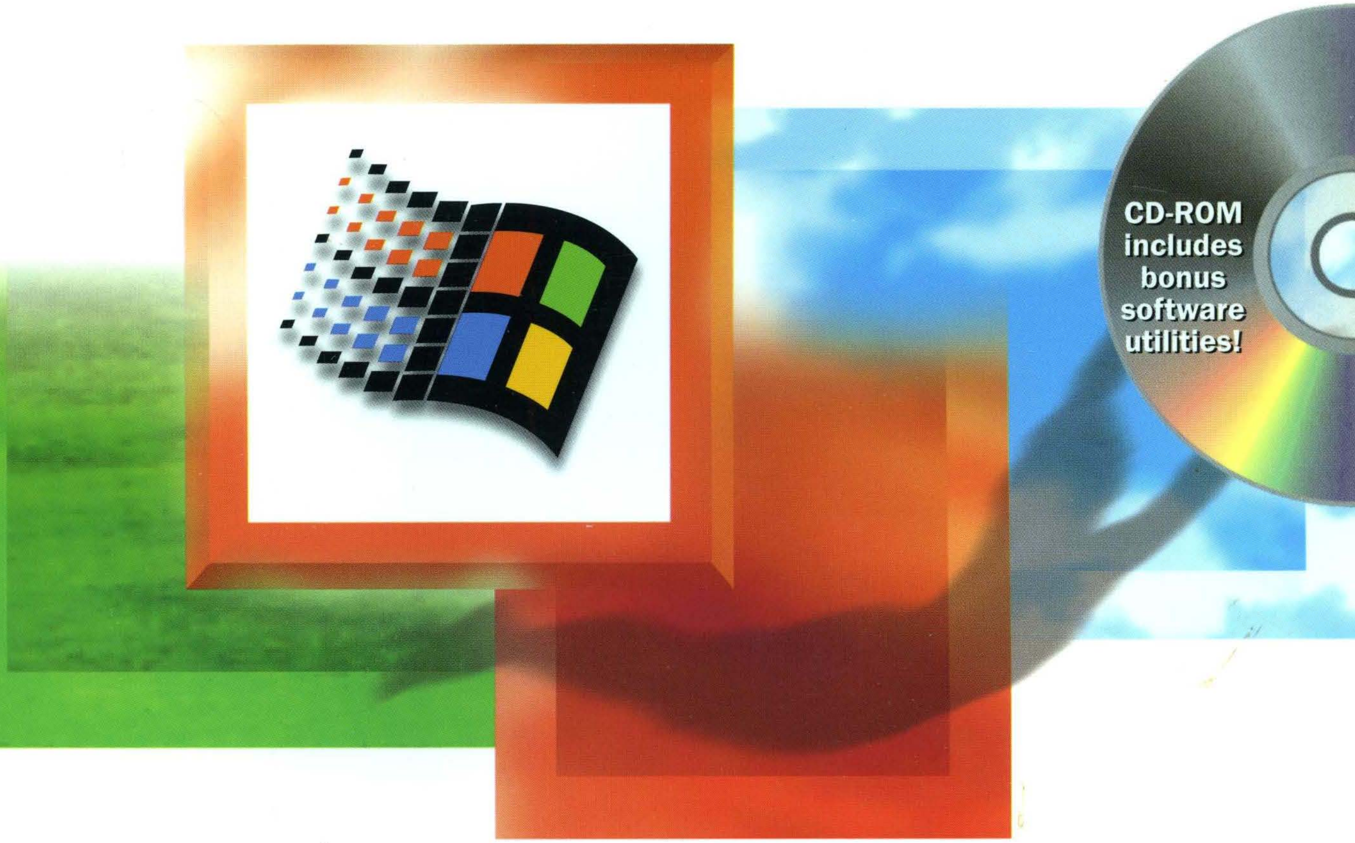
Microsoft®



Microsoft® Windows® 2000 Professional Expert Companion

Tips, Tricks, and Utilities for the Power User

Craig Stinson and Carl Siechert

Microsoft®

Microsoft® Windows® 2000 Professional Expert Companion

Craig Stinson and Carl Siechert

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

Library of Congress Cataloging-in-Publication Data pending.

Printed and bound in the United States of America.

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

Distributed in Canada by Penguin Books Canada Limited.

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

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at mspress.microsoft.com. Send comments to *mspinput@microsoft.com.*

Unless otherwise noted, the example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

Acquisitions Editor: Christey Bahn
Project Editor: Kim Fryer

Acknowledgments

Throughout many years and many changes, the folks at Microsoft Press have remained the best to work with.

Christey Bahn and Barb Ellsworth kicked off this project by helping us define the scope and content. Later on, Christey navigated the vast hallways of Microsoft to obtain permissions for various items on the companion CD—not a trivial task. Working with our old friend Kim Fryer in her new role as project editor was a delight. She managed to keep our feet to the fire in a way that actually felt good, like sitting by a blazing woodstove on a chilly night.

We also had some expert help with the writing. Chris Wood—the other half of Siechert & Wood Professional Documentation—wrote the bulk of Part 9, including the example programs, and some of Part 6. More important, he kept our other clients satisfied as he juggled multiple projects while Carl remained focused (mired?) in books about Windows 2000. Our colleague Blake Wesley Whittington wrote much of Part 7 and designed the companion CD. In addition, he taught us a lot during his tenure at Siechert & Wood, which concluded with the completion of this book.

Our thanks go to Jimmie Young, of ProImage, for managing the production of this book. And to the excellent editorial team he assembled: Mary Renaud, Susan Christopherson, Nancy Albright, and Allen L. Wyatt.

Those are the people whose fingerprints are somewhere on the manuscript. But we'd never be able to do this kind of work without the continuing love and support of our families. Jan, Jean, Russell, Miranda: we love ya!

Contents at a Glance

Part 1 **Setting Up and Starting Up**

Chapter 1 Installing Windows 2000 3

Chapter 2 Setting Startup Options 31

Chapter 3 Working with Multiple Operating Systems 47

Part 2 **Using Management Tools**

Chapter 4 Using and Customizing Microsoft Management Console 67

Chapter 5 Monitoring System and Application Activities with Event Viewer 83

Chapter 6 Finding Files with the Indexing Service 95

Chapter 7 The Windows 2000 Shell: Beyond the Basics 117

Part 3 **Managing Programs**

Chapter 8 Running Programs 133

Chapter 9 Installing and Removing Programs and System Components 145

Chapter 10 Using Programs for Other Operating Systems 153

Chapter 11 Using the Command Prompt 171

Part 4 **Managing Hardware**

Chapter 12 Managing Disks 197

Chapter 13 Managing a Print Server 221

Chapter 14 Using Removable Storage 235

Chapter 15 Power Management 257

Chapter 16 Using Device Manager and Hardware Profiles 269

Part 5 **Administering a System**

Chapter 17 Managing Users and Groups 283

Chapter 18 Using Group Policy 297

Chapter 19 Customizing Users Work Environments 311

Chapter 20 Managing Services 331

Chapter 21 Administering Remote Systems 347

Part 6 Managing Networks

Chapter 22 Making Network Connections 361
Chapter 23 Working with Shared Folders 371
Chapter 24 TCP/IP Core Networking Guide 387

Part 7 Using the Internet

Chapter 25 Making Internet Connections 415
Chapter 26 Internet Explorer: Beyond Browsing 435
Chapter 27 Managing a Web Server 463
Chapter 28 Managing Incoming Connections 485
Chapter 29 Communicating Over the Internet 501
Chapter 30 Using Telnet 515
Chapter 31 Using the FTP Clients 525

Part 8 Managing Security

Chapter 32 Using the NTFS File System 539
Chapter 33 Using Encryption 555
Chapter 34 Auditing Security 573
Chapter 35 Managing Security Certificates 583

Part 9 Automating Tasks

Chapter 36 Using Doskey Macros 599
Chapter 37 Using Batch Programs 609
Chapter 38 Using Windows Script Host 627

Part 10 Maintaining and Optimizing

Chapter 39 Working with the Registry 655
Chapter 40 Performing Routine Maintenance 669
Chapter 41 Viewing System Information 679
Chapter 42 Troubleshooting 689
Chapter 43 Monitoring System Performance 713

Part 11 Appendixes

Appendix A Companion CD Contents 741
Appendix B Windows 2000 Professional CD Contents 743

Table of Contents

Acknowledgments . . . . *iii*
Introduction . . . . *xv*

Part 1 Setting Up and Starting Up

Chapter 1 Installing Microsoft Windows 2000 3

Preparing for Installation 4
Installing on a Single Computer 12
Automating the Installation Process 14
Installing Other Programs as Part of Setup 26

Chapter 2 Setting Startup Options 31

Setting Pre-Logon Options 31
Setting Logon Options 37
Setting Up Recovery Console 42
Booting from Floppy Disks 42

Chapter 3 Working with Multiple Operating Systems 47

Understanding How Dual Booting Works 48
Understanding the Limitations of Dual Boot Setups 49
Adding an Operating System 53
Removing an Operating System 60
Using Third-Party Alternatives 62

Part 2 Using Management Tools

Chapter 4 Using and Customizing Microsoft Management Console 67

Running MMC Consoles 69
Using MMC Consoles 71
Creating Your Own MMC Consoles 73

Chapter 5 Monitoring System and Application Activities with Event Viewer 83

Running Event Viewer 85
Examining Event Details 87
Filtering the Log Display 88
Using Multiple Views of the Same Log 89
Searching for an Event 89
Setting Log-File Size and Longevity 90

Archiving and Clearing Log Files 91
Displaying an Archived Log File 91
Exporting Log-File Information 92
Backing Up Log Files 92
Monitoring Events on Remote Computers 93

Chapter 6 Finding Files with the Indexing Service 95

Security and the Indexing Service 96
Limitations of the Indexing Service 97
Activating the Indexing Service 98
Submitting Queries 99
Administering the Indexing Service 110

Chapter 7 The Windows 2000 Shell: Beyond the Basics 117

Removing Impediments 117
Using Cascading Folder Menus 123
Using Windows Explorer's Command-Line Syntax 124
Relocating Shell Folders 126
Adding or Changing Shortcut Menu Commands 128
Using Third-Party Shell Tools 130

Part 3 **Managing Programs**

Chapter 8 Running Programs 133

Using Command Lines, Paths, and MRUs 133
Controlling Programs and Services that Start at Logon 135
Scheduling Tasks 137
Running a Program Under a Different User Account 142
Downloading Compatibility Updates 143
Using Apcompat to Solve Compatibility Problems 143

Chapter 9 Installing and Removing Programs and System Components 145

The Benefits of the Windows Installer 145
Windows File Protection 147
Using Add/Remove Programs 147
Installing Programs Under a Different User Account 151
Creating MSI Files for Legacy Applications 151

Chapter 10 Using Programs Written for Other Operating Systems 153

Running Windows 3.x–Based Programs 154
Running MS-DOS-Based Applications 157
Running POSIX-Based Applications 169

Chapter 11 Using the Command Prompt 171

Starting and Ending a Command Prompt Session 172
Customizing Command Prompt Windows 174
Starting Programs 178
Using Commands 179
Using Environment Variables 185
Starting Command Prompt and Running a Command 187
Using AutoRun to Execute Commands When Command Prompt Starts 188
Using File and Folder Name Completion 189
Using Command Extensions 190
Using Cmd's Command-Line Syntax 190
Using Network Commands 191

Part 4 Managing Hardware

Chapter 12 Managing Disks 197

Using Disk Management 197
Understanding Disk Terminology 201
Working with Basic Disks 205
Working with Dynamic Disks 211
Performing Other Tasks 213

Chapter 13 Managing a Print Server 221

Sharing a Printer 221
Setting Printer Permissions 223
Setting Advanced Printer Properties 224
Using Separator Pages 227
Setting Up a Printer That's Connected Directly to the Network 228
Setting Up a Printer for Non–Windows 2000 Clients 229
Setting Server Properties 232

Chapter 14 Using Removable Storage 235

Getting Started with Removable Storage 236
Setting Up and Using Media Pools 237
Using Hardware Devices 241
Securing Devices and Media 251
Using Backup with Removable Storage 252

Chapter 15 Power Management 257

ACPI and APM—What's the Difference? 257
Enabling APM Power Management 260
Configuring Power-Management Features 261
Troubleshooting Power Management 266

Chapter 16 Using Device Manager and Hardware Profiles 269
Running Device Manager . . . 270
Viewing and Printing Your System's Configuration . . . 270
Changing a Device's Configuration . . . 274
Updating or Changing Device Drivers . . . 275
Understanding Device Manager's Error Codes . . . 278
Using Hardware Profiles . . . 279

Part 5 Administering a System

Chapter 17 Managing Users and Groups 283
Local Accounts vs. Domain Accounts . . . 283
Setting Up Local Users and Groups . . . 286
Setting Security for Users and Groups . . . 293

Chapter 18 Using Group Policy 297
Starting Group Policy . . . 298
Understanding the Local Group Policy Object . . . 301
Making Settings . . . 305
Making Different Settings for Different Users . . . 307

Chapter 19 Customizing User Work Environments 311
Understanding User Profiles . . . 312
Working with User Profiles . . . 316
Using Scripts That Run at Logon, Logoff, Startup, and Shutdown . . . 320
Using IntelliMirror Features Without Windows 2000 Server . . . 322

Chapter 20 Managing Services 331
Using the Services Snap-In . . . 331
Managing Services from a Command Prompt . . . 341
Adding and Removing Services . . . 341
Services Included with Windows 2000 Professional . . . 342

Chapter 21 Administering Remote Systems 347
Requirements for Remote Administration . . . 347
Using Computer Management . . . 348
Using Other MMC Consoles and Snap-Ins . . . 351
Managing Printers Remotely . . . 354
Editing a Remote Registry . . . 354
Setting Up Scheduled Tasks . . . 354
Using Command-Line Utilities . . . 355
Administering a Domain . . . 356

Part 6 Managing Networks

Chapter 22 Making Network Connections 361

Setting Up a Peer-to-Peer Network 361
Securing a Peer-to-Peer Network 368

Chapter 23 Working with Shared Folders 371

Using the Shared Folders Snap-In 371
Offline Files and Caching 376
Command-Line Utilities 380

Chapter 24 TCP/IP Core Networking Guide 387

Introduction to TCP/IP 387
Modifying Your TCP/IP Configuration 397
Using Tools for Network Troubleshooting 406
Setting Advanced Options 409
Setting Up Non-TCP/IP Connections 411

Part 7 Using the Internet

Chapter 25 Making Internet Connections 415

Creating Dial-Up Connections 416
Connecting to the Internet Through a LAN 418
Using Cable and DSL Connections 421
Configuring TCP/IP 422
Sharing an Internet Connection 423
Securing Your Internet Connection 428

Chapter 26 Internet Explorer: Beyond Browsing 435

Downloading from the Internet 435
Using Security and Privacy Features 440
Customizing Internet Explorer 446

Chapter 27 Managing a Web Server 463

Installing Internet Information Services 464
Using IIS 465
Managing Security on Your Site 472
Redirecting Requests to the Site 482
Using Content Ratings 482
Running an FTP Server 482
Using Your Web Site for Collaboration (WebDAV) 483
Setting Up IIS for Internet Printing 483

Chapter 28 Managing Incoming Connections 485

Creating Incoming Connections 486
Understanding Tunnels and Virtual Private Networks 489
Using IPSec 490

Chapter 29 Communicating Over the Internet 501

Using NetMeeting 502
Using Internet Instant Messaging 512

Chapter 30 Using Telnet 515

Using the Telnet Clients 516
Running a Telnet Server 521

Chapter 31 Using the FTP Clients 525

Understanding FTP 525
Using the Command-Line FTP Client 527
Using the Graphical FTP Client in Windows Explorer 534
Using the Text-Based FTP Client in Internet Explorer 535

Part 8 **Managing Security**

Chapter 32 Using the NTFS File System 539

Selecting a File System 539
Securing Folders and Files 544
Using Volume Mount Points to Create Mounted Drives 548
Enforcing Disk Quotas 550

Chapter 33 Using Encryption 555

Installing the High Encryption Pack 555
Encrypting Folders and Files 557
Backing Up Your Certificates 564
Recovering Encrypted Files and Folders 568
Disabling or Reenabling EFS 569

Chapter 34 Auditing Security 573

About Auditing 573
Viewing Audit Events 575
Enabling Auditing 576
Auditing File and Folder Access 578
Auditing Access to Printers 580

Chapter 35 Managing Security Certificates 583

Understanding Digital Certificates 584
Using the Certificates Dialog Box 591

Using the Certificates Snap-in 592
Signing and Encrypting E-mail Messages 595

Part 9 **Automating Tasks**

Chapter 36 Using Doskey Macros 599
Defining Macros 600
Managing Macros 600
Placing Comments in Macro Files 601
Using Parameters in Macros 601
Using Symbols in Macros 602
Replacing Windows 2000 Commands with Doskey Macros 604
Understanding Doskey Switches 606
Using Doskey Macros in Programs 606

Chapter 37 Using Batch Programs 609
Understanding Batch Program Basics 610
Using Batch Commands 610
Learning from a Simple Batch Program 612
Creating More Complex Batch Programs 615
Using Other Batch Program Tricks 624

Chapter 38 Using Windows Script Host 627
Finding Scripting Resources 628
Wscript vs. Cscript 628
Choosing a Scripting Language 629
Using the Script File Format 631
Debugging Scripts 632
Introducing Objects 637
Example Scripts 640

Part 10 **Maintaining and Optimizing**

Chapter 39 Working with the Registry 655
How the Registry Is Structured 656
Backing Up and Restoring the Registry 659
Regedit vs. Regedt32 660
Editing the Registry 661
Changing Registry Key Permissions 665
Working with a Remote Computer's Registry 666
Monitoring Changes to Your Registry 666

Chapter 40 Performing Routine Maintenance 669

Freeing Up Disk Space 669
Optimizing Disk Performance with Disk Defragmenter 672
Checking Disks for File-System and Media Errors 675
Using Windows Update to Maintain Driver and System Files 676
Backing Up 677
Keeping an Up-to-Date Emergency Repair Disk 678

Chapter 41 Viewing System Information 679

Browsing Your System 680
Exporting System Information 684
Opening and Closing Saved System Information Files 684
Running System Information from a Command Prompt 685

Chapter 42 Troubleshooting 689

Preparing for Disaster 690
Troubleshooting Tools Supplied with Windows 2000 692
Using the Windows Support Tools 700
Troubleshooting Resources Available on the Internet 704
What to Do If Your System Won't Start 706

Chapter 43 Monitoring System Performance 713

Monitoring Performance and Managing Applications with Windows Task Manager 714
Monitoring and Logging Performance with the Performance Console 722
What to Monitor 735

Part 11 Appendixes

Appendix A Companion CD Contents 741

Installing and Using Programs from the CD 741

Appendix B Windows 2000 Professional CD Contents 743

Value Added Folder 744
Learning More About Files Installed from the CD 746

Index 749

Introduction

When we first tackled this assignment, our goal was to fill the gap between *Running Microsoft Windows 2000 Professional* (our book for novice and intermediate end users of Windows 2000 Professional) and the *Microsoft Windows 2000 Professional Resource Kit* (a book for IT administrators). We were a little skeptical at first about whether this "reader space" would allow us enough material to fill a book.

What we envisioned as a narrow niche, however, turned out to be a gaping gorge. The more we used Microsoft Windows 2000—in everyday computing as well as research for this book—the more complexity we discovered.

In retrospect, we shouldn't have been so surprised. The paradox of software progress—for Microsoft software, at any rate!—is that simplicity and convenience for end users are achieved only through feature elaboration and internal complexity. As Microsoft's operating systems become easier for novices, they also become more replete with features to interest and challenge expert users. And for whatever reasons (fill in the blank here with your own guess or theory), the mysteries of Windows—those little things that confound and astound—will apparently always be with us, no matter how friendly and solid the operating system becomes.

In the end, we had to be quite selective about the information we included, and we pared our outline down to those topics we thought would be of most interest to you, the expert user. In doing so, we assumed that you already knew a lot about Windows, although not necessarily about the NT platform. Because this is a book about Windows 2000 Professional, not one of the server editions of Windows 2000, we also assumed that you were interested as much in end-user issues as in administrative matters—although you might well be in charge of a small business network, including one or more machines running Windows 2000 Server. We imagined that you might be the Windows guru for a department or a company. Above all, we pictured you as a person of intelligence and curiosity, eager to learn as much as possible about the operating system with which you live and work.

We arrived at a book in ten parts. Part 1 addresses setup issues. Part 2 is an overview of the management tools included with Windows 2000 Professional. Parts 3 and 4 deal with the management of software and hardware, respectively. Part 5 covers system administration—setting up groups and users, establishing policy, and so on. Part 6 is a guide to the higher levels of network plumbing under Windows 2000. Part 7 addresses the Internet, Part 8 discusses security matters, Part 9 details ways to automate tasks in Windows 2000, and Part 10 takes up maintenance and optimization.

The numbering of parts and chapters implies a linear organization, but we intended this to be a random-access book. If you're just setting up Windows 2000 or have only recently done so, you might want to begin with the setup chapters in Part 1. Beyond that, however, we hope you'll let your own needs and curiosity (with the help of our index and table of contents) be your guide.

On the CD-ROM that accompanies the book, you'll find programs (or links to programs) from Microsoft and third parties that we regard as valuable additions to your Windows 2000 toolkit. The CD also offers supplemental information of interest, including all the articles from Microsoft's Knowledge Base that are mentioned in this book.

This book is finished—at least for now! But we continue to discover new things about Windows 2000. If you have discoveries of your own to share or questions to ask, we invite you to contact us at *craigstinson@free-market.net* and *carl@swdocs.com.*

Part 1

Setting Up and Starting Up

Chapter 1
Installing Microsoft Windows 2000 3

Chapter 2
Setting Startup Options 31

Chapter 3
Working with Multiple Operating Systems 47

Chapter 1

Installing Microsoft Windows 2000

In This Chapter

Preparing for Installation 4
Installing on a Single Computer 12
Automating the Installation Process 14
Installing Other Programs as Part of Setup 26

The basic setup process for Microsoft Windows 2000 Professional has been considerably streamlined from the process used for earlier versions of Windows and Windows NT. With just a little bit of luck, you can successfully employ the typical "expert" approach: without reading a thing, tear off the shrink wrap, insert the CD into the drive, and click OK a few times. In fact, dyed-in-the-wool experts will be disappointed to see that the program provides no choice for Typical or Custom setup. (No real expert ever settles for Typical.)

Although setting up Windows 2000 Professional on a single computer has been reduced to an easy and (usually) trouble-free experience, the setup process offers a number of options that aren't readily apparent. These include options to automate installation. Microsoft has produced reams of information about "deploying" Windows 2000 throughout large enterprises, including all the necessary preparation and procedures. In this chapter, we distill that voluminous information to the essentials you need to know to automate installation in a small office. Along with a list of items to check before you begin installation, the automated installation options are the subject of this chapter.

Preparing for Installation

Before you install Windows 2000, you'll want to be sure that you have all the requisite information and that your computer is properly configured. You should

- Confirm that your computer meets the hardware requirements
- Check hardware and software compatibility
- Back up your files and configuration information
- Prepare the computer by uncompressing drives and disabling incompatible services
- Create a computer account on the domain controller
- Choose between upgrade and clean installation

Checking Hardware Requirements

Windows 2000 Professional requires processor speed, memory, and disk space in amounts that were unheard of only a few years ago. Your computer needs to meet the following minimum hardware requirements:

- A Pentium or higher processor (or equivalent), 133 megahertz (MHz) or faster. (The Setup program doesn't actually enforce the processor speed requirement, but you aren't likely to be satisfied running Windows 2000 on a slower system.) Windows 2000 Professional supports up to two processors on a single computer.
- 32 megabytes (MB) of random access memory (RAM). You probably won't be happy with less than 64 MB of RAM; more is better. Windows 2000 supports up to 4 gigabytes (GB).
- A hard disk with at least 650 MB of free space. (If you're installing from a shared network folder, you'll need approximately 300 MB of additional free space for temporary files.)
- A VGA or higher-resolution monitor.
- A keyboard.
- A Microsoft Mouse or compatible pointing device.

To install from the Windows 2000 Professional CD, you'll also need

- A CD-ROM or DVD drive
- A high-density 3.5-inch floppy disk drive (unless your computer's BIOS allows it to start from a bootable CD)

To install from a shared network folder, you'll also need

- A network adapter card compatible with Windows 2000
- Access to the network share that contains the setup files

Checking for Hardware and Software Compatibility

Windows 2000 Setup checks your hardware and software for compatibility and reports any problems. Before you begin, however, you might want to do your own review, particularly if you're planning to upgrade computers running Windows 9x. (If your computer is already running Windows NT, its hardware and most of its software are almost certainly compatible with Windows 2000.)

Checking Hardware Compatibility

Windows 2000 provides support for a wide variety of hardware—a much wider variety than its predecessor, Windows NT. Nonetheless, checking the Hardware Compatibility List (HCL) to see whether all your devices are supported is a good idea. You can find a text version in the \Support folder of the Windows 2000 Professional CD; an updated version is available at *www.microsoft.com/hcl*. In addition to its frequent updates, the Web version has other advantages: it's searchable, and when you find the item you're interested in, you can click its logo for more detailed support information and, in some cases, updated drivers.

An item's appearance on the HCL is no guarantee that it'll work properly in your configuration, and its absence doesn't mean that it absolutely won't work. But being on the HCL is a good indicator, and the list can help you identify problem devices.

Troubleshooting

If you encounter problems during setup—especially during hardware detection—try removing any devices that are not on the HCL. (One other possible solution to hardware-detection problems: use the BIOS setup program to change the BIOS setting to "non–Plug and Play operating system." Although Windows 2000 is, in fact, a Plug and Play operating system, the implementation of this option on some computers assigns resources in a way that precludes their use and control by Windows 2000.)

You can also avoid some problems by updating your computer's BIOS to the latest version. To find out whether an update is available, check with the manufacturer of your computer, its motherboard, or its BIOS. Identifying the BIOS and tracking down the appropriate source for updates can sometimes be daunting; you'll find good advice at *www.sysopt.com/bios.html* and *www.ping.be/bios* (information-rich sites that are not affiliated with any manufacturer).

Checking Software Compatibility

For security and stability reasons, not all software that runs in earlier versions of Windows runs in Windows 2000. In particular, the following types of programs are more than likely incompatible:

- Disk utilities (such as defragmenters) and antivirus programs written for Windows 9x or Windows NT.
- Programs that use virtual device drivers (VxDs) and .386 drivers (Windows 9x only). To see whether your system is loading any such drivers, check the [386Enh] section of the System.ini file.
- Third-party Control Panel applications and custom property pages.
- Custom power-management solutions written for Windows NT, which didn't offer much in the way of power management.
- Custom Plug and Play solutions written for Windows NT, which is not a Plug and Play operating system.

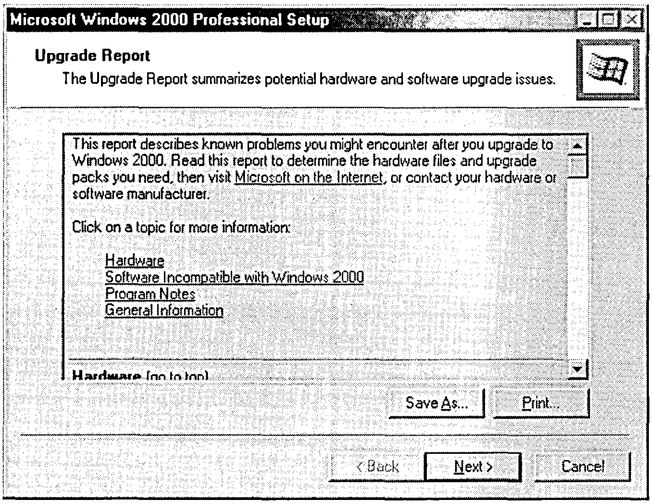
You should remove any such programs before you upgrade to Windows 2000.

In addition, some programs install differently on Windows 9x than on Windows 2000—that is, they use different program files or use different registry locations for storing data when installed under Windows 9x. Many publishers of programs for Windows 9x have created a migration dynamic-link library (DLL) for each of their programs that require one. A migration DLL can replace or upgrade files for earlier versions of Windows with Windows 2000–compatible versions, move application and user settings to the appropriate place in the Windows 2000 registry, and map other registry keys to the appropriate locations. The migration DLLs typically are called Migrate.dll, but they're more commonly known as *upgrade packs*. The Setup program asks whether you have any upgrade packs, so you should obtain any that you need before you begin installation. (Upgrade packs for some programs are on the Windows 2000 Professional CD—in the \I386\Win9xmig folder—but you can obtain others from the publishers' Web sites.) To find out which ones you need, use Setup's compatibility checker, described in the following section. Its report includes a list of programs for which you'll need upgrade packs.

Running Setup's Compatibility Checker

If your computer has Windows 9x or Windows NT installed, you can use the Setup program to check the system for compatibility with Windows 2000 and produce a report—without actually installing Windows 2000. The report lists installed hardware and software that might not be compatible with Windows 2000 and provides notes about using these items. To run the compatibility check, run Winnt32.exe (the Windows 2000 Setup program) with the /Checkupgradeonly switch. To do this from the Windows 2000 Professional CD, for example, use the Start menu's Run command to enter *d:\i386\winnt32 /checkupgradeonly*. Modify the path if you're running from a shared network folder or if your CD-ROM drive uses a different drive letter.

Setup displays its results on the screen (as shown in Figure 1-1) and saves the results in a text file. On systems running Windows 9x, the process usually takes several minutes, and it stores the resulting report in a file named Upgrade.txt in the Windows folder. On systems running Windows NT, the report is called Winnt32.log, and it's saved in the Winnt folder.



Microsoft Windows 2000 Professional Setup

Upgrade Report

The Upgrade Report summarizes potential hardware and software upgrade issues.

This report describes known problems you might encounter after you upgrade to Windows 2000. Read this report to determine the hardware files and upgrade packs you need, then visit Microsoft on the Internet, or contact your hardware or software manufacturer.

Click on a topic for more information:

Hardware
Software Incompatible with Windows 2000
Program Notes
General Information

Hardware (go to top)

Figure 1-1
Running the compatibility check in Windows 9x usually produces a lengthy report.

If you have to check a number of machines running Windows 9x, you can easily automate this process, as follows:

1. Use Notepad to create a short answer file with the following text, and save it as Check.txt:

```
[Unattended]
Win9xUpgrade=Yes

[Win9xUpg]
ReportOnly=Yes
SaveReportTo=a:\%computername%.txt
```

2. Use Notepad to create a batch file with the following text, and save it as Check.bat:

```
d:\i386\winnt32 /unattend:a:\check.txt /checkupgradeonly
```

3. Copy these two files to a floppy disk.

4. Go to each computer, insert the floppy disk and the Windows 2000 Professional CD, and run the Check batch file by opening it in Windows Explorer. The resulting report is saved in a file on the floppy disk; the computer name is used for the file name.

Backing Up Your Data

Unless you choose to format the partition onto which you're installing Windows 2000 (an option that you'll see during a clean install), the Setup program shouldn't destroy any data on your computer. But if your experience matches ours, the one way you can ensure that data will be lost is to fail to back it up before proceeding!

Backing Up Your Files

Most important: Use your existing backup program to back up all the files currently on the hard disk where you plan to install Windows 2000. The version of Microsoft Backup included with Windows NT allows you to back up your files to tape. The version included with Windows 9x can back up files to tape, a hard disk, a network drive, or removable disks. (If it's not on your Start menu, go to Add/Remove Programs and install it.) If you don't have a backup program or backup media, copy your important files to another computer on your network.

Exporting E-Mail and Web Browser Data

When you upgrade to Windows 2000, compatible programs continue to use their current data files. But if you perform a clean install, or if you're planning to change to different programs, the data is not readily available. If you have data such as mail or news account settings, e-mail messages, Web browser bookmarks, and cookies that you want to reuse, use your old program to export the data to a file that you can subsequently import into the equivalent Windows 2000–based program.

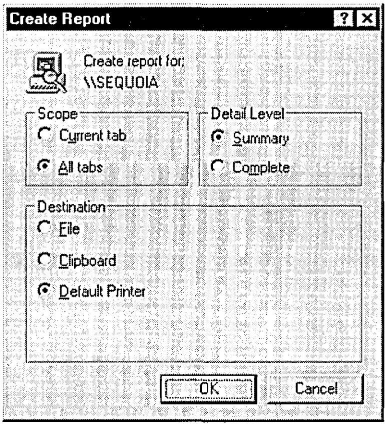
You might be tempted to export registry keys that contain the settings for your key applications—especially if you're planning a clean install. The settings for an application are typically saved in HKCU\Software\application, where *application* is the name of the program. Although you can use the registry editor to export this branch of the registry, it'll be of marginal value. If you simply perform a clean install of Windows and then import this registry branch, you'll be successful with only the simplest applications; others won't work or, at best, you'll bring along a lot of excess baggage. The exported registry might prove to be a useful reference as you reconfigure your system, however.

Printing Configuration Information

Hardware detection in Windows 2000 is much better than in any previous version of Windows. Nevertheless, the Setup program is occasionally stumped by certain hardware combinations and legacy (non–Plug and Play) devices. If your system is running an earlier version of Windows and all its devices are working well, a configuration report can help you identify and manually configure any devices that cause problems during setup.

To print a configuration report from Windows NT 4:

1. Open the Start menu and choose Programs | Administrative Tools (Common) | Windows NT Diagnostics.
2. Click Print.
3. In the Create Report dialog box, make the settings shown here and then click OK.



Create Report

Create report for:
\\SEQUOIA

Scope
○ Current tab
● All tabs

Detail Level
● Summary
○ Complete

Destination
○ File
○ Clipboard
● Default Printer

To print a configuration report from Windows 9x:

1. Right-click My Computer and choose Properties.
2. On the Device Manager tab, click Print.
3. In the Print dialog box, select System Summary and click OK.

Preparing the Computer

Before you install Windows 2000, you must first undo or disable features and programs from earlier versions of Window that can interfere with setup.

Uncompressing Compressed Drives

Windows 2000 is incompatible with DriveSpace and DoubleSpace—disk-compression programs that came with Windows 9x and MS-DOS 6—as well as with third-party disk-compression programs. If you have any compressed drives, you must uncompress them. (Doing so often creates a challenge because you must have enough room on the drive for all the files on the drive—after they're uncompressed. You might need to delete some files or move them to another drive before you can uncompress the drive.)

To uncompress a drive using Windows 9x:

1. Open the Start menu and choose Programs | Accessories | System Tools | DriveSpace.
2. In the DriveSpace dialog box, select the compressed drive.
3. Open the Drive menu and choose Uncompress.

To uncompress a drive using MS-DOS:

1. At the command prompt, type *drvspace* (if you have MS-DOS 6.22) or *dblspace* (if you have an earlier version).
2. Select the drive you want to uncompress.
3. Open the Tools menu and choose Uncompress.

Disabling Incompatible Services

Naturally, before you run Setup you should close all other applications. But you also need to stop any background services and applications that might cause problems. In particular, be sure to disable your antivirus program (because it prevents necessary changes to the boot sector and other critical files) and any third-party network clients and services (such as backup agents).

In Windows 9x or Windows NT, you can press Ctrl+Alt+Delete to display a task manager that shows which programs are currently running and lets you close them.

Creating a Computer Account

Computers on a network can be part of a *domain* (computers that share a security database on domain controllers running Microsoft Windows 2000 Server or Microsoft Windows NT Server) or a *workgroup*. To join a workgroup, all you need to know is the name of the workgroup. To join a domain, you need to know the name of the domain, and the computer needs to be connected to a working domain controller and DNS (Domain Name System) server.

In addition, if the computer you're setting up is going to be part of a Windows 2000 Server (or Windows NT Server) domain, it must have a computer account set up on the domain controller. You can do this before, during, or after installation:

- Before you set up the new computer, an administrator can create the computer account on the domain controller. In Windows 2000 Server, you use the Active Directory Users And Computers console to add a computer account; in Windows NT Server, you use Server Manager.

- During installation (near the end), the Network Identification Wizard runs. With it, you can create a computer account (if you haven't already set one up), provided that you can furnish the name and password of a domain administrative account that has authority to add domain computer accounts (typically, an account that's a member of the Domain Admins group). You can provide this information whether you run Setup in an interactive or unattended fashion.
- After installation, you can join a domain from the Network Identification tab of the System Properties dialog box. Again, if you haven't already set up a computer account on the domain controller, you can set one up from here—as long as you provide the name and password of a domain administrator account.

Choosing Between Upgrade and Clean Installation

If your computer has one of the following operating systems installed, you can *upgrade* your computer to Windows 2000 Professional:

- Windows 95 (all versions)
- Windows 98 (all versions)
- Windows NT Workstation 3.51
- Windows NT Workstation 4
- Windows 2000 Professional (evaluation version)
- Windows 2000 Professional beta Release Candidate 1 (build 2072) or later

Note To determine the build number of a Windows 2000 Professional beta version (as well as the expiration date of an evaluation version), open the Start menu, choose Run, and type *winver*.

With any of these operating systems, you have a choice: you can upgrade to Windows 2000 Professional, or you can perform a *clean install* of Windows 2000 Professional. (If you have a different operating system—including Windows NT Server, Windows NT Workstation versions earlier than 3.51, or Windows 3.1—or if you're installing onto a new, blank hard disk, your only choice is clean install.)

Note To perform an upgrade, you must start your existing operating system and then run Winnt32.exe, as described in the following section. Don't start Setup by booting from the Setup Boot Disk or the Windows 2000 Professional CD.

If you choose to upgrade, Setup replaces your existing Windows files, but it preserves user settings, such as desktop appearance, color schemes, network connections, and so on. More important, it retains the programs you have installed and all their settings. (Some programs that work in earlier versions of Windows do not work with Windows 2000, however. The upgrade report described earlier in this chapter identifies many such programs.) Therefore, after you complete the upgrade installation, you're ready to pick up right where you left off before installing—with the added features of Windows 2000.

In a clean installation, Setup installs Windows 2000 in a new folder. All Windows preferences and options will be set to their default settings, and you'll need to install the programs you use—even if you had already installed them under an earlier version of Windows. Although the programs' files might still be on your hard disk, the shortcuts, registry entries, and shared components that each program requires to run will not be. Be sure that you have available the original installation media for all your applications before you pursue this course.

Even on systems that meet the requirements for upgrading, a clean install has a significant benefit: it doesn't retain the detritus that accumulates on a computer over time as you install and uninstall programs, surf the Web (acquiring assorted applets along the way), and simply use the computer. Unused (or worse, maleficent) registry entries, multiple DLL file versions, .ini files, temporary files, and file fragmentation act like grains of sand in the gears of your well-oiled machine. A clean install—particularly if you go all the way and start by formatting the disk—can restore your computer's inner workings like no ordinary oil additive can. (During a clean install, you'll have the option of formatting the disk or leaving the current information intact.) If you're not afraid to get your fingers dirty, performing a clean install can be worthwhile.

Installing on a Single Computer

A good strategy for setting up a small workgroup is to start by setting up one computer using the basic installation method. You can then use that computer—and the experience you acquire during its setup—as the model for implementing the automated methods described later in this chapter.

Before you set up your first computer, print the files in the \Setuptxt folder of the Windows 2000 Professional CD. (They're ordinary text files that you can open and print using any text editor or print from an MS-DOS prompt.) For the most part, you'll find that the on-screen instructions adequately explain your options along the way, particularly if you've installed other versions of Windows before. But if you're stumped by any of the options presented, these files provide additional information that should help you.

Note If you plan to set up your system so that you can choose which of two or more operating systems to use whenever you start your computer (commonly called *dual boot*), you need to install Windows 2000 on its own partition. *For more information, see "Installing Each Operating System on a Separate Partition," page 51.*

Installing from the Windows 2000 Professional CD

To start an installation—upgrade or clean install—from a 32-bit version of Windows (Windows 9x, Windows NT, or an evaluation version of Windows 2000):

1. After Windows starts, insert the Windows 2000 Professional CD.
2. If a message appears that asks whether you want to upgrade your computer to Windows 2000 Professional, click Yes—even if you plan to perform a clean install.

   If no such message appears (because you've disabled AutoPlay), run \I386 \Winnt32.exe from the Windows 2000 Professional CD.
3. On the first page of the Windows 2000 Setup Wizard, select the appropriate option: Upgrade To Windows 2000 or Install A New Copy Of Windows 2000 (Clean Install).

If you don't have a 32-bit version of Windows installed, you cannot upgrade; you must perform a clean install. To begin the process, with your computer turned off, insert the Windows 2000 Professional CD (if your computer's BIOS allows it to start from a bootable CD) or Windows 2000 Setup Boot Disk 1. Then simply turn on the computer and follow the on-screen instructions.

Note For a bootable CD to work properly, set the boot order in BIOS so that CD is the first boot device, followed by the hard disk and floppy disk. (Each BIOS setup program is different. During bootup, watch for a message that tells you which key to press for setup. In the setup program, boot order is often an option on the page called Advanced CMOS Settings or something similar.)

Note If you don't have the four setup floppy disks, you can make a new set from the Windows 2000 Professional CD. To do that, run \Bootdisk \Makeboot.exe.

Installing from a Shared Network Folder

Even if you don't use the options for automation described later in this chapter, you might find it more convenient to install from a shared network folder instead of schlepping the CD around to each workstation. Installing from a network folder works perfectly well because, even though the computer must restart a few times during the setup process, the Setup program copies all the files it needs to a temporary location on the local hard disk before rebooting.

Setting Up the Distribution Folder

To set up the distribution folder—the shared network folder that contains the Windows 2000 files—follow these steps:

1. Create a folder on a server.
2. Copy the contents of the \I386 folder on the Windows 2000 Professional CD to the new folder.
3. In Windows Explorer, right-click the new folder's icon and choose Sharing.
4. Share the folder and set the permissions so that all users (the Everyone group if you're using Windows NT or Windows 2000) have read-only access. The settings you make on the Sharing tab vary depending on which version of Windows the server is running and on how your network is configured—but after you've made it this far, the correct choices should be self-evident.

Starting the Installation

To start a network installation—upgrade or clean install—from a 32-bit version of Windows (Windows 9x, Windows NT, or an evaluation version of Windows 2000), simply navigate to the distribution folder and run Winnt32.exe.

If you're installing from MS-DOS or Windows 3.x, you start the installation by connecting to the distribution folder and running Winnt.exe (not Winnt32.exe). But before you do that, be sure you're running SMARTDrive, a disk-caching program included with MS-DOS. This program makes a *huge* difference in the setup time; it can literally take hours longer without SMARTDrive. To run SMARTDrive, from the MS-DOS prompt (before you start Windows), run Smartdrv.exe, which is normally found in the \DOS directory. (You'll likely find a line that starts SMARTDrive in your Autoexec.bat file.)

Automating the Installation Process

As easy as the installation process is, it's not something you want to sit through more than once or twice. If you plan to install Windows 2000 Professional on more than a handful of computers, you'll want to use one of the automated installation methods:

- Answer files (automated installation scripts)

- Disk imaging (cloning)
- Remote installation
- Microsoft Systems Management Server (SMS)

The latter two methods, which are dependent on Windows 2000 Server, are most appropriate for deployment in large enterprises and therefore are not covered in this book. Remote installation allows a system with remote-boot capabilities to automatically install Windows 2000 from a Windows 2000 Server with Remote Installation Services (RIS) installed. You can find more information about RIS at the Windows 2000 Server Web site *(www.microsoft.com/windows/server)*. SMS allows an administrator to manage and monitor installations from a central location. For information about SMS, visit *www.microsoft.com/smsmgmt*. In addition, you can find information about RIS and SMS in the Deployment Planning Guide, which is installed with Support Tools. (To install Support Tools, run \Support\Tools\Setup.exe on the Windows 2000 Professional CD.)

Installing the Deployment Tools

The Windows 2000 Professional CD includes some programs and documentation that enable you to use the automated installation processes described in this chapter. These tools—Setup Manager and System Preparation Tool—are located in a .cab file (a compressed archive similar to a .zip file), so you must first extract them to your hard disk. To install the deployment tools:

1. Using Windows Explorer, open the \Support\Tools folder on the Windows 2000 Professional CD.
2. Open Deploy.cab.
3. Copy all the files in Deploy.cab to a folder on your hard disk.

The files include the following:

- **Setupmgr.exe.** Setup Manager, which is used for creating answer files.
- **Setupmgx.dll.** A DLL required by Setup Manager.
- **Sysprep.exe.** System Preparation Tool, which is used for creating and deploying disk images.
- **Setupcl.exe.** A tool that works with Sysprep.exe to generate new security identifiers (SIDs).
- **Deptool.chm.** A help file that describes the deployment tools.
- **Unattend.doc.** A Microsoft Word document with detailed reference information about all possible parameters for answer files and Sysprep.inf files.

Using Answer Files for Automated Installation

Windows 2000 Setup can accept answers to its user prompts from an answer file, which allows for unattended installation. An answer file can also contain answers to a number of questions that aren't posed by the interactive Setup program, which means that you actually have much greater control over installations. You can use an answer file whether you install from the Windows 2000 Professional CD or from a shared network folder.

Automated Installation Without a Script

You don't have to create an answer file to perform an automated installation. If you want the bare-bones, simplest method of upgrading a system, use the Start menu's Run command to enter this command:

```
d:\i386\winnt32 /unattend
```

(Replace *d:\i386* with the correct path to Winnt32.exe if your CD-ROM drive letter is not D or if you've copied the Windows 2000 files to a hard disk or a shared network folder.)

Using this method bypasses all the user prompts (with only a few exceptions, such as requesting the CD key) and performs an upgrade installation, preserving the existing file system, computer name, and user preferences. If the system had multiple user profiles (Windows 9x) or local user accounts (Windows NT), those user settings are migrated to local user accounts and profiles. *For information about user accounts, see Chapter 17, "Managing Users and Groups."*

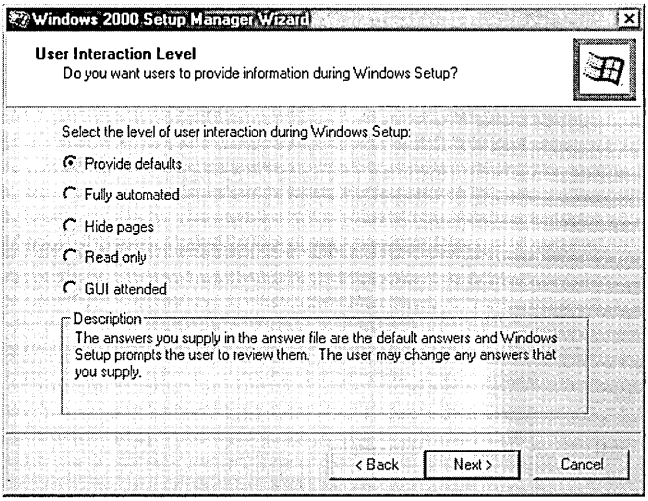
Creating an Answer File

An answer file is an ASCII text file that you can create and edit with any text editor, such as Notepad. An easier method—at least for preparing the initial framework—is to use Setup Manager, one of the tools in \Support\Tools\Deploy.cab on the Windows 2000 Professional CD. Setup Manager is a wizard that can do the following:

- Create answer files for automating the installation of Windows 2000
- Extract the information from a properly configured system to create an answer file that can be used to replicate the configuration on other machines
- Create a distribution folder for network installations, which can include (in addition to the Windows 2000 source files) additional applications and drivers that you want to install

Note Setup Manager runs only on Windows 2000.

To start Setup Manager, run Setupmgr.exe. After a few wizard pages with obvious answers, you'll reach the User Interaction Level page, shown in Figure 1-2. On this page, you specify how much you want the user to see during installation (for example, you can hide Setup Wizard pages for which you've provided the answers) and whether you want the user to be able to override the answers you provide in the answer file. A description of how each option works appears in the Description box when you select the option.



Windows 2000 Setup Manager Wizard

User Interaction Level

Do you want users to provide information during Windows Setup?

Select the level of user interaction during Windows Setup:

- ● Provide defaults
- ○ Fully automated
- ○ Hide pages
- ○ Read only
- ○ GUI attended

Description

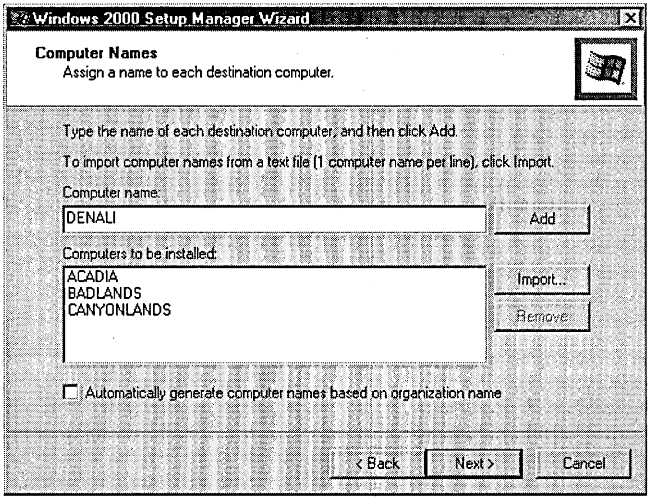
The answers you supply in the answer file are the default answers and Windows Setup prompts the user to review them. The user may change any answers that you supply.

Figure 1-2
Your choice here determines whether Setup allows the answers to be viewed or modified during installation.

From this point, the Setup Manager Wizard leads you through a series of questions that correlate to the questions that appear during interactive setup. Any questions that you leave unanswered can be answered during installation. For example, you might want to omit the user name from the answer file so that you can supply a different answer on each computer during installation. *(For a more elegant solution, see "Using a Differences File," page 22.)*

The Computer Names page, shown in Figure 1-3, offers two ways to provide a list of names for the computers you want to set up: you can type the names individually, or you can import a text file that contains the names. If you specify more than one computer name here (that is, if you want to use this answer file to automate installation of Windows 2000 on multiple computers), Setup Manager creates a differences file for you. Alternatively, select the check box if you want Setup to generate names;

these somewhat cryptic names append seemingly random letters and numbers to the first few letters of your organization name.



Computer Names

Assign a name to each destination computer.

Type the name of each destination computer, and then click Add.

To import computer names from a text file (1 computer name per line), click Import.

Computer name: DENALI

Computers to be installed:

ACADIA
BADLANDS
CANYONLANDS

□ Automatically generate computer names based on organization name

Figure 1-3
By specifying the names of multiple computers, you can use the same answer file to set up all your computers.

After you answer the Setup Manager Wizard's questions, it creates an answer file and stores it using the name and location you specify. By default, it names the file Unattend.txt—but you can use any name you like.

Customizing an Answer File

The easiest way to customize an answer file—if you simply need to modify some settings you made with Setup Manager—is to restart Setup Manager. On the wizard's second page, select Modify An Existing Answer File and specify the file name.

But there's much more you can do with an answer file; the Setup Manager Wizard guides you through only the most commonly used settings. If you want to get more creative with your automated installations, take a look at Unattend.doc, which is stored on the Windows 2000 Professional CD within \Support\Tools\Deploy.cab. This Word document provides a complete reference to all the answer file parameters. Although the document is well over 100 pages, the information is well organized and clearly presented, so don't let its bulk intimidate you. You might consider some of these additions or modifications:

- Use the [Components] section to specify which accessory programs get installed. You might not want your users distracted by Pinball, for example; this is the most effective way to prevent its use.
- Consider adding NtUpgrade=Yes and Win9xUpgrade=Yes to the [Unattended] section if you're upgrading computers with existing operating systems. Without

these keys (which Setup Manager does not put in), Setup installs Windows 2000 on the same partition as the existing operating system, but in a separate folder. This produces an unsupported dual boot system that's likely to cause problems and confusion. (Alternatively, you can use other settings to specify the partition or folder.)

- Use the [Win9xUpg] section to control how user accounts and passwords on Windows 9x computers are migrated to Windows 2000.
- Use ProductID in the [UserData] section to specify the CD key. (Although using the same CD key on all installations allows you to avoid entering it each time, there is a drawback: Microsoft Product Support Services uses parts of the CD key to identify customers who call for support and to determine eligibility for various support services.)
- Use the [Fax] section to configure the fax service.

As an ASCII text file, an answer file resembles the .ini files that were common in the Windows 3.x era. It consists of section headers—a section header is a word enclosed in square brackets ([ ]) on a line by itself—followed by keys and values. Each key begins on a new line, and it's usually followed by an equal sign (=) and a value for the key. If a value contains any spaces, it must be enclosed in quotation marks (" "). You can include comments in an answer file by putting a semicolon (;) at the beginning of each comment line. The listing that follows shows the first few sections of a typical answer file:

```
;SetupMgrTag
;Modified by Carl 3/20/2000 to add new Favorites entries

[Data]
    AutoPartition=1
    MsDosInitiated="0"
    UnattendedInstall="Yes"

[Unattended]
    UnattendMode=DefaultHide
    OemPreinstall=Yes
    TargetPath=\WINNT

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

[UserData]
    OrgName="Siechert & Wood, Inc."
    ComputerName=*
```

```
[Display]
    Xresolution=800
    YResolution=600
.
.
.
```

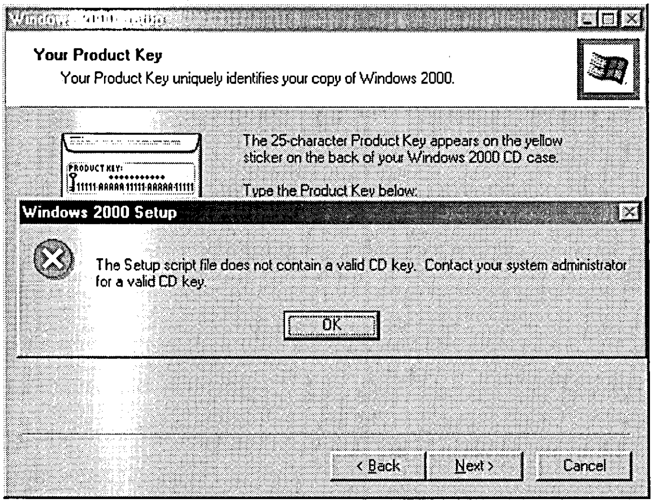
Warning Passwords in an answer file are stored as ordinary text. This includes the Administrator password for the target computer and the password for the administrative account that can create a computer account, if you specify it. Depending on security issues at your location, you might prefer to omit these parameters, requiring their entry during installation instead.

Using an Answer File During Setup

Using an answer file simply requires including the /Unattend switch (along with the file specification for the answer file) on the command line for Winnt32.exe, the Windows 2000 Setup program. For example, if you are installing from the Windows 2000 Professional CD and you want to use an answer file named Unattend.txt that's stored on a floppy disk, enter this command line:

```
d:\i386\winnt32 /unattend:a:\unattend.txt
```

You can enter this command using the Start menu's Run command or in a Command Prompt window. Setup begins and, depending on the level of user interaction that you specified (using the UnattendMode key in the [Unattended] section), proceeds on its merry way. If the answer file doesn't include some required information, Setup stops to prompt you, as shown in Figure 1-4.



Your Product Key

Your Product Key uniquely identifies your copy of Windows 2000.

The 25-character Product Key appears on the yellow sticker on the back of your Windows 2000 CD case.

Type the Product Key below:

Windows 2000 Setup

The Setup script file does not contain a valid CD key. Contact your system administrator for a valid CD key.

Figure 1-4
Setup stops to request required information that's not included in the answer file.

Similarly, to install from a distribution folder, navigate to the distribution folder and then enter *winnt32 /unattend:unattend.txt*. (This assumes that you stored the answer file in the distribution folder—the same folder that contains Winnt32.exe and the rest of the Windows 2000 files.)

Troubleshooting

Even simple errors in answer files can cause Setup to stop before it ever gets started—and you won't get any hints about where the problem lies. If you receive a message saying that your Setup script file is "inaccessible or invalid," check each line to see that it follows the proper format. Be sure that all values with spaces are enclosed in quotation marks. We were once stumped for quite some time because the basic answer file that Setup Manager produced wouldn't run. It seems that, because of a bug in Setup Manager, it sometimes omits the quotation marks if a string contains a comma!

If you used Setup Manager to create the answer file, the process of using the file is even simpler. Setup Manager creates a batch file using the same file name (but with a .bat extension) and location that you specify for the answer file. Simply navigate to the folder where you saved the answer file (usually the distribution folder, if you set one up, or a floppy disk) and launch the batch file. If you copy the batch file, the answer file, or both from the location where Setup Manager originally stored them, you might need to edit the batch file to update the path information.

Of course, you can also use an answer file to automate the installation on a new computer—and you don't have to enter any command lines at all. If your computer can boot from the Windows 2000 Professional CD, save the answer file on a floppy disk and name it Winnt.sif. Insert the CD and the floppy disk and turn on the computer. Setup runs from the CD and uses Winnt.sif as its answer file.

Using Automated Installations: The Simplest Way

If you have a small office—a few dozen computers or less—you don't need to pore through the stacks of deployment documentation that Microsoft has produced for large enterprise rollouts of Windows 2000. Instead, you can follow this simple, straightforward method for automating your installations:

1. Install Windows 2000 on one computer.
2. Install Setup Manager on the same computer.
3. Use Setup Manager to create an answer file. If you already have a network set up, use Setup Manager to create a distribution folder. Otherwise, tell Setup Manager that you'll install from the CD.
4. Using the information in Unattend.doc, edit the answer file you created to include any additional customizations you want.

(continued)

Using Automated Installations: The Simplest Way *(continued)*

5. If the computers you're targeting for installation don't have a working network connection, copy the answer file, the batch file, and the .udf file (if any) created by Setup Manager to a floppy disk.
6. At each computer, ensure that the computer is ready for Windows 2000 by going through all the preliminary steps described earlier in this chapter. *(See "Preparing for Installation," page 4.)*
7. At each computer, connect to the distribution folder (if you already have a working network) and run the batch file, or run it from the floppy disk. (If you specified more than one computer name, you'll need to append the computer name to the command line when you run the batch file.)

You'll find details about each of these steps in this chapter.

Enterprise IT managers must study the many alternatives to and variants of this simple procedure. Installing to thousands of computers demands that these managers invest the time and resources to find the absolute fastest method—and ensure that it's perfect from the first logon by a "real" user. Our goals for a small office installation needn't be so lofty; walking around to a handful of computers isn't that burdensome, and minor problems can be solved case by case.

Using a Differences File

A differences file (sometimes called a *uniqueness database file*, or Udf) provides variable information to supplement the information in an answer file. This allows you to create a single answer file that you can use for all your computers; information that changes for each computer (such as user name, computer name, and so on) is stored in a differences file. Like an answer file, a differences file is an ordinary text file that contains sections, keys, and values. The file name extension for a differences file is .udf.

If you use Setup Manager to create an answer file, it also creates a differences file if you specify more than one computer name on the Computer Names page (shown earlier in Figure 1-3, page 18). This is the simplest method for creating a basic differences file, which you can then enhance by editing it in Notepad. For example, we used Setup Manager to create this differences file for setting up four computers:

```
;SetupMgrTag
[UniqueIds]
    BADLANDS=UserData
    ACADIA=UserData
    CANYONLANDS=UserData
    DENALI=UserData

[BADLANDS:UserData]
    ComputerName=BADLANDS
```

```
[ACADIA:UserData]
    ComputerName=ACADIA

[CANYONLANDS:UserData]
    ComputerName=CANYONLANDS

[DENALI:UserData]
    ComputerName=DENALI
```

We edited the file to include additional specific information for each computer, like this information for the computer named Denali:

```
 [DENALI:UserData]
    ComputerName=DENALI
    FullName="Carl Siechert"
```

You can include any valid answer file sections and keys in the differences file, allowing you to use this capability to uniquely customize each of your installations with this one file. You might want some users but not others to have Pinball installed, for example. If a setting appears in both the answer file and the differences file, the setting in the differences file prevails.

To use the differences file, you must include the /Udf switch on the Winnt32 command line. You include the identifier (one of the keys listed in the [UniqueIds] section) and the name of the differences file. In our example, the differences file is named Diff.udf. Here is the complete command line for setting up the computer named Denali:

```
winnt32 /unattend:diff.txt /udf:DENALI,diff.udf
```

If you specify multiple computer names in Setup Manager, the batch file it creates simplifies entry of this command line. It uses the computer name as a command-line parameter so that, in this example (where the batch file is named Diff.bat), you simply type *diff denali* at the command prompt to set up the computer named Denali.

Using Disk Imaging

Windows 2000 includes Sysprep.exe, a program that allows you to install a system with Windows 2000–based applications and then duplicate it to other systems. (This has traditionally been a problem with Windows NT. Because each computer running Windows NT or Windows 2000 on a network must have a unique security identifier, or SID, it's not a simple matter of cloning a disk. Doing that would produce duplicate SIDs. Sysprep solves this problem by generating a unique SID the first time the computer is rebooted.) After the system has been duplicated, an abbreviated setup program runs. This "mini-Setup" requires only about five minutes to run. Because Sysprep duplicates an entire hard disk partition, you can use it to copy complete systems that have additional customizations and installed applications.

However, Sysprep might not be for you. Although Sysprep makes it easy to duplicate fully configured systems, it has some restrictions and requirements that limit its use:

- Most important, the master and target computers must have identical hard drive controllers, identical hardware abstraction layers (HALs), and identical BIOS versions. Although other components—such as modems, sound cards, network cards, and so on—need not be identical, this limitation effectively limits the use of Sysprep to fleets of identical computers. If you have a varied collection of computers of different ages and manufacturers, chances are good that Sysprep won't work for all of them.
- You'll need third-party software (or a hardware device) for disk duplication. Sysprep merely prepares the image for copying and then runs a version of Setup after the image has been copied to a new computer. But to actually make the copy, you'll need a program such as Norton Ghost (from Symantec) or Drive Image (from PowerQuest) or a disk-duplicating device.
- The hard disk on the target computer must be at least as big as the one on the master computer.

If these restrictions aren't a problem for you, you can follow these steps to use Sysprep:

1. Install Windows 2000 on a master computer. (Because you might go through this process several times before you get everything set up just the way you want, you should create an answer file and use it for setting up the master computer. *See the preceding section, "Using Answer Files for Automated Installation."*)

Note Do not join a domain—even if you intend to later—because running Sysprep removes the SID that allows the computer to connect to the domain. Set up the master computer in a workgroup. During setup on the target computers, you can join a domain.

2. Log on to the computer as Administrator.
3. Customize the computer as desired, and install applications that you want to be included on all target computers.
4. Create a folder named \Sysprep on the system partition and extract Sysprep.exe and Setupcl.exe from the \Support\Tools\Deploy.cab file on the Windows 2000 Professional CD to this folder.
5. Run Sysprep.exe. In a few moments, the system will shut down by itself (if it's ACPI compliant) or display a message stating that it's safe to turn off the computer.
6. Duplicate the hard disk. Depending on the duplication method, you might need to remove the hard disk from the system, or you might need to boot from a floppy disk that launches the third-party disk-duplication software.

When you start a computer that contains a duplicated disk (or, for that matter, when you turn on the master computer, if it still contains the master disk), Sysprep automatically does the following:

1. Detects Plug and Play devices
2. Runs a mini–Setup Wizard that lets you specify the user name, join a domain or workgroup, and make other basic setup choices
3. Deletes the \Sysprep folder and its contents
4. Reboots the computer

This entire process takes only about one-tenth the time that running Setup normally takes.

You can automate the mini–Setup Wizard by creating an answer file to provide some (or all) of the requested information. Use Setup Manager to create the answer file, being sure to select Sysprep Install on the Product To Install page. The file uses the same format, sections, keys, and values as an ordinary answer file. Settings that are unnecessary or inappropriate in the disk-imaging process are ignored. You must name the answer file Sysprep.inf, and you must place it in the \Sysprep folder before you run Sysprep.exe. Table 1-1 shows the information that the mini–Setup Wizard requests, along with the answer file sections and keys that you can use to automate the process.

Table 1-1. Answer File Keys for Automating MiniSetup

Mini-Setup Requests This Information	Unless You Use These Keys
Your agreement to the terms of the End User License Agreement (EULA)	[Unattended] OemSkipEula
Regional settings	[GuiUnattended] OemSkipRegional (Provide settings in the [RegionalSettings] section.)
Name and organization	[UserData] FullName, OrgName
Product key	[UserData] ProductID
Computer name	[UserData] ComputerName
Administrator password	[GuiUnattended] AdminPassword
Modem dialing information	[TapiLocation] AreaCode, CountryCode, Dialing, LongDistanceAccess
Date, time, and time zone	[GuiUnattended] TimeZone
Network identification	[Identification] DomainAdmin, DomainAdminPassword, JoinDomain, JoinWorkgroup

Installing Other Programs as Part of Setup

Automating installation of Windows 2000 with an answer file is terrific—but why stop there? You can also use answer files to initiate the installation of other programs as part of the installation process. When Setup finishes, you'll have a computer that's ready to use, with all your favorite applications already in place.

If you use disk imaging for installing Windows 2000, installing programs is automatic: you install the programs you want before you run Sysprep, and those programs—like everything else on the drive—become part of the disk image that gets duplicated.

Using answer files, two different methods support the installation of programs:

- Cmdlines.txt contains commands that run at the end of unattended setup.
- The [GuiRunOnce] section of the answer file contains commands that run the first time a user logs on.

The Cmdlines.txt method has the advantage of finalizing the setup process before your user ever logs on. It does have some drawbacks and limitations (as explained in the following section), so it's not appropriate in every case. Both methods are well suited to using custom installation packages that you create with IExpress or WinINSTALL LE, programs included on the Windows 2000 Professional CD that help you create installation packages for your programs. *For information about WinINSTALL LE, see "Creating MSI files for Legacy Applications," page 151.*

Setup Manager can create all the necessary entries and files for using either of these methods. To get to the necessary pages in the Setup Manager Wizard, you must select Yes, Edit The Additional Settings when you reach the Additional Settings page.

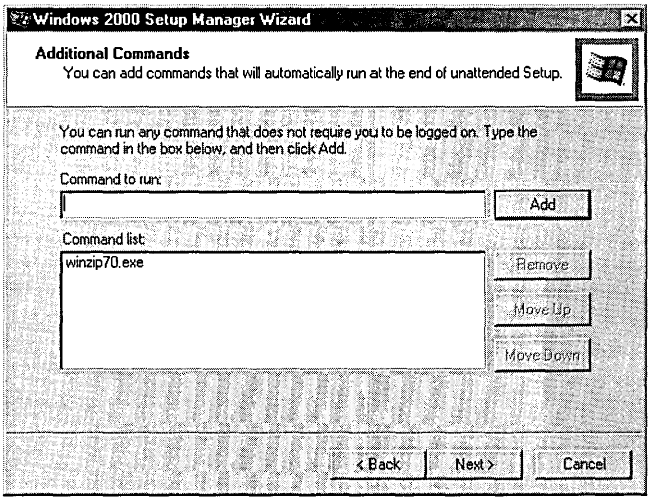
Using Cmdlines.txt

Cmdlines.txt is a text file that contains a list of commands to run immediately after Setup completes. These can include commands to set up applications. To use Cmdlines.txt, you need to create a distribution folder for Windows 2000 files; this method won't work for installing from a CD. (Let's qualify that: You can't use this method to install from the Windows 2000 Professional CD. But you could create a distribution folder and the necessary subfolders and then copy that folder structure to a CD-R if you have a CD burner.) You must create a subfolder of the distribution folder called OEM, which will contain Cmdlines.txt plus the files you're planning to install. Fortunately, Setup Manager takes care of these details for you.

Note When the commands in Cmdlines.txt run, no user is logged on. Therefore, user-specific information is written to the default user profile. Because no user is logged on, the computer might not have access to network files—including the distribution folder. You must put all files that are needed for application setup on the local hard disk. (This happens automatically when you use the OEM folder structure and OemPreinstall—in the [Unattended] section of the answer file—is set to Yes.)

Say, for example, you want to install WinZip (a program that manages .zip archives) onto every computer. To do that, make the following settings in Setup Manager:

1. When you get to the Additional Settings page, select Yes, Edit The Additional Settings.
2. On the Distribution Folder page, select Yes, Create Or Modify A Distribution Folder.
3. On the Additional Commands page, type the command that runs the application's setup program and then click Add. Setup for WinZip runs from an executable called Winzip70.exe. Repeat this step for additional commands you want to run.



Windows 2000 Setup Manager Wizard

Additional Commands

You can add commands that will automatically run at the end of unattended Setup.

You can run any command that does not require you to be logged on. Type the command in the box below, and then click Add.

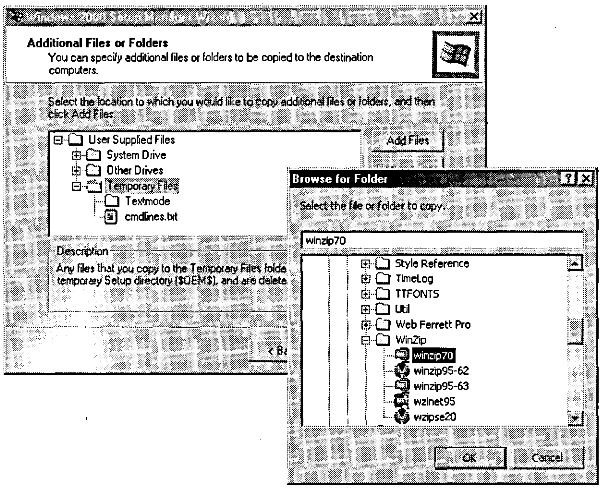
Command to run:

Command list:

winzip70.exe

4. On the Additional Files Or Folders page, select Temporary Files. This represents the OEM folder within the distribution folder. During Setup, the contents of this folder are copied to a temporary folder on the target computer. The temporary folder is deleted after Setup finishes. (The other folders in this dialog box represent additional folders in the OEM structure. In addition to directing files to a temporary folder, you can direct files to any permanent folder on the target computer. See the Description text as you select each folder for more information.)

5. Click Add Files, and then navigate to the file or folder you want to copy to the OEM folder (and ultimately to the target computer). (For WinZip, you need just a single file—Winzip70.exe. For other programs, you need to copy an entire folder.)



Windows 2000 Setup Manager Wizard

Additional Files or Folders

You can specify additional files or folders to be copied to the destination computers.

Select the location to which you would like to copy additional files or folders, and then click Add Files.

Description

Any files that you copy to the Temporary Files folde
temporary Setup directory (OEM), and are delete

Browse for Folder

Select the file or folder to copy.

winzip70

Using the [GuiRunOnce] Section

The [GuiRunOnce] section of the answer file contains a list of commands that run the first time a user logs on to the computer after Setup runs. This method works well with most application setup programs and also with Windows Installer packages that you create with WinINSTALL LE. Because these commands run when a user is logged on, they can refer to executables stored on a network server (assuming, of course, that the user has appropriate permissions for accessing the network resource). Alternatively, they can refer to local files that you copy using the OEM subfolder within a distribution folder.

Note You shouldn't use this method for installation programs that require a reboot, because other commands in the [GuiRunOnce] section won't run following the reboot.

You can control the order in which setup programs run and—perhaps more important—ensure that only one runs at a time by putting the commands in a batch file. Then place the batch file name in the [GuiRunOnce] section. In the batch file, precede each setup command with "Start /Wait." This command causes the batch file execution to wait until the command (that is, the setup program) completes before it runs the next command. For example, you could create a batch file that looks like this:

```
start /wait \\server\app1\setup.exe
start /wait \\server\app2\setup.exe
start /wait \\server\app3\setup.exe
exit
```

Use the Additional Files Or Folders page in Setup Manager to copy the batch file (or the setup programs, if you choose to go that route) to the target computer during setup. (Be sure, however, that you don't copy files or folders to the Temporary Folders section; those files are deleted before [GuiRunOnce] commands get executed.) Alternatively, store the batch file (or whatever commands you're going to run using [GuiRunOnce]) on a network server. When you add the commands to the [GuiRunOnce] section, be sure to include the full network path to the commands.

To add one or more commands to the [GuiRunOnce] section, make the following settings in Setup Manager:

1. When you get to the Additional Settings page, select Yes, Edit The Additional Settings.
2. On the Run Once page, type the name of the batch file or command that runs the application's setup program; then click Add. Repeat this step for additional commands you want to run.

Chapter 2

Setting Startup Options

In This Chapter

Setting Pre-Logon Options 31
Setting Logon Options 37
Setting Up Recovery Console 42
Booting from Floppy Disks 42

As you'll learn in this chapter, a lot goes on before the Windows 2000 desktop appears. On the way to the desktop, Microsoft Windows 2000 Professional presents a boot menu, a couple of progress bars and startup screens, a Welcome To Windows dialog box, and a Log On To Windows dialog box. Behind the scenes, Windows is detecting hardware and loading device drivers, services, and programs. *For information about what happens after Windows 2000 starts, see "Controlling Programs and Services that Start at Logon," page 135.*

This chapter shows how you can customize this startup process by changing the appearance of some screens, bypassing some screens altogether, and controlling security during startup. Learning about the startup options here also introduces you to some of the troubleshooting features you can use if your computer doesn't start up normally. *For details about using those features, see "What to Do If Your System Won't Start," page 706.*

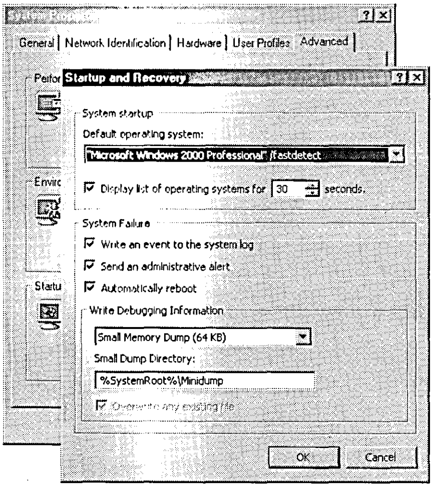
Setting Pre-Logon Options

If you're in the habit of turning on your computer, stepping out to get a cup of coffee, and returning to find a graphical screen with a Welcome To Windows dialog box, you've missed out on a few things. Your computer might display a boot menu, which we explain how to customize in this section. During the initialization, Windows also offers an Advanced Options menu, which we introduce here.

Setting Default Startup Options

If you have more than one operating system installed on your computer, a boot menu appears after you turn on or restart the computer. The boot menu lets you choose which operating system you want to run. *(For information about setting up multiple operating systems, see Chapter 3, "Working with Multiple Operating Systems.")* Ordinarily, following an installation of Windows 2000 Professional, the boot menu is set up to display the choices for 30 seconds. If you don't make a selection in that timeframe, Windows 2000 Professional starts up. When the boot menu appears, a 30-second countdown timer appears; pressing the Up Arrow key or Down Arrow key to highlight a different operating system disables the timer. Your highlighted choice is enacted when you press Enter.

From within Windows 2000, you can change the menu display time and specify which operating system starts by default. To make these settings, open the System Properties dialog box (right-click My Computer and choose Properties, or open System in Control Panel) and click the Advanced tab. Click Startup And Recovery to display the dialog box shown in Figure 2-1.



System startup

Default operating system: "Microsoft Windows 2000 Professional" /fastdetect

☑ Display list of operating systems for 30 seconds.

System Failure

☑ Write an event to the system log

☑ Send an administrative alert

☑ Automatically reboot

Write Debugging Information

Small Memory Dump (64 KB)

Small Dump Directory: %SystemRoot%\Minidump

☑ Overwrite any existing file

Figure 2-1
In the Startup And Recovery dialog box, you control how the boot menu works.

In the Default Operating System list, select the operating system that you want to be initially highlighted on the boot menu. Select the Display List check box if you want the default operating system to start automatically after the time you specify in the Seconds box. If you select the check box, the countdown timer appears on the boot menu and the default operating system starts up when the timer reaches 0. Clearing the check box is effectively the same as setting the time to 0 seconds: the default operating system starts up immediately.

Note You can't rename the operating systems in the Default Operating System list from this dialog box; to do that, you must edit Boot.ini, as described in the following section, "Modifying Boot.ini."

Overview of the Startup Process

When you turn on your computer, it goes through an elaborate startup process. The process begins when your computer performs its power-on self test (POST), which is followed by the POST for each adapter card that has a basic input/output system (BIOS) (SCSI adapters, for example). The system BIOS then reads the master boot record (MBR)—the first sector on the first hard disk—and transfers control to the code in the MBR, which is created by Windows 2000 Setup. Here's where Windows 2000 takes over the startup process.

The MBR reads the boot sector—the first sector of the active partition—which contains code that starts the operating system. (We're far from finished; in this context, "operating system" really refers to Ntldr, the bootstrap loader for Windows 2000.) Ntldr must be located in the root folder of the active partition, along with Ntdetect.com, Boot.ini, Bootsect.dos (if you're going to dual boot), and Ntbootdd.sys (if you're using certain SCSI adapters for the drive with the boot partition). *(For more information about sectors, partitions, and drives, see Chapter 12, "Managing Disks.")* The initial role of Ntldr is to switch the system to protected mode with paging enabled (to allow full memory addressing), start the file system, read the Boot.ini file, and display the boot menu.

If you select Windows 2000 from the boot menu, Ntldr runs Ntdetect.com to gather information about the currently installed hardware. Ntldr then uses the Advanced RISC Computing (ARC) pathname specified in Boot.ini to find the boot partition—the one where Windows 2000 is installed—and loads the two files that comprise the Windows 2000 core: Ntoskrnl.exe and Hal.dll. Both files must be located in the %SystemRoot%\System32 folder. Ntldr continues by reading the files that make up the registry, selecting a hardware profile and control set, and loading device drivers. At this point, Ntoskrnl.exe takes over and launches Winlogon.exe, which in turn starts Lsass.exe (Local Security Administration), the program that displays the Welcome To Windows dialog box.

Understanding the boot process can help you to pinpoint problems that occur during startup. *For more information, see "What to Do If Your System Won't Start," page 706.*

Modifying Boot.ini

Although these aren't essential tweaks—they're more appropriately categorized as Stupid Boot Tricks—you might want to open Boot.ini and make a few changes. The first trick is finding it; because it has hidden and system attributes, it doesn't appear in Windows Explorer even if you have Folder Options set to show hidden files. (To make these "super-hidden" files appear, you must also clear the Hide Protected Operating System Files check box on the View tab of Folder Options.) Fortunately, there is a simple trick, and you don't need to use Windows Explorer at all: simply use Start | Run and type *c:\boot.ini*. Doing so opens up the file in Notepad. A typical Boot.ini file might look like this:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(2)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Microsoft Windows 2000
   Professional" /fastdetect
C:\="Microsoft Windows 98"
```

With one exception, the [boot loader] section contains items that are more easily changed through the Startup And Recovery dialog box, as explained in the previous section. The exception is if you want the boot menu to be displayed until you press Enter, regardless of how much time elapses. To configure your boot menu to work that way, set the timeout value to –1. (You can't set that value in the Startup And Recovery dialog box.)

The main place that's ripe for editing is the [operating systems] section, in which each line represents a boot menu item. The line includes the ARC pathname (see the sidebar) of the operating system's boot partition, the text that appears on the boot menu (enclosed in quotation marks), and optional parameters. You might want to do the following:

- Change the text description for each operating system—particularly if you have multiple copies of the same operating system installed (for test purposes, for example).
- Append a parameter to the Windows 2000 line (following /Fastdetect, a parameter that disables serial mouse detection). Most are for development and debugging purposes only. (The *Microsoft Windows 2000 Professional Resource Kit* contains a more complete list.) Here are two you might want to try:
    - */Noguiboot* eliminates the Windows splash screen during startup. Instead you get to continue staring at the horizontal bar at the bottom of the screen.
    - */Sos* displays the name of each driver as it loads and provides additional text descriptions of what's occurring during startup. It also shows the Windows 2000 build number, service pack level, number of processors, and amount of installed memory, providing a quick confirmation that Windows 2000 is installed properly and that it's properly recognizing your computer's configuration.

- Remove an item from the menu. Doing so won't free the space used by the operating system whose line you remove; it simply removes the item from the menu. However, you can subsequently remove that operating system's files after you boot into one of the remaining operating systems in the list. *For more information, see "Removing an Operating System," page 60.*

Warning Don't remove the line that matches the default setting in the [boot loader] section.

ARC Pathnames in Boot.ini

In the [operating systems] section of the Boot.ini file, you'll find a somewhat cryptic line for each installed copy of Windows 2000 or Windows NT. This line uses Advanced RISC Computing (ARC) pathnames to specify the location of the boot partition. The ARC path in Boot.ini looks like one of the following examples:

- **multi(0)disk(0)rdisk(0)partition(2)\WINNT** This form is used for IDE, EIDE, ESDI, and some SCSI disks. With this form, Ntldr uses interrupt (INT) 13 BIOS calls to locate Ntoskrnl.exe and other files that it loads at startup.
- **signature(8b467c12)disk(1)rdisk(0)partition(2)\WINNT** This form, new with Windows 2000, supports the Plug and Play architecture. By relying on a disk signature rather than a SCSI controller number, it continues to work if the controller number changes from one startup to another—something that's likely to occur if you install an additional SCSI controller, for example. It's used for boot partitions that are larger than 7.8 GB or have an ending cylinder number greater than 1024; it's also used for boot partitions on disks connected to SCSI controllers whose BIOS is disabled (and therefore can't use INT 13 BIOS calls).
- **scsi(0)disk(0)rdisk(0)partition(1)\WINNT** This form is used for SCSI disks. It's a relic of Windows NT, but Windows 2000 setup leaves this form in place if the Boot.ini file contains multiple scsi() entries.

The first parameter identifies the disk controller. In the multi() form, it should always be 0. In the signature() form, the number is the disk signature; Ntldr looks for the partition with that signature, without regard to which SCSI controller the drive is connected to. In the scsi() form, it's the ordinal number (starting with 0) of the disk controller.

The disk parameter is not used in the multi() form and should always be 0. In the signature() and scsi() forms, it's the SCSI ID of the disk.

The rdisk parameter in the multi() form specifies the ordinal number on the controller (starting with 0) of the disk that contains the boot partition. In the signature() and scsi() forms, it's the SCSI logical unit number (LUN) of the disk.

(continued)

ARC Pathnames in Boot.ini *(continued)*

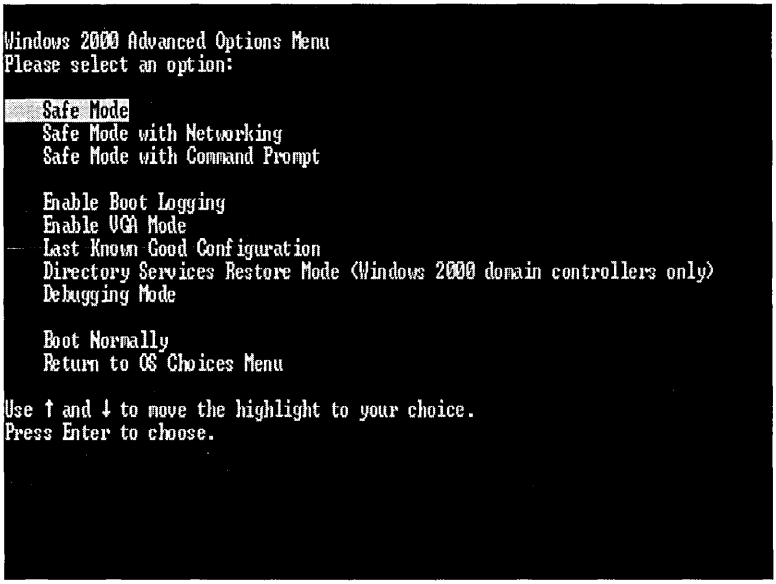
The partition parameter identifies the partition number of the boot partition. Partitions on a disk are numbered starting with 1.

The last part of the ARC pathname (usually \WINNT) identifies the path to the folder where Windows 2000 is installed.

It's rare that you'd ever need (or want) to edit any of the ARC pathnames in Boot.ini. But if you need to revive a system that's lost its Boot.ini and other key startup files, you'll need this information.

Using the Advanced Options Menu

For a few seconds before the Windows splash screen appears (and while the boot menu appears, if you have more than one operating system installed), a message is displayed at the bottom of the screen: "For troubleshooting and advanced startup options for Windows 2000, press F8." In case you've never had the guts or the quick finger to press F8, Figure 2-2 shows what you've missed.



```
Windows 2000 Advanced Options Menu
Please select an option:

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable VGA Mode
    Last Known Good Configuration
    Directory Services Restore Mode (Windows 2000 domain controllers only)
    Debugging Mode

    Boot Normally
    Return to OS Choices Menu

Use ↑ and ↓ to move the highlight to your choice.
Press Enter to choose.
```

Figure 2-2
The Advanced Options menu provides troubleshooting options.

None of these options are "advanced" in the sense that they provide some additional useful capabilities for power users. (If you're a diehard power user who thinks graphical user interfaces are for wimps, you might be tempted to try Safe Mode With Command Prompt in the hope that it gives you a command-line interface without the overhead of the GUI. But because it's safe mode, many essential services—including networking—are disabled, leaving you as an emasculated power user.) Rather, all of these options (with the exception of Boot Normally, of course) are for troubleshooting and correcting systems that don't run properly. *For information about these options, see "What to Do If Your System Won't Start," page 706.*

Setting Logon Options

After Windows 2000 finishes its initial startup tasks, you might see a Welcome To Windows dialog box and a Log On To Windows dialog box before you're allowed to see the Windows desktop—or you might not. If your computer is in a secure location and you're not concerned that others might use it to access your data, you can bypass those dialog boxes.

Warning Consider the risks before you decide to bypass either of these dialog boxes.

Pressing Ctrl+Alt+Delete as required by the Welcome To Windows dialog box ensures that the Log On To Windows dialog box that follows is really the one that's part of Windows 2000 Professional—and not an imposter designed to capture your password. Only Windows itself can respond to the Ctrl+Alt+Delete key combination.

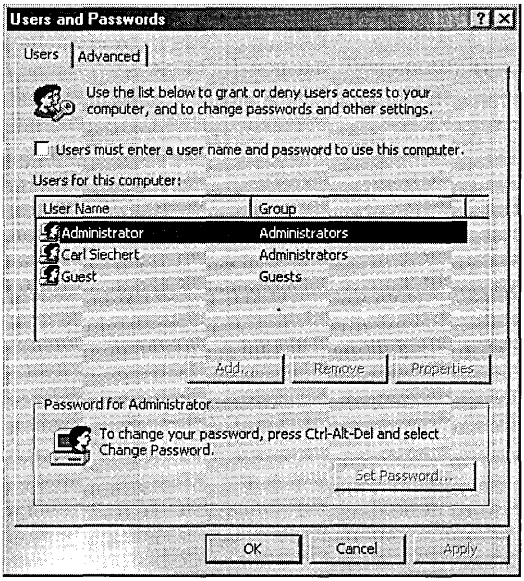
Bypassing the Log On To Windows dialog box means that the system effectively enters your user name and password when you turn on the power. Anyone who has physical access to your computer can then log on as "you" and have access to all computer resources that you normally have.

To bypass the Welcome To Windows dialog box (the one that asks you to press Ctrl+Alt+Delete):

1. In Control Panel, open Users And Passwords.
2. On the Advanced tab of the Users And Passwords dialog box, clear the Require Users To Press Ctrl-Alt-Delete Before Logging On check box.

To bypass the Log On To Windows dialog box (the one that asks for your user name and password):

1. In Control Panel, open Users And Passwords.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

□ Users must enter a user name and password to use this computer.

Users for this computer:

User Name	Group
Administrator	Administrators
Carl Siechert	Administrators
Guest	Guests

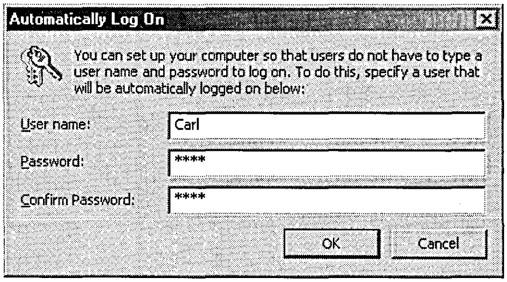
Password for Administrator

To change your password, press Ctrl-Alt-Del and select Change Password.

2. On the Users tab, clear the Users Must Enter A User Name And Password To Use This Computer check box and click OK.

Note This check box does not appear if your computer is part of a domain. Only computers that are not connected to a network or are part of a workgroup can bypass this dialog box. Domain users must enter a user name and password, even to log on locally.

The Automatically Log On dialog box appears.



You can set up your computer so that users do not have to type a user name and password to log on. To do this, specify a user that will be automatically logged on below:

User name: Carl

Password: ****

Confirm Password: ****

3. Type the user name and password for the account that you want to be logged on each time you start your computer.

Note Bypassing the Log On To Windows dialog box obviates the need to press Ctrl+Alt+Delete, so Windows automatically skips the Welcome To Windows dialog box when you choose this option.

Customizing the Logon Screen

The logon screen—the one that appears while the Welcome To Windows and Log On To Windows dialog boxes are displayed—is rather mundane. You're free to change the colors, wallpaper, and screen saver that appear at this time. However, Windows provides no easy or intuitive way to change these elements; you must edit the registry. *For information about editing the registry, see Chapter 39, "Working with the Registry."*

- To set the colors of the desktop, title bars, buttons, and so on, set values in the HKU\.Default\Control Panel\Colors key. To set fonts, border sizes, and so on, set values in HKU\.Default\Control Panel\Desktop\WindowMetrics.
- To specify the wallpaper, set the Wallpaper and TileWallpaper values in HKU\.Default\Control Panel\Desktop.
- To enable a screen saver, in the HKU\.Default\Control Panel\Desktop key, set ScreenSaveActive to 1, set ScreenSaveTimeout to the number of seconds before the screen saver kicks in, and set the Scrnsave.exe value to the file name of the screen saver you want. (The screen savers included with Windows 2000, which have an .scr file name extension, are stored in %SystemRoot%\System32. You don't need to include the path if your screen saver is in this folder.) To set its parameters, set values in the HKU\.Default\Control Panel\Screen Saver.*name* key, where *name* is the name of the screen saver.

Note In addition to defining parameters for the logon screen, the HKU \.Default key provides the initial parameters for all new user accounts that you create.

Some of these settings are rather mysterious. In particular, the color settings, which are string values comprising decimal representations of the red, green, and blue component values, are difficult to visualize using a registry editor alone. Fortunately, you can use an easier way:

1. Using the Display Properties dialog box (right-click the desktop and choose Properties, or open Display in Control Panel), configure your own desktop the way you want the logon screen to appear. Use the Appearance tab to set colors, the Background tab to set wallpaper, and the Screen Saver tab to configure a screen saver.

2. Open Regedit.exe (not Regedt32.exe). Navigate to \HKCU\Control Panel—the repository for your own Control Panel settings. Then select the key that contains the information you modified in the Display Properties dialog box—Colors for color settings, or Desktop for font, wallpaper, and screen saver settings. (If you made changes to Colors *and* Desktop, you'll need to repeat this and the following steps; working with these two keys separately is easier and safer than also copying their containing folder, which also contains numerous other settings that you might not want copied to the default profile.)
3. Choose Registry | Export Registry File and provide a file name. Be sure that Selected Branch is selected and that it shows either HKEY_CURRENT_USER \ Control Panel\Colors or HKEY_CURRENT_USER\Control Panel\Desktop. Click Save to save the registry branch as a text file with a .reg extension.
4. In a Windows Explorer window, right-click the new .reg file and choose Edit, which opens the file in Notepad.
5. In Notepad, change each occurrence of the key name HKEY_CURRENT_USER to HKEY_USERS\.Default. (If you exported the Desktop branch, you might also want to remove all values except those associated with your desired font, wallpaper, and screen saver settings.) Save the file.
6. Back in Explorer, double-click the revised .reg file. Doing so merges the entries into the registry.
7. Log off to see the effects of your changes.

Troubleshooting

If the logon screen doesn't appear the way you expect it to, be sure you're using a bitmap image for wallpaper; JPEG images require Active Desktop, which is not covered by this procedure. If that doesn't solve the problem, check permissions. The built-in SYSTEM user must have (at least) Read permission for any files accessed by the logon screen, such as a wallpaper bitmap, font, or screen saver.

Setting Logon Security Options

A number of local security policies affect the appearance and capabilities of the logon screen. These local security policies are part of the local Group Policy object, and you can set them using either Local Security Policy (Secpol.msc) or Group Policy (Gpedit.msc). (In the steps that follow, we chose Local Security Policy simply because it provides a shorter path to the settings we want to change.) To make any of these changes—in fact, even to launch either console application—you must be logged on as a member of the local Administrators group. *For more information about policies, see Chapter 18, "Using Group Policy."*

Warning Don't use a registry editor to make these changes, even though these policy settings are stored in the registry. Whenever Windows provides a method for making changes through consoles, Control Panel, or other programs, use that method instead of editing the registry directly; it's much safer (and usually easier).

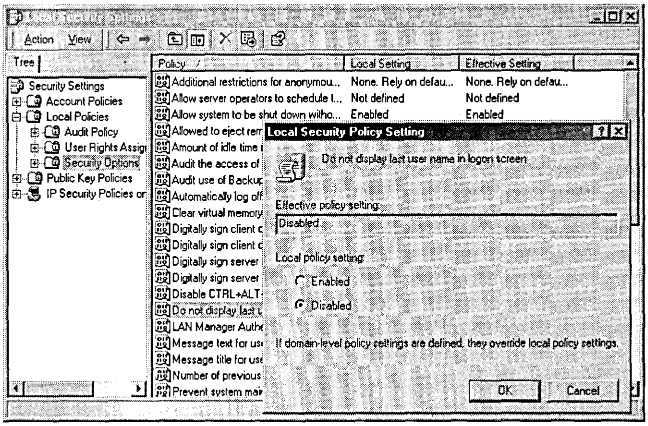
You might want to change one or more of the following policies:

- **Do Not Display Last User Name In Logon Screen.** Ordinarily, when the logon screen appears, it shows the name of the last user who successfully logged on. This is the best setup for computers that are normally used by only one person, for it means that person doesn't have to type his or her user name at every logon. For security reasons, you might want to enable this policy, thereby leaving a blank User Name field in the Log On To Windows dialog box.
- **Allow System To Be Shut Down Without Having To Log On.** By default, the Log On To Windows dialog box includes a Shutdown button. (It appears only when you click Options >> to expand the dialog box.) Clicking the button shuts down the computer. If you enable this policy, the button is dimmed, which allows only a user who successfully logs on to shut down the computer. (And through another policy—the Shut Down The System policy in Security Settings\Local Policies\User Rights Assignment—you can specify which logged-on users are allowed to shut down the computer.)
- **Disable CTRL+ALT+DEL Requirement For Logon.** When enabled, this policy bypasses the Welcome To Windows dialog box—the one that asks you to press Ctrl+Alt+Delete to log on—and displays the Log On To Windows dialog box on the logon screen. Your setting here, if any, overrides the setting you make in Users And Passwords.
- **Message Text For Users Attempting To Log On** and **Message Title For Users Attempting To Log On.** These policies set the body text and title bar text for a message box that appears before the Log On To Windows dialog box is displayed. This feature is intended for legal notices—such as a warning to users about the consequences of misusing company information or to inform them that their actions may be monitored—but you might find a more innocuous reason to use it. Note that you must provide both message text and message title, or the message box doesn't appear.

To modify any of these policies:

1. In Control Panel, choose Administrative Tools | Local Security Policy to open the Local Security Settings console. (Alternatively, use the Start | Run command to launch Secpol.msc.)
2. In the console tree, go to Security Settings\Local Policies\Security Options.

3. Double-click the policy you want to change. See Figure 2-3.



Policy	Local Setting	Effective Setting
Additional restrictions for anonymou...	None. Rely on defau...	None. Rely on defau...
Allow server operators to schedule t...	Not defined	Not defined
Allow system to be shut down witho...	Enabled	Enabled
Allowed to eject rem		
Amount of idle time		
Audit the access of		
Audit use of Backup		
Automatically log off		
Clear virtual memory		
Digitally sign client c		
Digitally sign client c		
Digitally sign server		
Digitally sign server		
Disable CTRL+ALT		
Do not display last u		
LAN Manager Authe		
Message text for us		
Message title for use		
Number of previous		
Prevent system mair		

Do not display last user name in logon screen

Effective policy setting: Disabled

Local policy setting:

○ Enabled

● Disabled

If domain-level policy settings are defined, they override local policy settings.

Figure 2-3
You can reach the same set of local security policies through Local Security Policy (shown here) or Group Policy.

Setting Up Recovery Console

Recovery Console is a command-line console that can help you restore your system to working order if it doesn't start up properly. With Recovery Console, you (assuming that you're a member of the Administrators group) can access files and folders on your hard drives, format drives, start and stop services, replace corrupt files, and so on. *We take up the topic of using Recovery Console in greater depth in Chapter 42, "Troubleshooting."* Before you need to use Recovery Console, however, setting it up on your system so that it's an option on your boot menu is a good idea. Then when trouble comes knocking, you'll be prepared. To set up Recovery Console, you'll need to run the Windows 2000 Professional Setup program, Winnt32.exe (on the Windows 2000 Professional CD in the \I386 folder), with the /Cmdcons switch. The easiest way: go to Start | Run and type *d:\I386\winnt32.exe /cmdcons* (modifying the path as necessary for your purposes). The next time you start your computer, you'll have a new entry on the boot menu. Try it; type *help* at the command prompt to see what commands are available.

Booting from Floppy Disks

In earlier versions of Windows (not Windows NT) and MS-DOS, you could create a bootable floppy disk. This allowed you to start your computer and get to an MS-DOS prompt—without invoking Windows or any of the other drivers or programs that normally start when you boot from your hard drive. One use, in fact, was to boot your computer when files on your hard disk were corrupt; you could use MS-DOS-based utilities to try to recover data from the hard disk and restore it to working condition.

The Recovery Console provides similar capabilities for restoring corrupted files. Certain conditions, however, render even the Recovery Console impotent, and your best recovery tool is a startup floppy disk. If your computer can't even begin the boot process (that is, you never get to the boot menu or the progress bar at the bottom of the screen), you might have one of the following problems, which can often be solved with the help of a startup floppy disk:

- Corrupted MBR
- Corrupted boot sector
- Certain virus infections
- Missing or corrupt Ntldr or Ntdetect.com
- Incorrect, missing, or corrupt Ntbootdd.sys (which is a renamed copy of the device driver for your computer's SCSI controller)

A startup floppy disk uses the files on the floppy disk to initiate the startup process, but the process still ultimately goes to the Windows 2000 files on your hard disk. Fitting a working version of Windows 2000 on a floppy disk—or even a stack of floppy disks!—is not possible.

Troubleshooting
A startup floppy disk won't help with corrupted device drivers that prevent startup or with startup problems that occur after Ntldr starts. To work around these problems, press F8 during startup to display the Advanced Options menu and choose Last Known Good Configuration.

Creating a Startup Floppy Disk

A startup floppy disk needs only three (or, in some cases, four) files:

- Ntldr
- Ntdetect.com
- Boot.ini
- Ntbootdd.sys (necessary only if the signature() or scsi() forms are used in Boot.ini, which occurs when Windows 2000 is installed on a SCSI drive and the SCSI BIOS is disabled)

Note

If your system is set up for dual booting with MS-DOS or Windows 9x, you can retain that capability on your startup floppy disk by also including these files: Autoexec.bat, Bootsect.dos, Command.com, Config.sys, Io.sys, and Msdos.sys.

If you're smart, you'll create a startup floppy disk *while your computer is working properly*. In that case, you can simply copy the files from the root folder of your computer's system drive to a formatted floppy disk. (You'll need to set Folder Options to display protected operating system files in order to see these files in Windows Explorer.) Be sure that the floppy disk is formatted by Windows 2000 or Windows NT so that it has the correct partition boot sector.

If you're like most of us—the idea of creating a startup disk occurs *after* you have a problem that requires it—you can still create a startup floppy disk. It's just a little more difficult. You can copy Ntldr and Ntdetect.com from the \I386 folder of the Windows 2000 Professional CD. You can copy Boot.ini from another system that works—you might need to edit it to match your computer's disk configuration—or you can create it from scratch, using Notepad or another text editor. This chapter explains the format of Boot.ini and ARC pathnames, but you still need to know how your disk is configured. Getting Ntbootdd.sys is also problematic: you need to know the name of the driver file for your SCSI controller. (Some are intuitive, like AHA154X.sys for Adaptec AHA-1542 controllers, but many are not. The easiest way to find the correct driver file name is while your system still works: you can find it in Device Manager by displaying the properties dialog box for the controller, clicking the Driver tab, and clicking Driver Details.) After you know the file name, you can expand the file from the \I386 folder on the CD (assuming that it's a driver that ships with Windows 2000) to the floppy disk and then rename it to Ntbootdd.sys. Use the Expand command, which is also in the \I386 folder. In a Command Prompt window, navigate to that folder and enter these commands, substituting the name of your driver file for *aha154x*:

```
expand -r aha154x.sy_ a:\
ren a:\aha154x.sys ntbootdd.sys
```

Now wouldn't it have been easier to make a startup floppy disk while your system was working?!

Using an MS-DOS Startup Floppy Disk

You can always start your computer using a startup disk that you create from MS-DOS or Windows 9x. This will get you to the timeworn A:\> prompt. What you can do from that point, however, depends on the format of your hard drives, the content of your startup disk, and the configuration of your computer.

If your hard drives are formatted as FAT or FAT32, you can read and modify their contents just as you could in Windows 9x. (It wouldn't be accurate to state without qualification that you can read and modify any FAT-formatted partition, because it depends on which version of MS-DOS you're using and the level of BIOS support for your hard drive. If you're trying to read a huge hard drive that you've installed in an old computer, it probably won't work. Also, you can't access dynamic disks—regardless of their format—with any operating system other than Windows 2000.)

If your hard drives are formatted using the NTFS file system—the recommended format for Windows 2000 use—you won't be able to read them using MS-DOS alone. Third-party solutions are available that let you read and write to NTFS partitions from MS-DOS. Systems Internals (*www.sysinternals.com*) offers several versions of a program called NTFSDOS, including a freeware version that can read (but not write to) NTFS partitions.

Warning Tools such as NTFSDOS can be lifesavers when you're trying to recover files from a corrupted disk, or even when you just want the convenience of accessing your NTFS partitions from Windows 9x. However, they also present a potential security risk. With these tools, no password is required to access any file. Therefore, if you're concerned about a snoop examining (or stealing) your files and your computer is not in a secure location, you should take the following precautions:

- Remove all operating systems except Windows 2000 or Windows NT from your hard drive.
- In your system BIOS, set the boot order so that the hard disk is first in the boot sequence.
- In your system BIOS, set a password that prevents unauthorized users from changing BIOS settings.
- Use encryption for your most sensitive files; NTFSDOS and similar tools can't read encrypted files. *For information, see Chapter 33, "Using Encryption."*

An MS-DOS startup floppy disk is likely to have other limitations as well:

- Without proper drivers, you might not be able to access your CD drive.
- Without proper drivers, you might not be able to access your SCSI drives.
- Without proper drivers, you won't be able to access your network.
- Even programs such as NTFSDOS can't access fault-tolerant or multivolume drives, including volume sets, mirrors, and stripe sets. *For information about these features, see Chapter 12, "Managing Disks."*

The bottom line: whether you're using a Windows 2000 startup floppy disk or an MS-DOS startup floppy disk, it's important to create it *and test it* before you need it to repair an ailing system.

Chapter 3

Working with Multiple Operating Systems

In This Chapter

Understanding How Dual Booting Works 48
Understanding the Limitations of Dual Boot Setups 49
Adding an Operating System 53
Removing an Operating System 60
Using Third-Party Alternatives 62

Microsoft Windows 2000 Professional includes *dual boot* capability, which allows you to install two or more operating systems on your computer and then select which one you want to use when you start the computer. (In fact, because it allows you to install more than two operating systems, this capability is sometimes called *multiboot* or *multiple booting*.) Why would you want to do this?

- You might want to use an application that doesn't run properly in Windows 2000. For example, many games—particularly older ones—run better in Windows 98 or even MS-DOS.
- You might need to support or test applications in different environments. If you develop applications, for example, you'll want to test them in each environment that your customers will use.
- You're afraid to take the plunge into a new operating system, and you want to keep the old one around as a security blanket.

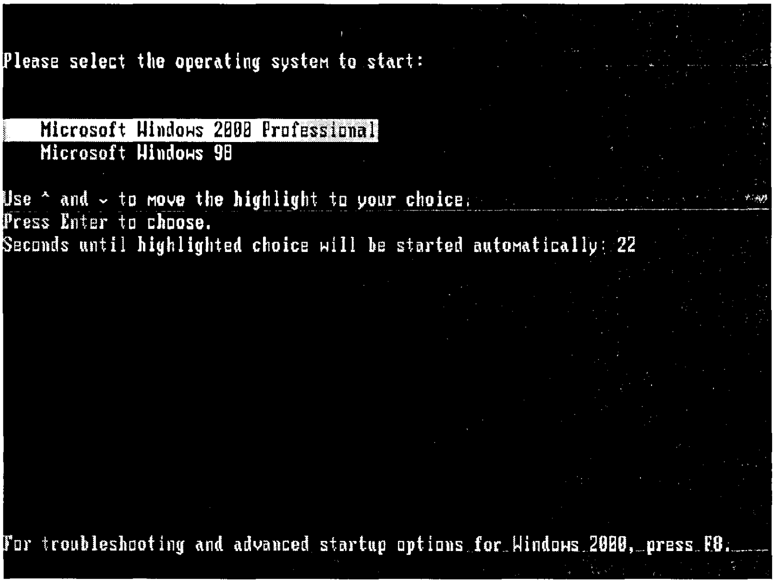
In this chapter, we explain what you need in order to use dual booting and how to set up your computer to work with multiple operating systems. We also show you how to remove an operating system if you find that you no longer need it. Finally, we look at some alternatives to the Windows 2000 boot manager.

Understanding How Dual Booting Works

The boot manager in Windows 2000 Professional supports booting from the following operating systems:

- MS-DOS
- Windows 95 or Windows 98 (but not both)
- Windows NT (multiple copies)
- Windows 2000 (multiple copies)

In Chapter 2, we explained the startup process and the role of Ntldr in displaying the boot menu. *(See "Overview of the Startup Process," page 33.)* The boot menu, shown in Figure 3-1, derives its choices from data in Boot.ini. When you choose Windows 2000 (or Windows NT, which relies on the same startup process) from the boot menu, Ntldr executes Ntdetect.com, which eventually launches Windows 2000 (or Windows NT) from the partition pointed to by the Boot.ini entry you chose. (Boot.ini specifies the partition by its disk signature and partition number, which allows you to have multiple installations of Windows 2000 and Windows NT.)



```
Please select the operating system to start:


    Microsoft Windows 2000 Professional
    Microsoft Windows 98

Use ^ and v to move the highlight to your choice.
Press Enter to choose.
Seconds until highlighted choice will be started automatically: 22









For troubleshooting and advanced startup options for Windows 2000, press F8.
```

Figure 3-1
The boot menu lets you choose which operating system to use when you start your computer.

When you choose MS-DOS, Windows 95, or Windows 98, the boot manager does something completely different. Instead of executing Ntdetect.com, Ntldr reads the contents of Bootsect.dos into memory and performs a warm reboot. The computer then executes the code in Bootsect.dos as if it were contained in the master boot record. That code continues the normal MS-DOS boot process, which loads Msdos.sys and Io.sys. This process is used by Windows 9x as well as by MS-DOS. Because the Windows 2000 boot manager looks for Bootsect.dos only in the root folder of the system partition (the first partition on the first hard disk, more commonly known as drive C), it supports only one instance of MS-DOS, Windows 3.x, or Windows 9x. However, because Windows 9x has its own dual boot capabilities, you can choose Windows 9x from the Windows 2000 boot menu, and then choose Previous Version Of MS-DOS from the Windows 9x boot menu. *For more information, see "Dual Booting with MS-DOS (and Windows 3.x)," page 53.*

System Partitions and Boot Partitions

Contrary to what common sense would tell you, the system partition has boot files, and the boot partition has system files. Don't ask why.

The *system partition* is the active partition, which is normally the first primary partition on the first hard disk. It contains the files necessary to boot Windows 2000 or another operating system.

The *boot partition* is the partition that contains Windows 2000 and its support files (in other words, the partition with the %SystemRoot% folder, which is normally called \Winnt). The boot partition can be the same as the system partition, but it doesn't need to be.

For more information about partitions, see Chapter 12, "Managing Disks."

Understanding the Limitations of Dual Boot Setups

Making it possible for different generations of operating systems to coexist on a computer was not an easy task for Microsoft. Over the years, hardware has changed significantly (remember when the first hard disks came out, with a capacity of 10 MB?!), and operating systems have evolved to keep pace. This evolution has resulted in some incompatibilities between systems, which you must consider when you set up a dual boot system.

Using Compatible File Systems

Although Windows 2000 can read and write disks that are formatted in the NTFS, FAT16, and FAT32 file systems, other operating systems cannot. Table 3-1 shows file system compatibility for each of the dual boot operating systems. *For more information about file systems, see "Selecting a File System," page 539.*

Table 3-1. File System Compatibility

Operating System	FAT16	FAT32	NTFS
MS-DOS, Windows 3.x	Yes	No	No*
Windows 95 (versions 4.00.950 and 4.00.950A; the latter is also known as SP1, OEM Service Release 1, or OSR 1)	Yes	No	No*
Windows 95 (all later versions)	Yes	Yes	No*
Windows 98	Yes	Yes	No*
Windows NT	Yes	No*	Yes
Windows 2000	Yes	Yes	Yes

*This operating system doesn't include native support for this file system, but you can obtain third-party software that lets you read (and, in some cases, write to) drives with this format. Systems Internals (*www.sysinternals.com*) offers several programs that let you use otherwise inaccessible drives, including NTFSDOS, NTFS for Windows 98, and FAT32 for Windows NT 4.0.

The limitations created by the file compatibility issue have two ramifications:

- Each operating system must be installed on a partition that's formatted with one of the file systems compatible with that operating system.
- When you boot into an operating system, it can read only the partitions that are formatted with a compatible file system.

Both of these restrictions seem obvious enough, but they mean that setting up dual boot requires some advance planning. Of course, you must place all files that you need to use while you're booted into a particular operating system on a partition with a compatible format. But you also need to be aware of how each operating system assigns drive letters to partitions as it starts up. *(For information about how Windows 2000 enumerates drives, see "Assigning a Drive Letter or Drive Path," page 215.)* Windows 9x, for example, does not reserve a drive letter for an NTFS-formatted partition; it's as if the drive doesn't exist. If you have CD-ROM drives or other partitions after the NTFS-formatted partition, those drives will have different drive letters when you boot into Windows 9x than when you boot into Windows 2000. This might not have any adverse affects. But if you have a document containing links to other files, and those links contain drive letters in their path information, the links will be broken except when you use the same operating system in which you created the linked document. Older programs that rely on private .ini files are also heavily dependent on consistent application of drive letters. (Registry entries that contain drive letters, while much more common, are actually less problematic because each operating system must maintain its own separate registry.)

Installing Each Operating System on a Separate Partition

The setup programs for all versions of Windows (including Windows NT and Windows 2000) let you install a new operating system on any partition, including one that already contains an operating system. We implore you: install each operating system on a separate partition! Doing otherwise is not worth the hassles that are bound to crop up later.

The biggest problem with installing multiple operating systems on a single partition arises with applications, many of which reside in the \Program Files folder on the boot partition (the partition where the operating system is installed, typically in the \Winnt or \Windows folder). Setup routines for some programs allow you to choose an alternative installation folder; many do not. You'll need to install each application separately from each operating system. (In other words, if you have Windows 9x and Windows 2000 on the same partition, you need to install each application two times: once from Windows 9x and once from Windows 2000.) This is also true if you install on different partitions, but in that case, you aren't installing each copy to the same location, which can cause problems such as these:

- Programs that have different versions for Windows 9x and Windows 2000 (or Windows NT) might not work because the installation from one operating system overwrites files that are needed to run the program in the other operating system.
- Preferences, options, and settings you've chosen in one operating system don't show up when you use the other operating system because each stores its own registry entries.
- If you uninstall an application, its entries still show up on the Start menu, on the Add/Remove Programs list, and throughout the registry of the other operating system—yet the program files are gone.

You might encounter still other problems with multiple operating systems on a single partition. If you're thinking about calling Microsoft Product Support Services for help with such problems, don't get your hopes up. Microsoft does not support such installations. That alone should be a clear indication that it's not a good idea!

One final argument in favor of separate partitions: if you decide to delete an operating system from your dual boot system—whether it's Windows 2000 or another operating system—you'll find that it's much easier if each one is on a separate partition.

Although we recommend that you use separate partitions for each operating system, there's no reason you can't share data on a common drive that's available to all operating systems. In fact, you might want to change the target folder location of your My Documents folder in each operating system so that it points to the same folder.

Warning If you plan to share your Outlook Express data among multiple operating systems, be sure to use the same version of Outlook Express on each operating system.

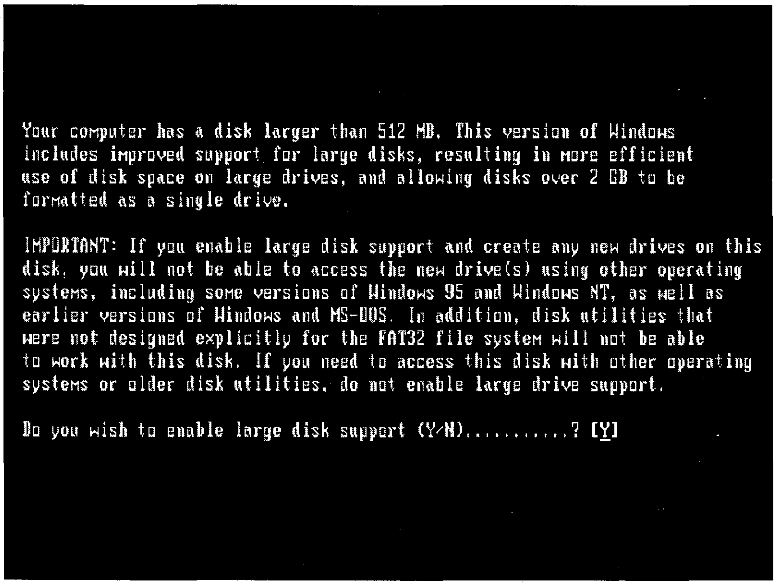
Working Around the Limitations

If you're trying to adapt a system that already has one or more operating systems installed, it might not be feasible to change its partition layout or file systems. But if it's at all possible, here's the best way to set up a system for dual booting:

1. Set up enough drives (or partitions) so that you have one for each operating system you want to be able to boot. From MS-DOS (or from a Windows 9x startup floppy disk), you can use the Fdisk program to partition your drives. (Note, however, that Fdisk's capabilities are limited to destructive deletion of existing partitions and creation of new, blank partitions. If you need to resize a partition that holds existing data, you must back up all the data, delete the partition, create a new partition and format it, and then restore the data. Alternatively, you can use a third-party partition manager, such as PartitionMagic from PowerQuest.) From Windows NT or Windows 2000, you can use Disk Management to partition your drives. Its limitations and workarounds are similar to those for Fdisk. *For details, see Chapter 12, "Managing Disks."*
2. Format the system partition (drive C) using a format that can be read and written by all operating systems you plan to install. *(Refer to Table 3-1, page 50.)* If you're going to use any operating systems other than Windows NT and Windows 2000, this means that the system partition should use FAT format.

Note

The Fdisk program included with versions of Windows that support FAT32 asks whether you want to enable large disk support:



```
Your computer has a disk larger than 512 MB. This version of Windows
includes improved support for large disks, resulting in more efficient
use of disk space on large drives, and allowing disks over 2 GB to be
formatted as a single drive.

IMPORTANT: If you enable large disk support and create any new drives on this
disk, you will not be able to access the new drive(s) using other operating
systems, including some versions of Windows 95 and Windows NT, as well as
earlier versions of Windows and MS-DOS. In addition, disk utilities that
were not designed explicitly for the FAT32 file system will not be able
to work with this disk. If you need to access this disk with other operating
systems or older disk utilities, do not enable large drive support.

Do you wish to enable large disk support (Y/N)..........? [Y]
```

Answer No if you plan to install an operating system that doesn't support FAT32 (MS-DOS, early versions of Windows 95, or Windows NT). Your choice here determines whether the Format command applies the FAT16 format (if you answer No) or the FAT32 format (if you answer Yes).

3. Format each additional partition using a format that's compatible with the operating system you plan to install there and with any other operating systems that must access the partition. (Note that you can format a partition as part of the Windows 2000 or Windows NT setup process. For Windows 9x installations, you should format before you run Setup.) To minimize the effect of shuffling drive letters, consider using FAT for the lowest numbered partitions and NTFS only for the highest numbered partitions. You might want to consider using FAT for all partitions on a dual boot system, which means that all operating systems can access all drives and that the drive letters will be the same in each operating system. However, this approach sacrifices the benefits of NTFS. *For more information, see "Selecting a File System," page 539.*

Adding an Operating System

It's possible to install operating systems in any order, and we explain how to do that in this section. Ideally, however, you should install the operating systems you want in the following order. It's much easier and less trouble prone.

1. MS-DOS
2. Windows 95 or Windows 98
3. Windows NT
4. Windows 2000

Dual Booting with MS-DOS (and Windows 3.x)

If you already have MS-DOS installed, it's a simple matter to install Windows 2000 for dual booting. From the MS-DOS prompt (or from Windows 3.x), run \I386 \Winnt.exe (not Winnt32.exe) to start the Setup program. That's it.

Note Because Windows 3.x is, in effect, a program that runs under MS-DOS, we don't treat it separately.

Because MS-DOS (and even Windows 3.x, as long as you don't install Windows 2000 to the \Windows folder) doesn't share any folders with Windows 2000, the two operating systems can safely coexist on the same partition. This is the one exception to the limitations described earlier. Even in this case, however, you might want to consider separate partitions for MS-DOS and Windows 2000. Why? If you plan to upgrade your MS-DOS or Windows 3.x to Windows 9x, it will then need to be on a separate partition.

Installing MS-DOS After Windows 2000 Is Installed

Adding MS-DOS to a system that's already running Windows 2000 is much trickier—and generally not worth the effort. You'll need to install MS-DOS (by using its setup program) or use the Sys command from an MS-DOS boot floppy disk. Either way, you'll wipe out the Windows 2000 boot sector—and, possibly, the master boot record—which you'll then need to restore. *(For details, see "Recovering the Windows 2000 Boot Loader," page 56.)* Then you'll also need to edit Boot.ini to add this line to the [operating systems] section:

```
C:\="MS-DOS"
```

Using Other Ways to Boot to MS-DOS

If you have installed Windows 9x to dual boot with Windows 2000, you can use the Windows 9x dual boot capability to launch MS-DOS. When the Windows 2000 boot menu appears, select Windows 95 or Windows 98 and press Enter. Then press F4 to boot into MS-DOS. (As an alternative to F4, you can press F8 to display the Windows 9x startup menu. Then select Previous Version Of MS-DOS.)

Note To enable booting to MS-DOS from Windows 9x, the [Options] section of Msdos.sys (a hidden, read-only file in the root folder of drive C) must contain this line:

```
BootMulti=1
```

If you often switch among Windows 2000, Windows 9x, and MS-DOS, you can set up a true triple boot system that has all three choices on the initial Windows 2000 boot menu. The details of that setup are documented in Microsoft Knowledge Base article Q157992, which you can find on the companion CD.

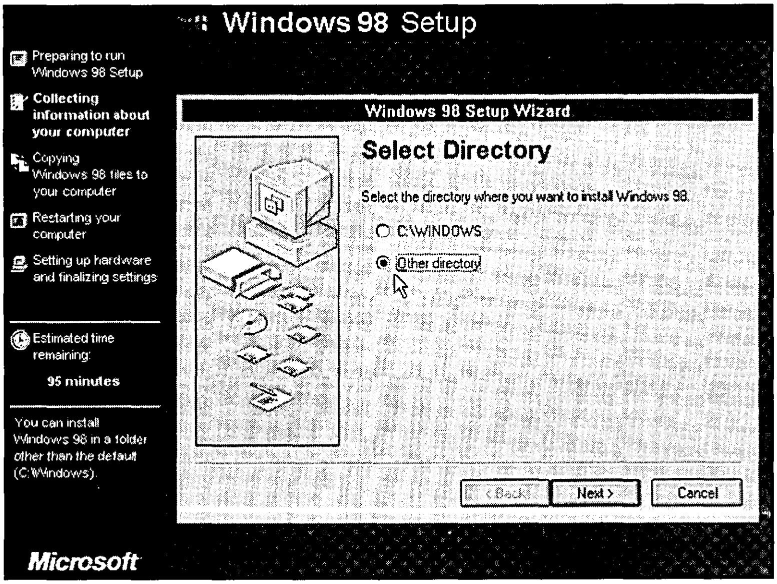
If you need to boot into MS-DOS only rarely, the simplest and most effective way might be to avoid installing MS-DOS on your hard drive altogether. Instead, use an MS-DOS boot floppy disk whenever you want to boot into MS-DOS. (Of course, you'll still need to use FAT16 for any hard disk partitions that you want to be able to use while you're running MS-DOS.)

Dual Booting with Windows 9x

The ideal setup for dual booting Windows 9x and Windows 2000 is to install Windows 9x on drive C and then install Windows 2000 on drive D (or any other partition). If you do it in that order and in those locations, life is easy. *For information about installing Windows 2000 in this fashion, see "Installing Windows 2000 on a Computer with Another Operating System," page 59.*

If, on the other hand, you feel compelled to install Windows 9x *after* you have installed Windows 2000, you've got your work cut out for you. Installing Windows 95 overwrites the Windows 2000 boot sector with its own boot sector, which prevents you from booting into Windows 2000 (or anything else managed by the Windows 2000 boot manager). The Setup program for Windows 98 is supposed to recognize the Windows 2000 (or Windows NT) boot sector, leaving it in place, and politely add itself to the Windows 2000 boot menu. However, while testing various scenarios for this book, we had some Windows 98–over–Windows 2000 installations go without a hitch and had others end up with a system that would boot only to Windows 98. So whether you're installing Windows 95 or Windows 98, you should be prepared to repair the boot sector, as explained in the accompanying sidebar, "Recovering the Windows 2000 Boot Loader." This is the procedure for installing Windows 9x:

1. Be sure that you have an up-to-date Emergency Repair Disk for your Windows 2000 installation. Better yet, make a new one right now. (Go to Start | Programs | Accessories | System Tools | Backup | Emergency Repair Disk.)
2. Be sure that drive C is formatted with a compatible FAT file system (FAT16 for early versions of Windows 95; FAT16 or FAT32 for all others). And if Windows 2000 is installed on drive C, be sure to have another drive that's formatted with a compatible FAT file system; this is where you'll install Windows 9x.
3. Install Windows 9x. Note that you can't run the Setup program for Windows 9x from Windows 2000. If you have a setup boot floppy disk (provided with some OEM versions of Windows 9x), you can use it to boot the computer and launch Setup from the CD-ROM. Alternatively, you can boot to MS-DOS (or a previous version of Windows) and launch Setup from there.
4. When Setup displays the Select Directory page, select Other Directory and specify the appropriate drive letter if Windows 2000 is already installed on drive C.


Windows 98 Setup
Preparing to run Windows 98 Setup
Collecting information about your computer
Copying Windows 98 files to your computer
Restarting your computer
Setting up hardware and finalizing settings
Windows 98 Setup Wizard
< Back
Next >
Cancel
Microsoft

Estimated time remaining: 95 minutes

You can install Windows 98 in a folder other than the default (C:\Windows).

Select Directory

Select the directory where you want to install Windows 98.

○ C:\WINDOWS

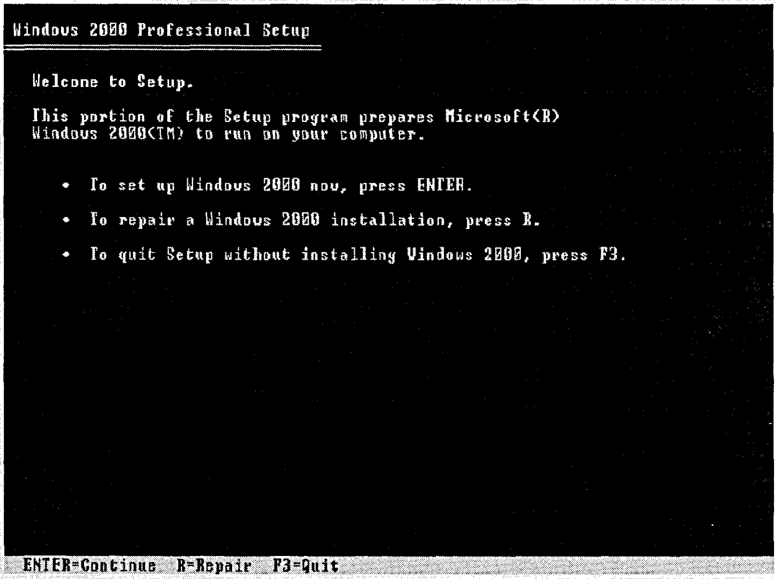
● Other directory

5. After Setup finishes, reboot your computer. If the Windows 2000 boot menu appears, you're done! (This will happen only if you're installing Window 98 and you're a little bit lucky.) If your computer immediately boots into Windows 9x, you'll need to repair the boot sector, as explained in the sidebar.

Recovering the Windows 2000 Boot Loader

Installing Windows 9x on a computer that already has Windows 2000 (or Windows NT) installed is rife with danger; the most common hazard is that the installation overwrites the boot sector, which prevents the Windows 2000 boot loader from working. Fortunately, it's fairly easy to fix:

1. Boot from the Windows 2000 Professional CD if your computer supports bootable CDs. Otherwise, boot from the Windows 2000 setup floppy disks. (To make a set, boot to another operating system—or use another computer—and run \Bootdisk\Makeboot.exe.)
2. When you reach this screen, press R to repair the installation:



```
Windows 2000 Professional Setup

  Welcome to Setup.

  This portion of the Setup program prepares Microsoft(R)
  Windows 2000(TM) to run on your computer.

     •  To set up Windows 2000 now, press ENTER.

     •  To repair a Windows 2000 installation, press R.

     •  To quit Setup without installing Windows 2000, press F3.

 ENTER=Continue  R=Repair  F3=Quit
```

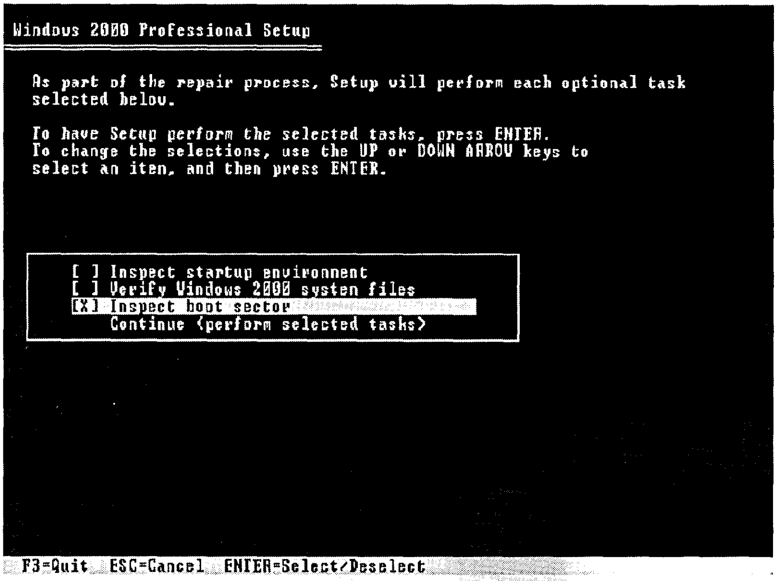
3. The screen that follows offers a choice of using recovery console (press C) or using the emergency repair process (press R). Either method should work.

   To use the recovery console, you must provide the password for the Administrator account. At the prompt, type *fixboot* to replace the boot sector, and then type *exit* to restart your computer.

(continued)

Recovering the Windows 2000 Boot Loader *(continued)*

To use the emergency repair process, press M (manual repair) and then clear all selections except Inspect Boot Sector, as shown here:



```
Windows 2000 Professional Setup

  As part of the repair process, Setup will perform each optional task
  selected below.

  To have Setup perform the selected tasks, press ENTER.
  To change the selections, use the UP or DOWN ARROW keys to
  select an item, and then press ENTER.


          [ ] Inspect startup environment
          [ ] Verify Windows 2000 system files
          [X] Inspect boot sector
              Continue (perform selected tasks)

F3=Quit  ESC=Cancel  ENTER=Select/Deselect
```

Follow the on-screen instructions to complete the repair.

This process copies the current boot sector to Bootsect.dos and then replaces it with the Windows 2000 boot sector. (Therefore, you can also use this procedure to replace a lost or corrupted Bootsect.dos file. Before you begin the steps just outlined, boot from an MS-DOS floppy disk and type *sys c:* to overwrite the Windows 2000 boot sector with the MS-DOS/Windows 9x boot sector. Then follow the steps we described to reverse the damage you've just inflicted, creating a new Bootsect.dos in the process.)

Regardless of the order in which you install the operating systems, you'll need to boot into each operating system and then install all the applications you want to use with that system. Unless you never plan to uninstall a particular application, don't point the separate installations to the same folder. Even though it wastes disk space with duplicate files, you're much better off installing each copy separately. For the simplest setup, install each application to a subfolder of the \Program Files folder on the same partition as the operating system from which you're installing.

Sharing a Paging File

One way you *can* save disk space in a dual boot system is to use the same virtual memory paging file (sometimes called a *swap file*) for each operating system. Because

(continued)

Sharing a Paging File *(continued)*
each operating system uses its paging file only when it's running (and the file doesn't need to be saved between sessions), you can direct Windows 9x to use the Windows 2000 paging file (as long as the file is on a FAT partition). To do that, follow these steps:

1. Open the System.ini file in the Windows 9x folder (normally C:\Windows).
2. In the [386Enh] section, add a new line (changing the *d* shown here to the letter of the drive where your Windows 2000 paging file resides):

```
pagingfile=d:\pagefile.sys
```

Now you can delete the \Windows\Win386.swp file. (You can't do this from Windows 9x.) The next time you start Windows 9x, it'll use the Windows 2000 paging file. *For more information about virtual memory, see Chapter 43.*

Dual Booting with Windows NT

Windows 2000 and Windows NT 4 coexist nicely, and you can have multiple installations of each (as long as each is on a separate partition) if you're so inclined. But before you add Windows 2000 to your Windows NT system, you must be aware of two gotchas:

- If you're using NTFS with Windows NT, you must install Service Pack 4 (SP4) or later before you install Windows 2000. Windows 2000 uses a new version of NTFS (sometimes called NTFS 5) that adds features such as disk quotas and encryption. The original release of Windows NT can't read or write this new version, but SP4 contains an updated Ntfs.sys driver that enables Windows NT 4 to read and write to NTFS 5 volumes. (The new features are unavailable from Windows NT, however.) When you install Windows 2000, it converts *all* mounted NTFS volumes to the new format.
- If your computer is a member of a domain, each installation of Windows NT and Windows 2000 must use a different computer name. The computer account on the domain controller associates the computer name with each installation's unique security identifier (SID). As a security measure, the domain controller refuses entry when a logon request comes from a SID that's different from the one associated with that computer name in its security database. You simply need to create a computer account—with a different computer name—on the domain controller for each Windows NT/2000 installation that will participate in the domain.

Importing Complex Disk Configurations

If you install Windows 2000 on a system that already has Windows NT installed and if the system has existing volume sets, stripe sets, stripe sets with parity, or mirror sets, you must import the disk configuration so that Windows 2000 can access those volumes. To do so, follow these steps:

1. In Windows NT, use Disk Administrator to save the disk configuration to a floppy disk. (In Disk Administrator, choose Partition | Configuration | Save.)
2. After you install Windows 2000, use Disk Management to import the configuration. (In Disk Management, choose Action | Restore Basic Disk Configuration.)

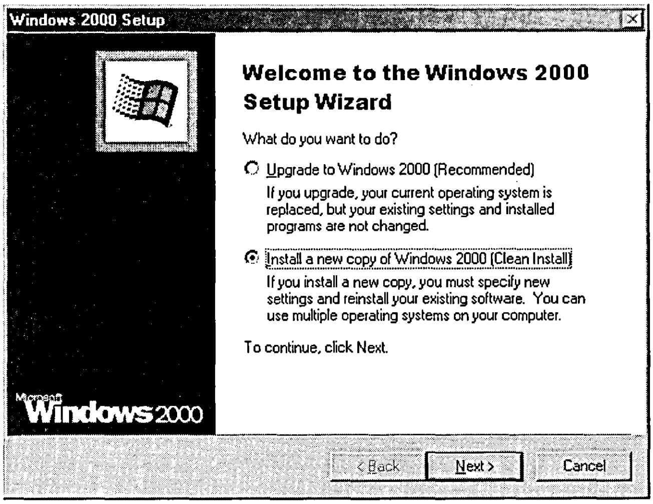
Installing Windows NT After Windows 2000 Is Installed

Because of the lack of NTFS 5 support in the original version of Windows NT, adding Windows NT to a system that already has Windows 2000 installed is a little trickier. The system partition must be formatted as FAT16, and you must install to a FAT16 partition; as shipped, Windows NT doesn't support FAT32 or NTFS 5. To install Windows NT, run Winnt32.exe from the SP4 (or later) CD—not from the Windows NT CD. After installing Windows NT and applying the service pack, you can also convert any or all of the FAT16 partitions to NTFS by using the Convert command. (At a command prompt, type *convert d: /fs:ntfs*, where *d* is the letter of the drive you want to convert.)

Installing Windows 2000 on a Computer with Another Operating System

You've made the wise choice: you installed your other operating system(s) before installing Windows 2000. Now choosing to install Windows 2000 as an additional operating system (instead of upgrading your current one) is a simple matter of making a few selections in the Windows 2000 Setup Wizard.

Start Setup from your existing operating system. Then, on the Welcome page (see Figure 3-2), select Install A New Copy Of Windows 2000 (Clean Install). On the Select Special Options page, click Advanced Options (see Figure 3-3), and then select I Want To Choose The Installation Partition During Setup. After that, it should be clear sailing.



Windows 2000 Setup

Welcome to the Windows 2000 Setup Wizard

What do you want to do?

○ Upgrade to Windows 2000 (Recommended)

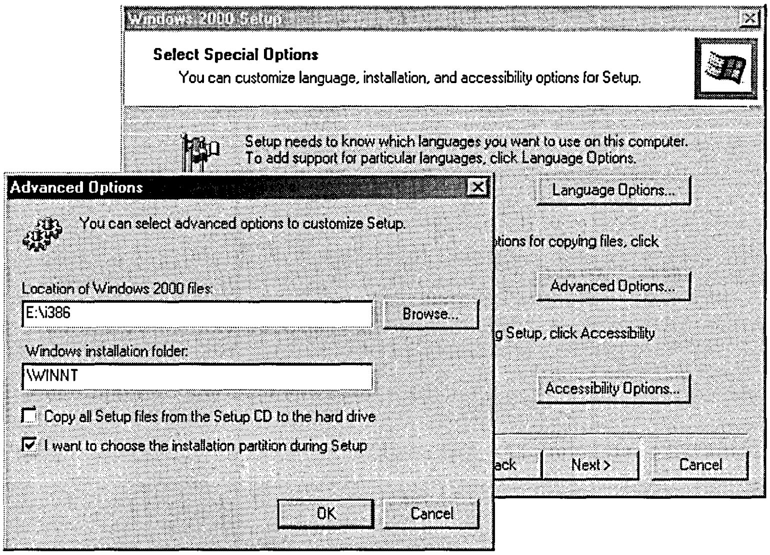
If you upgrade, your current operating system is replaced, but your existing settings and installed programs are not changed.

● Install a new copy of Windows 2000 (Clean Install)

If you install a new copy, you must specify new settings and reinstall your existing software. You can use multiple operating systems on your computer.

To continue, click Next.

Figure 3-2
To set up Windows 2000 for dual booting, you must select Clean Install.



Windows 2000 Setup

Select Special Options

You can customize language, installation, and accessibility options for Setup.

Setup needs to know which languages you want to use on this computer. To add support for particular languages, click Language Options.

ptions for copying files, click

g Setup, click Accessibility

Advanced Options

You can select advanced options to customize Setup.

Location of Windows 2000 files: E:\i386

Windows installation folder: \WINNT

□ Copy all Setup files from the Setup CD to the hard drive

☑ I want to choose the installation partition during Setup

Figure 3-3
Selecting the second check box in the Advanced Options dialog box ensures that you retain control over where Windows 2000 is installed.

Removing an Operating System

So you no longer play the game that required Windows 98. (Or maybe the game now offers Windows 2000 support.) Or the folks you support have all migrated to Windows 2000, so you no longer need to test in other environments. Or, after a fastidious evaluation of different operating systems, you've decided on one (we hope it's Windows 2000!), and you want to jettison the other. No problem.

The easiest way to remove any operating system from a dual boot system is to delete its entry from Boot.ini. Then boot into a remaining operating system and delete the files related to the operating system you want to remove. Or, for a more aggressive approach, you can format the partition of the operating system you removed from Boot.ini.

Removing Windows 9x or MS-DOS

Depending on how Windows 9x or MS-DOS was installed on your computer, you might have an uninstall option, which is intended to restore your computer's previous operating system, whatever that was. Forget about it. The uninstall option is unlikely to work properly, and it *is* likely to mess up your Windows 2000 configuration. (If you ignore our advice and proceed with the uninstall option, be sure to have an Emergency Repair Disk on hand!) If you're trying to remove Windows 9x or MS-DOS and you want to leave Windows 2000 in place, follow these steps:

1. Boot into Windows 2000.

2. Edit Boot.ini to delete the C:\="Microsoft Windows" entry in the [operating systems] section. (The easiest way to open Boot.ini for editing is with the Start | Run command: simply type *c:\boot.ini* and click OK.)

3. Remove the files that are used only with the operating system you're deleting. This would include everything in the \Windows, \Program Files, and \DOS folders. Be sure that you're deleting the folders from the Windows 9x partition—not from the partition for an operating system you plan to keep. And before you deep-six them, be sure to move any documents or other files you want to keep. In particular, be sure that you locate the My Documents folder (which is sometimes located in a subfolder of \Windows\Profiles).

   If you're certain that you don't need *any* files from the Windows 9x partition (or if you've already moved them to another drive), you can take the scorched earth approach and format the partition instead of deleting individual folders and files. (Don't format if Windows 9x or MS-DOS was installed on the system partition, however.)

4. Delete the Windows 9x boot files—Autoexec.bat, Config.sys, Io.sys, Msdos.sys, and Command.com—from the root folder of drive C. If you don't plan to reinstall any version of Windows 9x or MS-DOS, you can safely delete Bootsect.dos.

Removing Windows 2000 or Windows NT

If you have multiple installations of Windows 2000 or Windows NT, you can delete any one of them using the same procedure as detailed in the first three steps of the previous section. (The My Documents folder and other data files that you might want to keep reside under \Documents And Settings or \Winnt\Profiles; be sure to check those locations before you begin nuking files and folders.)

If you want to remove *all* Windows 2000 and Windows NT installations and revert to Windows 9x or MS-DOS only, the process is actually quite simple:

1. If you want to keep any files that are on an NTFS volume, move them to a FAT volume or other media (such as a Zip disk). Once you carry out the next steps, you won't be able to access your NTFS volumes.
2. Boot from an MS-DOS or a Windows 9x startup floppy disk. (not Win ME)
3. Type *sys c:* to overwrite the Windows 2000 boot sector.
4. If the operating system you're removing is on a FAT volume and you don't want to format the partition, you can remove the \Winnt, \Program Files, and \Documents And Settings folders after you move any data files you want to keep. In addition, you can delete the Windows 2000 boot files—Ntldr, Ntdetect.com, Boot.ini, Ntbootdd.sys, and Bootsect.dos—from the root folder of drive C.
5. Use Fdisk to delete any NTFS-formatted partitions, and then create new partitions in their place. Then format the partitions.

Using Third-Party Alternatives

The Windows 2000 boot manager does a serviceable job in most situations. The following tools, which are available from other vendors, offer some additional flexibility, convenience, and capabilities. For more information about these programs and links to the vendors, see the companion CD.

Partition Managers

These alternatives to Fdisk let you resize a partition without destroying the data it contains, and they offer other features (such as converting NTFS to FAT32) as well:

- PartitionMagic, from PowerQuest Corporation *(www.powerquest.com)*
- Partition Commander, from V Communications *(www.v-com.com)*

Boot Managers

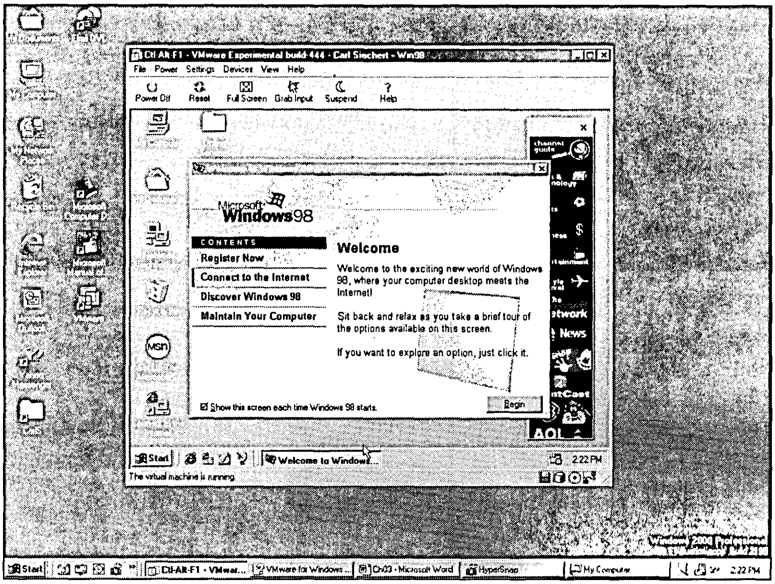
These alternatives to the Windows 2000 boot manager let you install more than one copy of Windows 9x and provide better support for additional operating systems:

- BootMagic, from PowerQuest Corporation
- BootPart, from Gilles Vollant Software *(www.winimage.com/bootpart.htm)*
- System Commander Deluxe, from V Communications

Something Completely Different

A company called VMware *(www.vmware.com)* has created a completely different alternative that allows you to use multiple operating systems. Their product, also called VMware, sets up multiple virtual machines within your Windows 2000 host machine. (See Figure 3-4.) The virtual machine runs in a window (or you can run it full screen), and it looks and acts just like the real thing—starting with the BIOS routine that runs when you click the Power On button. It can give you access to all your computer's hardware resources, including network cards and CD-ROM drives. You can even set up an entire "network" of virtual machines on a single computer. It's a truly remarkable program, and it seems to work much better than earlier emulation programs.

The main drawback to this approach is that it's much slower than running a single operating system. For that reason alone, it's not an appropriate way to play your Windows 98 shoot-'em-up games. But it's a great test platform. For example, with VMware you can install new applications and test them on a virtual machine—without any concern that they'll harm your "real" computer or be impossible to uninstall if you decide you don't like them. You can set up a virtual machine so that it reverts to its original configuration at the end of each session, which allows you to test applications on a known configuration. And it's a nifty tool for book authors: we used it to obtain seemingly impossible screen captures, such as the boot menu, the logon screen, blue screens, and so on.



Welcome

Welcome to the exciting new world of Windows 98, where your computer desktop meets the Internet!

Sit back and relax as you take a brief tour of the options available on this screen.

If you want to explore an option, just click it.

☑ Show this screen each time Windows 98 starts.

Figure 3-4
VMware runs a virtual machine—which can run any operating system—within a Windows 2000 host.

Hardware Solutions

Yet another way to boot from multiple operating systems is to install each one on a separate hard drive—and then have a way to select which hard drive you want to boot from. This is easy to do with removable hard drives; you simply install the hard drive with the operating system and files you want before you turn on your computer. A number of vendors make removable drive assemblies. With these devices, you install a drawer with a connector in your computer case. You then install an ordinary hard drive into a carrier that slides into the drawer.

UniPress Software *(www.unipress.com/winux)* offers a product called Winux. Winux is a hard drive selector switch that lets you switch among three bootable drives installed in a computer. It effectively works like a removable hard drive system; you select which drive you want before you start your computer, and your other drives are unavailable. The difference is the convenience of selecting a drive by pressing a button instead of removing one and sliding in another.

Part 2

Using Management Tools

Chapter 4
Using and Customizing Microsoft Management Console 67

Chapter 5
Monitoring System and Application Activities with Event Viewer 83

Chapter 6
Finding Files with the Indexing Service 95

Chapter 7
The Windows 2000 Shell: Beyond the Basics 117

Chapter 4

Using and Customizing Microsoft Management Console

In This Chapter

Running MMC Consoles 69

Using MMC Consoles 71

Creating Your Own MMC Consoles 73

Microsoft Management Console (MMC) is an application that hosts administrative tools. If you've explored your system a bit, you've probably already encountered MMC in various contexts. If you've right-clicked My Computer and chosen the Manage command, for example, you've seen MMC in action hosting a set of tools known as Computer Management. If you've opened Administrative Tools in Control Panel and checked out some of the options there, you've seen some other examples of MMC.

By itself, MMC performs no administrative services. Rather, it acts as host for one or more snap-ins. The snap-ins do the administrative work. MMC's job is to provide a certain degree of user-interface consistency so that you or the users you support see more or less the same style of application each time you need to carry out some kind of management task.

The combination of MMC with one or more snap-ins is called an MMC console. A large number of MMC consoles come with Microsoft Windows 2000 Professional. Because Microsoft is encouraging independent hardware and software vendors to use MMC for their own administrative tools, you quite possibly have some third-party MMC consoles on your system in addition to those that come with the operating system. Table 4-1 lists the MMC consoles supplied with Windows 2000 Professional. You'll find most of these in your %SystemRoot%\System32 folder.

Table 4-1. MMC Consoles Included with Windows 2000

File Name	Friendly Name
Adsiedit.msc*	ADSI Edit
Certmgr.msc	Certificates
Ciadv.msc	Indexing Service
Comexp.msc	Component Services
Compmgmt.msc	Computer Management
Devmgmt.msc	Device Manager
Dfrg.msc	Disk Defragmenter
Diskmgmt.msc	Disk Management
Eventvwr.msc	Event Viewer
Faxserv.msc	Fax Service Management
Fsmgmt.msc	Shared Folders
Gpedit.msc	Group Policy
Ias.msc	Internet Authentication Service
Iis.msc**	Internet Information Services
Lusrmgr.msc	Local Users And Groups
Msinfo32.msc	System Information
Ntmsmgr.msc	Removable Storage
Ntmsoprq.msc	Removable Storage Operator Requests
Perfmon.msc	Performance
Secpol.msc	Local Security Settings
Services.msc	Services
Sidwalk.msc*	SIDWalker Security Manager
Wmimgmt.msc	Windows Management Infrastructure

*Installed as part of Windows 2000 Support Tools.

**Installed as part of Internet Information Services.

The creation of snap-ins requires programming expertise and knowledge about ActiveX (because snap-ins are ActiveX controls). That topic lies beyond the scope of this book. (You can learn more about programming snap-ins by typing *mmc* on a command line, choosing Microsoft On The Web from MMC's Help menu, and then choosing either Snap-In Gallery or Product News from the submenu. These choices take you to Web sites where you can find useful information about snap-in development.)

You don't have to be a programmer, however, to make your own custom MMC consoles. All you need to do is run MMC and add one or more of the snap-ins available on your system. (You'll find a list of these in one of MMC's dialog boxes.)

Alternatively, you can customize some of the MMC consoles supplied by Microsoft or others, simply by adding or removing snap-ins.

Why might you want to do this? Because neither Microsoft nor any other vendor can anticipate your every need and desire. Perhaps you'd like to take some of the functionality from two or more existing MMC consoles and combine them into a single console. (You might, for example, want to combine the Fax Management console with the Event Viewer console, the latter filtered to show only those events generated by the Fax Service.) Or perhaps you would like to simplify some of the existing consoles by removing snap-ins that you seldom use.

You also might find MMC customization worthwhile if you support others in your organization who occasionally need to perform administrative tasks. You can set up consoles that supply only the functionality that your colleagues need, removing or disabling components that might distract or confuse. Certain of the snap-ins available on your system, for example, are designed to administer remote as well as local computers. If the user you're supporting needs to be able to administer only his or her own machine, you might want to create a custom console for that person that has remote-administrative capabilities disabled.

In this chapter, we explore MMC's user interface and the steps required to create custom MMC consoles.

Running MMC Consoles

Many of the MMC tools provided with the operating system are stored in the Administrative Tools folder. To get there, choose Start | Programs | Administrative Tools, or Start | Control Panel | Administrative Tools.

Troubleshooting

Each time you open an MMC instance, Windows 2000 creates a 16-MB temporary file in your %Temp% folder. If the disk on which that folder resides is full, or if you don't have permission to create a file there, you will receive an error message and MMC will not start. If this happens, free some disk space or make sure that you have the appropriate permissions.

By default, MMC consoles have the extension .msc, and .msc files are associated by default with MMC. Thus you can run any MMC console by double-clicking its file name in a Windows Explorer window or by specifying the file name on a command line—using the Start menu's Run command, a Command Prompt window, a shortcut, a batch file, or a script.

MMC consoles can be run in author mode or in three varieties of user mode. Author mode gives you full access to MMC's menus and options. In its user modes, elements of MMC's functionality are removed. *(To learn about the different user modes, see "Choosing Among MMC's Three User Modes," page 80.)*

When you run an MMC console, the console by default runs in the mode in which it was last saved. But you can always run any console in any mode.

Running a User-Mode Console in Author Mode

To run a console in author mode, right-click its entry in a Windows Explorer window and choose Author from the shortcut menu. Alternatively, you can run a console in author mode using the following command-line syntax:

```
filename.msc /a
```

where *filename* is the name of the console file. (You might need to include a path specification if Windows 2000 can't find your console file. But most of the consoles supplied with the operating system are in %SystemRoot%\System32, and you don't need to specify a path to execute those.) So, for example, to open Computer Management in author mode, you could type

```
compmgmt.msc /a
```

Running a Console and Specifying a Target Computer

Many of the consoles supplied by Microsoft are set up to operate on the local computer by default, but—provided you have the appropriate permissions—they can also be used to manage remote computers. To open such a console and specify a target computer, use this command-line syntax:

```
filename.msc /computer=computername
```

For example, to run Computer Management on your local computer and manage the computer whose network name is Fafner, you could type

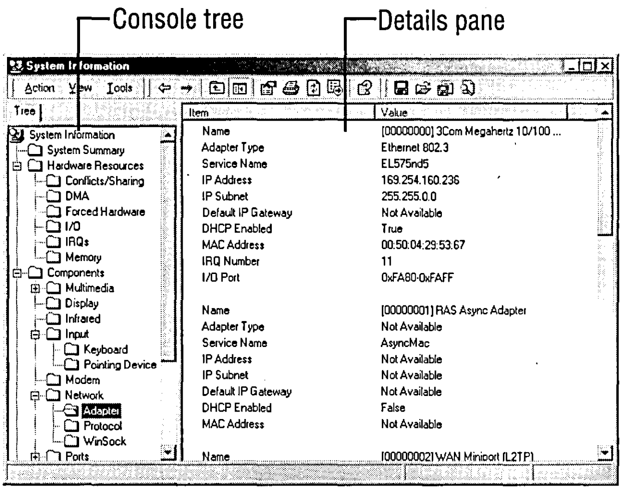
```
compmgmt.msc /computer=fafner
```

Be aware that if you use the /Computer switch with a console that has not been set up to allow remote-computer management, you do not get an error message. Instead, you simply get the console applied to the default (typically, the local) computer. In the console tree, you can look at the top-level entry for a snap-in to confirm that you're working with the right target computer.

Note also that some of the Windows 2000–supplied consoles that are designed to work with remote as well as local computers include a menu command for connecting to a different computer. The Computer Management console (Compmgmt.msc), for example, lets you switch from one computer to another while the console is running. Others, such as Shared Folders (Fsmgmt.msc), can be used with remote computers, but these consoles manage the local computer unless you specify a different target computer on the command line.

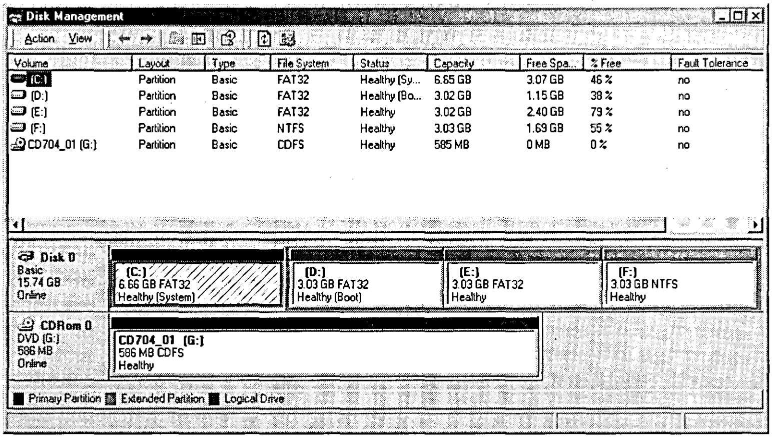
Using MMC Consoles

Notwithstanding the fact that MMC is intended to provide user-interface consistency across administrative applications, actual MMC consoles can take on quite a variety of appearances. Figures 4-1 and 4-2 show rather different-looking examples of MMC consoles provided with Windows 2000 Professional. Figure 4-1, the System Information console, includes a window divided into two vertical panes. The console's menu includes three commands—Action, View, and Tools—and the toolbar includes 13 icons. Figure 4-2, the Disk Management console, has a window divided horizontally, a top-level menu without Tools, and a much smaller toolbar.



Item	Value
Name	[00000000] 3Com Megahertz 10/100 ...
Adapter Type	Ethernet 802.3
Service Name	EL575nd5
IP Address	169.254.160.236
IP Subnet	255.255.0.0
Default IP Gateway	Not Available
DHCP Enabled	True
MAC Address	00:50:04:29:53:67
IRQ Number	11
I/O Port	0xFA80-0xFAFF
Name	[00000001] RAS Async Adapter
Adapter Type	Not Available
Service Name	AsyncMac
IP Address	Not Available
IP Subnet	Not Available
Default IP Gateway	Not Available
DHCP Enabled	False
MAC Address	Not Available
Name	[00000002] WAN Miniport (L2TP)

Figure 4-1
Most of the MMC consoles that come with Windows 2000 include a console tree and a details pane.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Tolerance
(C:)	Partition	Basic	FAT32	Healthy (Sy...	6.65 GB	3.07 GB	46 %	no
(D:)	Partition	Basic	FAT32	Healthy (Bo...	3.02 GB	1.15 GB	38 %	no
(E:)	Partition	Basic	FAT32	Healthy	3.02 GB	2.40 GB	79 %	no
(F:)	Partition	Basic	NTFS	Healthy	3.03 GB	1.69 GB	55 %	no
CD704_01 (G:)	Partition	Basic	CDFS	Healthy	585 MB	0 MB	0 %	no

Disk 0
Basic
15.74 GB
Online

(C:)
6.66 GB FAT32
Healthy (System)

(D:)
3.03 GB FAT32
Healthy (Boot)

(E:)
3.03 GB FAT32
Healthy

(F:)
3.03 GB NTFS
Healthy

CDRom 0
DVD (G:)
586 MB
Online

CD704_01 (G:)
586 MB CDFS
Healthy

Figure 4-2
Some MMC consoles, like this one, bear only minimal resemblance to the one shown in Figure 4-1.

In short, beyond the presence of an Action menu and a View menu, the consoles shown in Figures 4-1 and 4-2 bear little resemblance to each other. That's because MMC is designed to be extremely flexible. Snap-ins can add elements to the MMC user interface (the Tools menu in Figure 4-1, for example), and console designers (including you, of course, if you decide to create custom consoles) can hide or display UI elements as needs dictate.

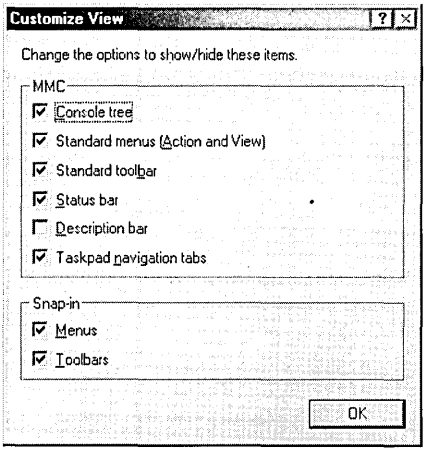
Nevertheless, *most* of the consoles that come with your operating system look somewhat like Figure 4-1, and we can make a few generalizations about their use.

- **Using the console tree and the details pane.** If the console is divided into panes vertically, the one on the left is called the *console tree* and the one on the right is called the *details pane*. The console tree functions pretty much the way the Folders bar in Windows Explorer does. It shows the organization of the console and allows easy navigation between snap-ins. Outline controls in the console tree function just the way they do in Windows Explorer. The vertical split bar between the console tree and the details pane can be dragged to the left or right, like its counterpart in Windows Explorer.

  The details pane shows information related to the item currently selected in the console tree. In Figure 4-1, for example, Components\Network\Adapter is selected in the console tree, and the details pane shows the properties of the local system's network adapter.

- **Using the action and view menus.** The Action menu, if present, provides com•mands specific to the current snap-in. In other words, this is the menu you use to carry out administrative tasks. The View menu, if present, lets you choose among alternative ways of presenting information. In many MMC consoles, for example, the View menu offers Large Icons, Small Icons, List, and Details commands, just like the View menu in Windows Explorer. The View menu might also include a Customize command. This command presents the dialog box shown in Figure 4-3, which allows you, among other things, to hide or display the console tree. If you're working in relatively low resolution and want more screen space for the details pane, you might find it useful to suppress the console tree temporarily.

- **Using shortcut menus.** Whether or not an Action menu is present, you'll probably find that the easiest way to carry out an administrative task is to right-click the relevant item in the console tree and choose an action from the item's shortcut menu. That's because the shortcut menu *always* includes all the actions available for the selected item. (If you don't immediately find the command you need, look for an All Tasks command; the action you want is probably on the All Tasks submenu.) The shortcut menu also always includes a Help command.



Change the options to show/hide these items.

MMC

☑ Console tree

☑ Standard menus (Action and View)

☑ Standard toolbar

☑ Status bar

□ Description bar

☑ Taskpad navigation tabs

Snap-in

☑ Menus

☑ Toolbars

Figure 4-3
You can use the Customize View dialog box to control various elements of the MMC display.

- **Working with content in the details pane.** If the details pane provides a tabular presentation, like the one shown in Figure 4-1, you can manipulate content using the same techniques you use in Windows Explorer. You can sort by clicking column headings, control column width by dragging the borders between column headings (double-click a border to make a column just wide enough for the widest entry), and rearrange columns by dragging headings.

  To hide or display particular columns, look for a Choose Columns command on the View menu. Here you can specify which columns you want to see, as well as the order in which you want to see them.

- **Exporting data to text or .csv files.** Many of the MMC consoles that come with Windows 2000 include commands for saving data in their own native formats. You can save Event Viewer event logs to .evt files, for example, or a system summary from System Information to an .nfo file. In most consoles that produce tabular displays, however, you can also use an Export List command to generate a tab-delimited or comma-delimited text file, suitable for viewing in a word processor, spreadsheet, or database program. If this command is available, you'll find it on the Action menu or any shortcut menu.

Creating Your Own MMC Consoles

Creating your own MMC console or modifying an existing one involves the following steps (not necessarily in this order):

- Run MMC with no snap-in, or open an existing MMC console in author mode.
- Display the console tree if it's not already visible.

- Add folders to the console tree if appropriate for your needs.
- Add or remove snap-ins and, if appropriate, extensions (modules that extend the functionality of snap-ins).
- Add or remove ActiveX controls and Internet links if appropriate.
- Add taskpad views (customized pages that appear within the details pane of a snap-in) if appropriate.
- Manipulate windows and other display elements to suit your taste.
- Add items to the Favorites menu if appropriate.
- Name the console and choose an icon for it.
- Choose author mode or one of the three user modes.
- Further restrict user options if appropriate.
- Use the Console menu to save your .msc file.

Running MMC with No Snap-In

To run MMC with no snap-in, simply type *mmc* on a command line. An empty, author-mode MMC console appears, looking like Figure 4-4. Note the following:

- In author mode, MMC includes an additional menu bar (Console, Window, Help).

  You'll use this menu bar to build your custom console. If you save the console in user mode, this top-level menu bar disappears.
- The Console Root window that appears by default is a child window.

MMC is a multiple-document interface (MDI) application, although most of the consoles supplied with Windows 2000 do their best to disguise this fact. You can create consoles with multiple child windows, and those windows can be maximized, minimized, restored, resized, moved, cascaded, and tiled.

Displaying the Console Tree

If the console tree is not visible in the application you're creating or modifying, choose Customize View from the View menu. In the Customize View dialog box (see Figure 4-3, page 73), select the Console Tree check box. You can also use this dialog box to control other elements of the MMC display.

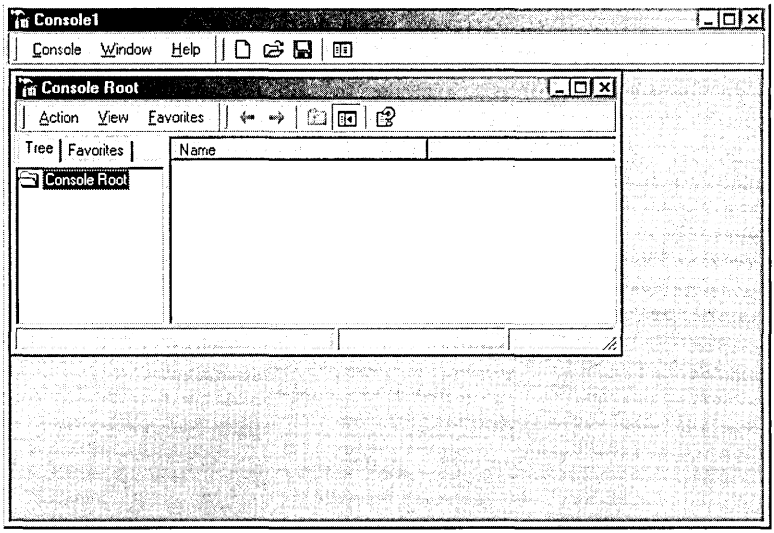


Figure 4-4
An empty, author-mode MMC console looks like this.

Adding Folders to the Console Tree

If the console you're designing will include several snap-ins, you might want to consider using folders to create logical subdivisions within your console tree. To see how folders can be helpful, check out the Computer Management console (right-click My Computer and choose Manage, or run Compmgmt.msc) included with Windows 2000. Computer Management uses three folders—System Tools, Storage, and Services And Applications. These folders allow the user to control the amount of detail shown in the console tree and simplify navigation from one point in the application to another.

To add one or more folders to an MMC console:

1. From the Console menu, choose Add/Remove Snap-In (or press Ctrl+M).
2. In the Snap-Ins Added To field of the Add/Remove Snap-In dialog box, choose the parent of the new folder. (In a brand-new MMC application, this folder must be Console Root.)
3. Click Add.
4. In the Add Standalone Snap-In dialog box, select Folder and then click Add. Repeat if you want more folders; then click Close.
5. In the Add/Remove Snap-In dialog box, click OK.
6. In the console tree, right-click the new folder, choose Rename, and supply a meaningful name.

Adding Snap-Ins and Extensions

To add a snap-in to your console:

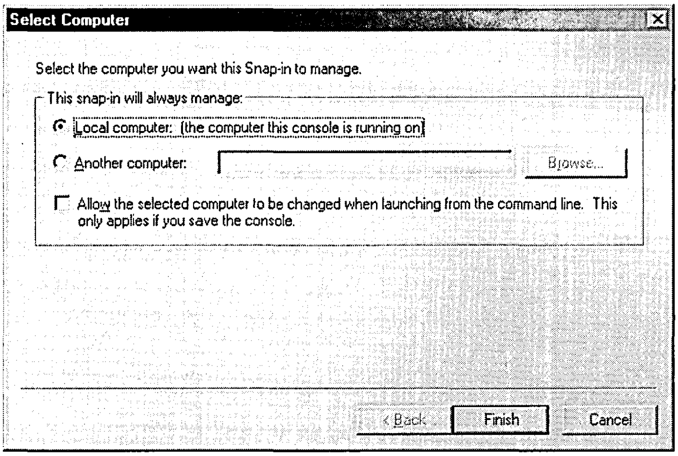
1. From the Console menu, choose Add/Remove Snap-In (or press Ctrl+M).
2. In the Snap-Ins Added To field of the Add/Remove Snap-In dialog box, choose the parent of the new snap-in. This folder can be Console Root or a folder that you've already added.
3. Click Add.
4. In the Add Standalone Snap-In dialog box, select the snap-in you want and then click Add.

   If the selected snap-in supports remote management, you might see a dialog box similar to the one shown in Figure 4-5. Supply the name of the computer you want to manage. Also select the check box if you want the user of your custom console to be able to specify the target computer by means of a command-line switch. (This option is not available for all remote-management snap-ins.) Then click Finish.
5. When you have finished adding snap-ins, click Close.
6. Some snap-ins come with optional extensions. You can think of these as snap-ins for snap-ins—modules that provide additional functionality to the selected snap-in. To add an extension to a snap-in, select it in the Add/Remove Snap-In dialog box and then click the Extensions tab. There you can select the extensions that you want to use.
7. When you have finished adding snap-ins and extensions, click OK.

Adding ActiveX Controls and Internet Links

The Add Standalone Snap-In dialog box includes the entries ActiveX Control and Link To Web Address, as well as snap-ins. If you choose ActiveX Control, a new wizard appears, allowing you to choose and configure the control you want to add. The control itself arrives in the details pane when you select its name in the console tree.

If you choose Link To Web Address, a dialog box appears that lets you specify a hyperlink or browse to an Internet resource. The hyperlink you enter does not have to be a Web URL. It can be another kind of Internet URL (a mailto, for example) or a link to a local or network folder. If you do specify a Web link, MMC displays the Web content in the details pane when you select the link in the console tree. If the item must be downloaded from the Internet, you must already be online; MMC does not activate a dial-up connection for you. If you specify a local or remote folder, selecting that folder in the console tree causes MMC to display the folder's contents in the details pane.



Select the computer you want this Snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

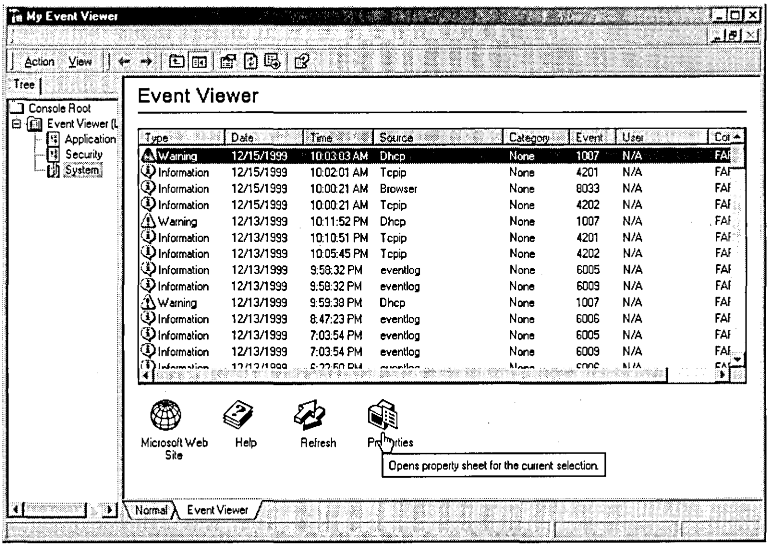
○ Another computer: [ ] Browse...

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Figure 4-5
If your snap-in can manage a remote computer, you will see a dialog box similar to this.

Adding Taskpad Views

A taskpad is a customized page that appears within the details pane of a snap-in. The main value of a taskpad is that it lets you create icons that encapsulate menu commands, command strings, scripts, URLs, and shortcuts to Favorites items. Figure 4-6 shows a taskpad view with four such task shortcuts.



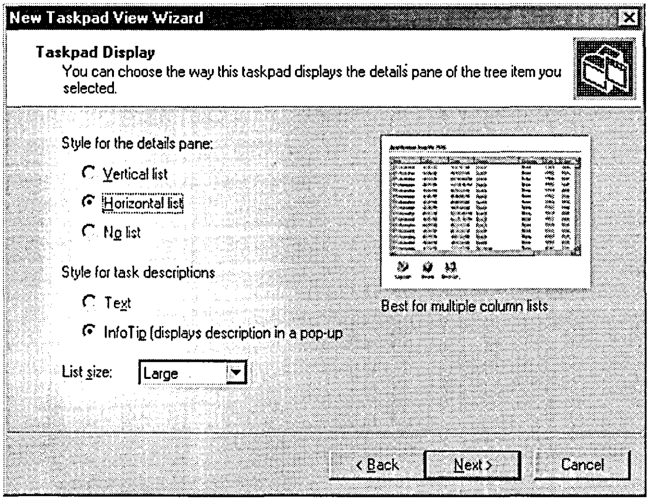
Type	Date	Time	Source	Category	Event	User	Cor
Warning	12/15/1999	10:03:03 AM	Dhcp	None	1007	N/A	FAI
Information	12/15/1999	10:02:01 AM	Tcpip	None	4201	N/A	FAI
Information	12/15/1999	10:00:21 AM	Browser	None	8033	N/A	FAI
Information	12/15/1999	10:00:21 AM	Tcpip	None	4202	N/A	FAI
Warning	12/13/1999	10:11:52 PM	Dhcp	None	1007	N/A	FAI
Information	12/13/1999	10:10:51 PM	Tcpip	None	4201	N/A	FAI
Information	12/13/1999	10:05:45 PM	Tcpip	None	4202	N/A	FAI
Information	12/13/1999	9:58:32 PM	eventlog	None	6005	N/A	FAI
Information	12/13/1999	9:58:32 PM	eventlog	None	6009	N/A	FAI
Warning	12/13/1999	9:59:38 PM	Dhcp	None	1007	N/A	FAI
Information	12/13/1999	8:47:23 PM	eventlog	None	6006	N/A	FAI
Information	12/13/1999	7:03:54 PM	eventlog	None	6005	N/A	FAI
Information	12/13/1999	7:03:54 PM	eventlog	None	6009	N/A	FAI
Information	12/13/1999	6:22:50 PM	eventlog	None	6005	N/A	FAI

Figure 4-6
Task shortcuts in this taskpad view simplify life for the end user.

Notice the navigational tabs at the bottom of the taskpad view in Figure 4-6. These make it easy for your user to switch between the taskpad view and a normal view of the same data. You can suppress these tabs (by means of the Customize View dialog box shown in Figure 4-3, page 73) if you don't want to give your console's user this freedom.

To create a taskpad view, start by selecting an item in the console tree to which you want to apply the view. As you'll see in a moment, when you create your taskpad view, you have the option of applying it only to the selected console-tree item.

Next, right-click that console-tree entry and choose New Taskpad View from the shortcut menu. (If you don't see the New Taskpad View command, try again. You need to select the console-tree item and then right-click it—in two separate steps.) A wizard appears. After you acknowledge the wizard's welcome screen, you'll come to the following page of display options.



New Taskpad View Wizard

Taskpad Display

You can choose the way this taskpad displays the details pane of the tree item you selected.

Style for the details pane:

○ Vertical list

● Horizontal list

○ No list

Style for task descriptions

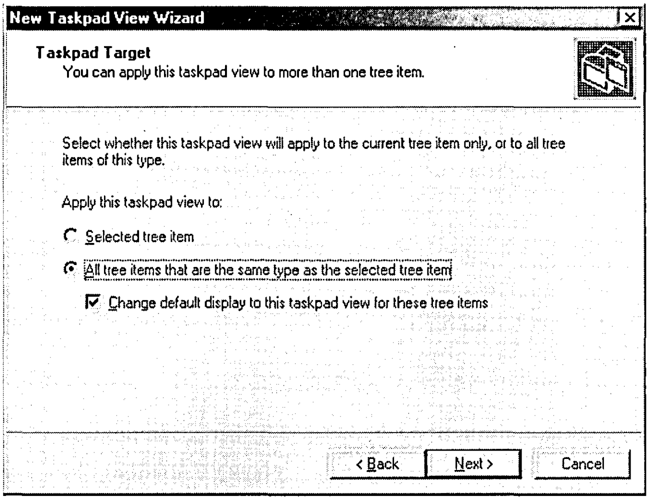
○ Text

● InfoTip (displays description in a pop-up

List size: Large

Best for multiple column lists

The sample table at the right side of this page makes the options pretty self-explanatory. The default choices—a large, horizontal list with InfoTips—work well in most situations. Clicking Next takes you to the following page.



Taskpad Target

You can apply this taskpad view to more than one tree item.

Select whether this taskpad view will apply to the current tree item only, or to all tree items of this type.

Apply this taskpad view to:

○ Selected tree item

● All tree items that are the same type as the selected tree item

☑ Change default display to this taskpad view for these tree items

The default selections apply the new taskpad view to all comparable console-tree items and make the taskpad the default view for those items. Moving on from this screen, you have the opportunity to assign a name and some descriptive text to the new view. You can see in Figure 4-6 that we chose to forego the latter option but assigned the unimaginative name Event Viewer to the view itself.

On the wizard's final page, select the Start New Task Wizard check box if you want to create one or more task shortcuts. This selection summons a new wizard that walks you through the process of creating your first shortcut. On the final page of this wizard, select Run This Wizard Again if you have additional shortcuts to create.

Manipulating Windows

The Action menu's New Window From Here command lets you create a new child window rooted on the current console-tree selection. You might want to use this command to create multiple-window applications—for example, a console consisting of the Indexing Service in one window and a filtered list of Indexing Service events in a second. After you have your windows, you can use Window menu commands to tile or cascade them.

You can also use the New Window From Here command to get rid of that pesky and irrelevant Console Root item that appears atop your default console tree:

1. Select the first item below Console Root.
2. Choose New Window From Here from the Action menu (or right-click and choose it from the shortcut menu).
3. Close the original window (the one with Console Root).

Controlling Other Visual Elements

The Customize View command (see Figure 4-3, page 73) lets you hide or display various elements of the MMC visual scene, including taskbars, menus, and the navigational tabs that appear below taskpad views. You'll find this command on the View menu. Note that selections in the Customize View dialog box take effect immediately. You don't need to hit an Apply button or leave the dialog box, so you can easily try each option and see whether you like it.

Using the Favorites Menu

The Favorites menu, on the menu bar of an MMC console's child window, allows you to store pointers to places within your console tree. If you create a particularly complex MMC console, you might want to consider using Favorites to simplify navigation. To add a console-tree item to your list of favorites, select that item and then choose Add To Favorites from the Favorites menu.

If you create favorites, the user of your console will be able to navigate to a favorite in either of two ways: by choosing its name from the Favorites menu or by clicking the Favorites tab (to the right of the Tree tab; see Figure 4-4, page 75). If you save a console in user mode without having created any favorites, the Favorites menu and Favorites tab disappear.

Naming Your Console

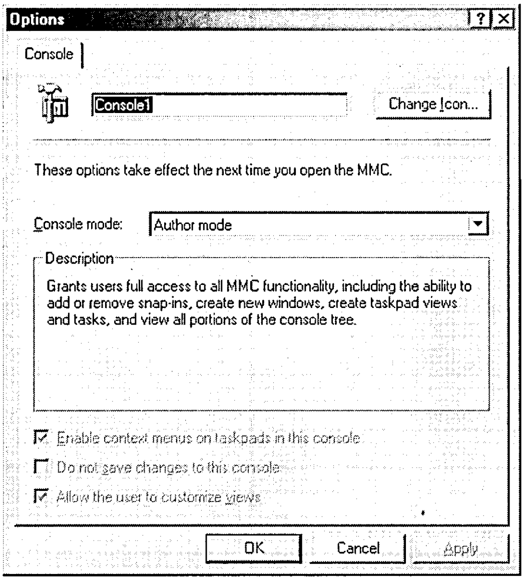
To assign a name to your console, choose Options from the Console menu. (See Figure 4-7.) Your entry in the field at the top of the Options dialog box will appear on the title bar of your console, regardless of the file name you apply to its .msc file. If you do not make an entry here, MMC will replace Console1 with the console's eventual file name.

If you don't like the default MMC icon, you can use the Change Icon button to replace it.

Choosing Among MMC's Three User Modes

In the Console Mode field of the Options dialog box, you can choose among MMC's three user modes:

- User Mode Full Access
- User Mode Limited Access, Multiple Window
- User Mode Limited Access, Single Window



Console1

These options take effect the next time you open the MMC.

Console mode: Author mode

Description

Grants users full access to all MMC functionality, including the ability to add or remove snap-ins, create new windows, create taskpad views and tasks, and view all portions of the console tree.

☑ Enable context menus on taskpads in this console

□ Do not save changes to this console

☑ Allow the user to customize views

Figure 4-7
Use the Options dialog box to name your console and specify a console mode.

In full-access mode, the top-level menu (Console, Window, and Help) is present, but the Console menu has a single command—Exit—and Microsoft On The Web is removed from the Help menu.

In both limited-access modes, the top-level menu disappears, leaving users to work with only the two snap-in menus, Action and View (provided you haven't suppressed those menus via the Customize View command). In the single-window limited-access mode, the current child (snap-in) window is maximized, and MMC essentially loses its MDI character. If you have two or more child windows open at the time you save an MMC console in single-window mode, a confirmation prompt warns you that the user will see only the current child window.

In multiple-window limited-access mode, MMC retains its MDI character (whether or not you've created multiple child windows), allowing child windows to be minimized, maximized, restored, resized, and repositioned.

Imposing Further Restrictions

If you choose one of the three user modes, the three check boxes at the bottom of the Options dialog box become available. Your choices here are as follows:

- **Enable Context Menus On Taskpads In This Console.** If you set up an application to restrict the user to a taskpad view (by using Customize View to remove the taskpad navigation tabs), you might want to clear this check box. Shortcut menus (referred to here as context menus) offered by line items in the taskpad view will become unavailable, and your user will be restricted to using the task icons you've set up.

- **Do Not Save Changes To This Console.** With this check box cleared (its default), MMC saves the state of your application automatically when a user closes it. The user's selection in the console tree, for example, is preserved from one use to the next. If you want your user to always see the same thing each time he or she runs the console, select this check box.
- **Allow The User To Customize Views.** This check box, selected by default, keeps the Customize View command available, allowing your user, for example, to hide or display the console tree. Clear the check box if you want to deny the user this freedom.

Chapter 5

Monitoring System and Application Activities with Event Viewer

In This Chapter

Running Event Viewer 85
Examining Event Details 87
Filtering the Log Display 88
Using Multiple Views of the Same Log 89
Searching for an Event 89
Setting Log-File Size and Longevity 90
Archiving and Clearing Log Files 91
Displaying an Archived Log File 91
Exporting Log-File Information 92
Backing Up Log Files 92
Monitoring Events on Remote Computers 93

In Microsoft Windows 2000, an *event* is any occurrence that is potentially noteworthy—to you, to other users, to the operating system, or to an application. Events are recorded by the Event Log service, and their history is preserved in these three log files: Security (SecEvent.evt), Application (AppEvent.evt), and System (SysEvent.evt). Event Viewer, a Microsoft Management Console snap-in supplied with Windows 2000, allows you to review and archive these three event logs.

Why would you want to do this? The most likely reasons are to troubleshoot problems that have occurred, to keep an eye on your system in order to forestall problems, and to watch out for security breaches. If a device has failed, a disk has filled close to capacity, a program has crashed repeatedly, or some other critical difficulty has arisen, the information recorded in the event logs can help you, or a technical support specialist, figure out what's wrong and what corrective steps are required. Watching the event logs can also help you spot serious problems before they occur. If trouble is brewing but hasn't yet erupted, an eye on the event logs may tip you off before it's too late. For example, if a network adapter is failing intermittently or a network cable is improperly connected, you might begin to see items in the event log showing frequent disconnections from and reconnections to the network. Finally, you can use one of the event logs to track such things as unsuccessful logon attempts or attempts by users to read files for which they lack access privileges. Such occurrences might alert you to actual or potential security problems in your organization.

Security events are recorded in the Security log, SecEvent.evt. Monitoring these events is called *auditing* and is the subject of Chapter 34, "Auditing Security." In the remainder of this chapter, we focus on the other two event logs, AppEvent.evt and SysEvent.evt. AppEvent.evt and SysEvent.evt record application events and system events, respectively.

Application events are generated by applications, including programs that you install, programs that come with Windows 2000, and operating-system services. For example, events relating to Microsoft Office, the Dr. Watson diagnostic utility that comes with Windows 2000, and the Windows 2000 Fax service are all recorded in AppEvent.evt.

System events are generated by Windows 2000 itself and by installed components, such as device drivers. If a driver fails to load when you start a Windows 2000 session, for example, that event is recorded in the System log.

(If you're curious about what elements of your system generate events and where those events are recorded, use one of the registry editors to inspect the following registry keys: HKLM\System\CurrentControlSet\Services\Eventlog\Application, HKLM\System\CurrentControlSet\Services\Eventlog\Security, and HKLM\System\CurrentControlSet\Services\Eventlog\System. Each entity capable of generating an event has a subkey under one of those three keys. *For information about using the registry editors, see Chapter 39, "Working with the Registry."*)

The System and Application logs recognize three types of events:

- *Errors* are events that represent possible loss of data or functionality. Examples of errors include events related to network contention or to a malfunctioning network adapter and loss of functionality caused by a device or service that doesn't load at startup.
- *Warnings* are events that represent less significant or less immediate problems than errors. Examples of warning events include a nearly full disk, a timeout by the network redirector, and data errors on a backup tape.

- *Information* events are other events that Windows 2000 logs. Examples of information events include someone using a printer connected to your computer and a successful dial-up connection to your ISP.

As you'll see momentarily, when you're using Event Viewer to scan your event logs, you can filter the display to show only the event types in which you're most interested.

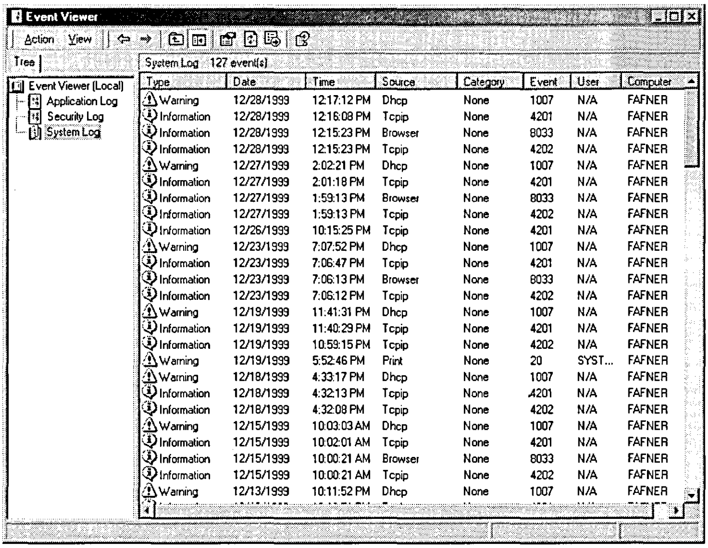
Running Event Viewer

To start Event Viewer, do one of the following:

- Open Administrative Tools in Control Panel and choose Event Viewer.
- From the Start menu, choose Programs | Administrative Tools | Event Viewer.
- In your %SystemRoot%\System32 folder, double-click Eventvwr.msc.
- On any command line, type *eventvwr.msc.*

You can also run Event Viewer by right-clicking My Computer and choosing Manage. The Computer Management console that appears includes the Event Viewer snap-in, along with a number of other administrative tools.

Figure 5-1 shows an example of what you might see when you open Event Viewer. The console tree displays the names of the three event logs, allowing you to move from one log to another. The details pane presents a columnar view of the current log.



Type	Date	Time	Source	Category	Event	User	Computer
Warning	12/28/1999	12:17:12 PM	Dhcp	None	1007	N/A	FAFNER
Information	12/28/1999	12:16:08 PM	Tcpip	None	4201	N/A	FAFNER
Information	12/28/1999	12:15:23 PM	Browser	None	8033	N/A	FAFNER
Information	12/28/1999	12:15:23 PM	Tcpip	None	4202	N/A	FAFNER
Warning	12/27/1999	2:02:21 PM	Dhcp	None	1007	N/A	FAFNER
Information	12/27/1999	2:01:18 PM	Tcpip	None	4201	N/A	FAFNER
Information	12/27/1999	1:59:13 PM	Browser	None	8033	N/A	FAFNER
Information	12/27/1999	1:59:13 PM	Tcpip	None	4202	N/A	FAFNER
Information	12/26/1999	10:15:25 PM	Tcpip	None	4201	N/A	FAFNER
Warning	12/23/1999	7:07:52 PM	Dhcp	None	1007	N/A	FAFNER
Information	12/23/1999	7:06:47 PM	Tcpip	None	4201	N/A	FAFNER
Information	12/23/1999	7:06:13 PM	Browser	None	8033	N/A	FAFNER
Information	12/23/1999	7:06:12 PM	Tcpip	None	4202	N/A	FAFNER
Warning	12/19/1999	11:41:31 PM	Dhcp	None	1007	N/A	FAFNER
Information	12/19/1999	11:40:29 PM	Tcpip	None	4201	N/A	FAFNER
Information	12/19/1999	10:59:15 PM	Tcpip	None	4202	N/A	FAFNER
Warning	12/19/1999	5:52:46 PM	Print	None	20	SYST...	FAFNER
Warning	12/18/1999	4:33:17 PM	Dhcp	None	1007	N/A	FAFNER
Information	12/18/1999	4:32:13 PM	Tcpip	None	4201	N/A	FAFNER
Information	12/18/1999	4:32:08 PM	Tcpip	None	4202	N/A	FAFNER
Warning	12/15/1999	10:03:03 AM	Dhcp	None	1007	N/A	FAFNER
Information	12/15/1999	10:02:01 AM	Tcpip	None	4201	N/A	FAFNER
Information	12/15/1999	10:00:21 AM	Browser	None	8033	N/A	FAFNER
Information	12/15/1999	10:00:21 AM	Tcpip	None	4202	N/A	FAFNER
Warning	12/13/1999	10:11:52 PM	Dhcp	None	1007	N/A	FAFNER

Figure 5-1
Event Viewer's details pane presents a columnar view of the log selected in the console tree.

Figure 5-1 shows all eight of Event Viewer's columns. You can use the View menu's Choose Columns command to hide columns you don't need or to change the order in which columns appear. By default, events are sorted chronologically, with the most recent at the top. You can change the sort order by clicking column headings.

Note that, while the details pane includes some useful information, it doesn't provide many details about what events portend or why they occurred. You can get more of that information by inspecting the details for individual events. *(See the following section, "Examining Event Details.")* Here is a column-by-column rundown of what the details pane does display:

- **Type.** As mentioned, events in the System and Application logs are of three types: Information, Warning, and Error. The icon at the left side of the Type column helps you spot the event types in which you're interested. (The Error type, not shown in Figure 5-1, is marked by an unmistakable red X.)
- **Date** and **Time.** The Event Log service records the date and time of each event's occurrence in Greenwich mean time, and Event Viewer translates those Greenwich mean time values into dates and times appropriate for your own time zone.

Daylight Saving Time, Remote Computers, and Changes to the System Clock

When you move from standard time into daylight saving time or vice versa, Event Viewer changes the displayed Time (and possibly Date) values for events that have already occurred. For example, if an event occurred at 6 P.M. in standard time, after you move into daylight saving time that event will appear as if it had occurred at 7 P.M. That's because Event Viewer applies a single offset from Greenwich mean time to all events in its logs and decrements that offset by one hour when you pass from standard into daylight saving time.

If you monitor events on remote computers in other time zones, be aware that Event Viewer always displays those events' dates and times in your (local) time zone. It records occurrences in Greenwich mean time but applies your time zone's Greenwich mean time offset for display purposes. Thus, for example, an event occurring at noon in New York will be reported in Los Angeles as having occurred at 9 A.M.

If you change the clock on your system, the times reported in event logs do not change, because your offset from Greenwich mean time has not changed. If you change your time zone, however, Event Viewer applies the new offset and changes the times displayed for all events in the log.

- **Source.** The source column reports the application or system component that generated each event.
- **Category.** Some event sources use categories to distinguish different types of events they may report. Many sources do not. As you can see, none of the

four sources exemplified in Figure 5-1 (Dhcp, Tcpip, Browser, and Print) use categories.

- **Event.** All events are identified by a numerical value. This number is associated with a text description that appears when you view an event's properties. There's no system-wide code in use here—each event source's designer simply decides what numbers to use and records those numbers in the registry—and there's no requirement that each event source use a unique set of numbers. After spending some time in your event logs, however, you might begin to recognize particular events by their arbitrary numbers. For example, events 6006 and 6009, generated by the Event Log service itself (eventlog, in the Source column) occur respectively when the Event Log service is stopped and started. Because the Event Log service is ordinarily never stopped while your computer is running, these events represent system shutdown and restart.
- **User.** The User column records the user account associated with each event. Not all events are associated with a particular user account. Many events, particularly system events, are not generated by a particular user. These events show up as N/A.
- **Computer.** The Computer column records the computer on which the event occurred.

Examining Event Details

To learn more about an event than Event Viewer's details pane tells you, you need to display individual information for the event. Select the event you're interested in and do one of the following:

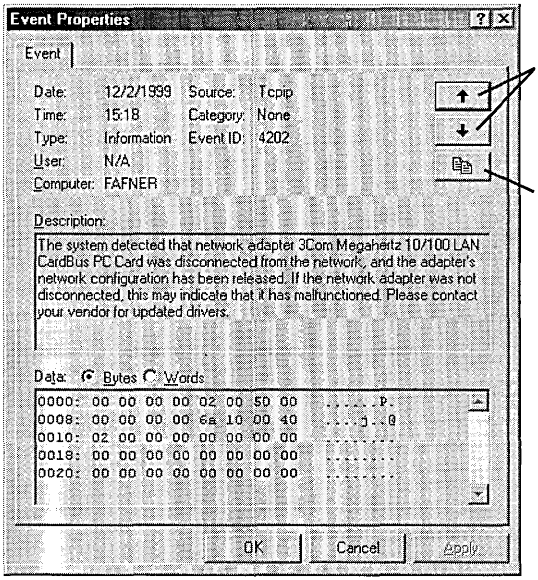
- Double-click the event.
- Press Enter.
- Choose Properties from Event Viewer's Action menu.

Figure 5-2 shows the properties dialog box for an event in the System log.

The summary information in the top third of the properties dialog box is identical to the information that appears in Event Viewer's columnar details pane. The description in the middle third of the window is the plain-language description of what has occurred. For localization purposes, this information is kept separate from the log (.evt) file. Each event type listed in the registry is mapped to descriptive text that lives elsewhere, in whatever file the application's or component's designer chooses to use. (The event message file is recorded in the EventMessageFile registry value in HKLM\System\CurrentControlSet\Services\Eventlog\*logname**eventsource*, where *logname* is the name of the log—System, for example—and *eventsource* is the name of the application or component that generates the event in question.)

Some events generate binary data that can be useful to programmers or support technicians who are familiar with the product that generated the event. If binary data is available, it appears in the bottom third of the properties dialog box.

If you want to view details for other events, you can do so without first returning to the details pane: click the arrow buttons in the upper right corner of the properties dialog box to move to the previous or next event.



Date: 12/2/1999 Source: Tcpip
Time: 15:18 Category: None
Type: Information Event ID: 4202
User: N/A
Computer: FAFNER

Description:

The system detected that network adapter 3Com Megahertz 10/100 LAN CardBus PC Card was disconnected from the network, and the adapter's network configuration has been released. If the network adapter was not disconnected, this may indicate that it has malfunctioned. Please contact your vendor for updated drivers.

Data: ● Bytes ○ Words

```
0000: 00 00 00 00 02 00 50 00   ......P.
0008: 00 00 00 00 6a 10 00 40   ....j..@
0010: 02 00 00 00 00 00 00 00   ........
0018: 00 00 00 00 00 00 00 00   ........
0020: 00 00 00 00 00 00 00 00   ........
```

Move to previous or next event

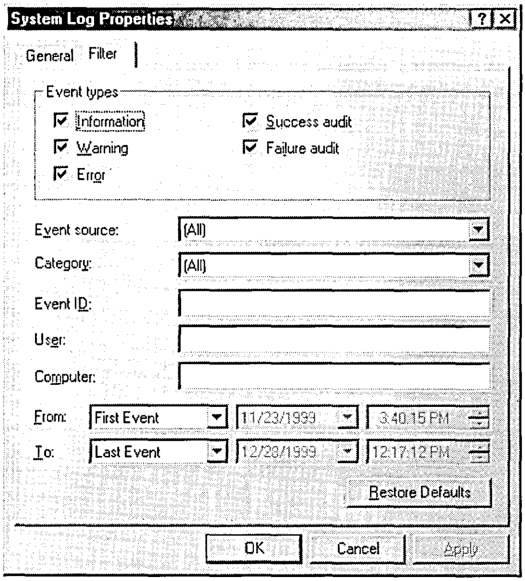
Copy current event to the clipboard

Figure 5-2
The properties dialog box for an event can provide useful diagnostic information.

Directly below the Next Event button, near the upper right corner of the window, is a handy Copy button. A click here sends the entire contents of the properties dialog box to the clipboard, allowing you, for example, to paste the information into an e-mail message and send it to a support technician. (You can also copy some or all of the description text by selecting it in the middle third of the window and pressing Ctrl+C.)

Filtering the Log Display

As you can see from a cursory look at your System log, events can pile up quickly, obscuring those of a particular type (such as print jobs) or those that occurred at a particular date and time. To filter a log so that Event Viewer displays only the items you currently care about, select the log's name in the console tree and choose Filter from the View menu. Then fill out the Filter tab of the log's properties dialog box (see Figure 5-3) and click OK. To restore the unfiltered list, return to this dialog box and click Restore Defaults.


System Log Properties

General | Filter

Event types

☑ Information ☑ Success audit
☑ Warning ☑ Failure audit
☑ Error

Event source: (All)

Category: (All)

Event ID:

User:

Computer:

From: First Event 11/23/1999 3:40:15 PM

To: Last Event 12/28/1999 12:17:12 PM

Figure 5-3
You can use this dialog box to filter a log's display on any of Event Viewer's eight columns.

Using Multiple Views of the Same Log

With the help of the Action menu's New Log View command, you can switch quickly between filtered and unfiltered views of a log—or between one filtered view and a different filtered view. Simply select the log in which you're interested, right-click, and choose New Log View. Event Viewer adds the new view to the console tree. Select the new view and filter to taste. Now you can move between views by navigating the console tree.

Searching for an Event

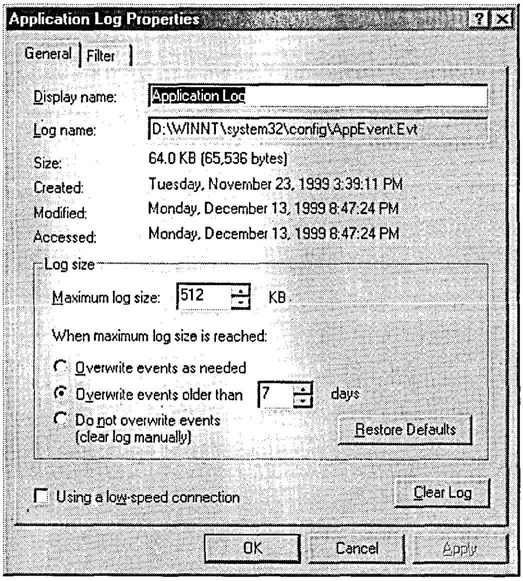
The Find command on Event Viewer's View menu allows you to locate particular items in the current log. The Find dialog box looks a lot like the one shown in Figure 5-3 but includes a Description box in which you can specify all or a portion of an event's descriptive text. To locate the most recent event that involved any kind of failure, therefore, you could select the first event in the log (assuming you've kept the default chronological sort order), choose Find, type *fail* on the description line, and click Find Next.

Setting Log-File Size and Longevity

Log files don't continue to pile up new events forever. If they did, they'd eventually consume an unmanageable amount of disk space. By default, each log file has a maximum size of 512 KB. You can adjust that downward or upward in 64-KB increments.

Also by default, events in each log file have a minimum longevity of seven days. That means that if a file reaches its maximum size, new events overwrite the oldest ones—but only if the oldest ones are at least seven days old. That too is an adjustable parameter.

To change either a log file's maximum size or its events' minimum longevity, select the log in question in the console tree. Then choose Properties from the Action menu. Figure 5-4 shows a log file's properties dialog box. (You must have administrative privileges to use this dialog box; otherwise, the controls all appear dimmed.)



Application Log Properties

General | Filter

Display name: Application Log

Log name: D:\WINNT\system32\config\AppEvent.Evt

Size: 64.0 KB (65,536 bytes)

Created: Tuesday, November 23, 1999 3:39:11 PM

Modified: Monday, December 13, 1999 8:47:24 PM

Accessed: Monday, December 13, 1999 8:47:24 PM

Log size

Maximum log size: 512 KB

When maximum log size is reached:

○ Overwrite events as needed

● Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

□ Using a low-speed connection

Figure 5-4
The properties dialog box lets you control the size and lifespan of your event logs.

If the Event Log service is unable to add new events to a log, either because you have told it never to overwrite or because it has reached capacity before the oldest events have reached their minimum age, you'll receive a warning message. Then you can remedy the situation, either by simply clearing the log or by archiving and then clearing it.

Troubleshooting

If you run out of space on the disk where your log files reside, the Event Log service will be unable to record new events and you will receive an error message to that effect. If you cannot create free space on the full disk, you can work around the problem by changing the default location of the log files. Doing so requires three modifications to your registry. Proceed as follows:

1. Run Regedit or Regedt32.
2. Navigate to the key HKLM\System\CurrentControlSet\Services\Eventlog \Application.
3. Double-click the File value.
4. Change the File value's data to specify a path to a disk that isn't full. For example, if the current data is %SystemRoot%\System32\Config\AppEvent.evt and you have room to put the AppEvent.evt file in E:\SomeFolder, change the File value's data to E:\SomeFolder\AppEvent.evt.
5. Repeat these steps for the File value in HKLM\System\CurrentControlSet \Services\Eventlog\Security and HKLM\System\CurrentControlSet\Services \Eventlog\System.
6. Close Regedit or Regedt32.

For additional information about modifying the registry, see Chapter 39, "Working with the Registry."

Archiving and Clearing Log Files

To archive a log, select it in the console tree and choose Save Log File As from the Action menu. In the dialog box that appears, be sure to choose the default file type, Event Log (*.evt). The resulting file includes all events (ignoring the current filter, if any) and all the recorded information (including the binary details).

To clear a log, either click the Clear Log button in the log's properties dialog box (see Figure 5-4) or select the log in the console tree and choose Clear All Events from the Action menu. You must have administrative privileges to clear a log.

Displaying an Archived Log File

After you have saved a log file in the .evt format, you can redisplay its contents at any time by using the Open Log File command on the Action menu. You need to tell the system what kind of log file—Application, Security, or System—you're reopening when you specify the file's name.

A reopened archive appears as a new entry in the console tree. You can view it, filter it, and search it, just as you would any other log file. You can also delete it—something you can't do to the default Application, Security, and System logs.

Exporting Log-File Information

Saving a log in its native (.evt) format creates a complete replica of the log, but you can view that replica only in Event Viewer (or a third-party application capable of reading native event logs). Event Viewer can also export log data to tab-delimited and comma-delimited text files, however, and you can easily import these into database, spreadsheet, or even word processing programs. When you save a log in one of these formats, you get everything in the log except the binary data associated with certain events.

To save an entire log file in a text format, select the log in the console tree, choose Save Log File As from the Action menu, and select either Text (Tab Delimited) or CSV (Comma Delimited) from the Save As Type list.

The Save Log File As command always exports all of the current log, regardless of how the log might be filtered for display purposes. If you want to generate a text report showing only particular kinds of events, first filter the log to display those events and then use the Action menu's Export List command. Like Save Log File As, Export List provides tab-delimited and comma-delimited options. It also offers the option to save in Unicode—something that could prove handy if your local language includes non-Latin characters. Do not, however, select the Save Only Selected Rows check box in the Export List dialog box unless you want a report that includes only column headers and a single event.

Backing Up Log Files

Because the Event Log service is ordinarily running at all times, the three log files—AppEvent.evt, SecEvent.evt, and SysEvent.evt—are, under ordinary circumstances, open at all times. *Do not try to back up these log files using Windows Explorer or the command line!* Windows Explorer and the Copy command will copy your open log files without complaint, but if you copy them back to your %SystemRoot%\System32\Config folder (the default log-file location), Event Viewer will find them corrupted and will be unable to display their contents.

If for some reason you must back up your logs with Windows Explorer or the Copy command (a circumstance difficult to imagine), first disable the Event Log service and then restart Windows 2000. Those actions will close the log files and prevent them from being opened when Windows 2000 starts. After you've made your copies, reenable the service and restart Windows 2000. *(For information about disabling/reenabling services, see "Starting and Stopping Services," page 332.*

Fortunately, the Windows 2000 Backup program (Ntbackup.exe) can back up and restore log files without corrupting them in the process and without your having to disable the log service. You can use Windows 2000 Backup to schedule regular backups of your log files.

Troubleshooting

If Event Viewer reports on startup that one or more of your log files is corrupt, you can remedy the situation as follows:

1. Disable the Event Log service. *(For information about disabling a service, see "Starting and Stopping Services," page 332)*
2. Restart Windows 2000.
3. Delete the corrupt log(s)—AppEvent.evt, SecEvent.evt, and/or SysEvent.evt—from %SystemRoot%\System32\Config (or wherever they may be).
4. Reenable the Event Log service.
5. Restart Windows 2000.

Note that you cannot delete or rename the log files while the Event Log service is running.

Monitoring Events on Remote Computers

You can use Event Viewer to monitor events on computers other than your own. To monitor a remote computer, start Event Viewer with the following command line:

```
eventvwr.msc /computer=computername
```

where *computername* is the network name of the remote computer.

You can also use Event Viewer's Open Log File command to read log (.evt) files that have been saved from a remote system. Be aware, however, that when you open a log file saved from a remote system, your local copy of Event Viewer will read that log file using your local registry settings, not those of the remote computer. If you try to examine the details for an event whose source is registered on the remote computer but not on your own, you'll see an error message indicating that the description for this particular event can't be found. You can work around this problem by adding the remote event source to your own registry.

For example, suppose the remote system generates events from an application called MyApp, which is not registered on your local system. To modify your system so that you can read these events in a log saved from the remote system:

1. On the remote computer, run Regedit (not Regedt32).
2. Navigate to the key HKLM\System\CurrentControlSet\Services\Eventlog \Application\MyApp.

   (If the remote events in question appear in the System log, not the Application log, substitute System for Application in this key.)
3. In Regedit's right pane, look for the value EventMessageFile. The data for this value specifies the remote system's event message file, and you will need to copy this file to an identical path on your own system. For example, if the data reads %SystemRoot%\System32\Myapp.ocx, you need to copy the file to %SystemRoot%\System32 on your own system.
4. With the MyApp key selected in the left pane, choose Export Registry File from Regedit's Registry menu. Supply a file name with the extension .reg.
5. Close Regedit.
6. On your own system, double-click the .reg file you just saved from the remote system to merge it into your registry.
7. Copy the remote system's event message file to your own system.
8. Close and restart Event Viewer. You should now be able to read the log file saved from the remote system and have the information translated correctly.

Chapter 6

Finding Files with the Indexing Service

In This Chapter

Security and the Indexing Service 96
Limitations of the Indexing Service 97
Activating the Indexing Service 98
Submitting Queries 99
Administering the Indexing Service 110

Created for and first delivered with Microsoft Internet Information Server (IIS), the Indexing Service is a feature originally designed to facilitate fast and flexible searches for information stored on Web sites. Because its query technology can be applied to ordinary disk stores as well as to Web sites, the Indexing Service has become a core component of Microsoft Windows 2000 and is integrated with the Search Assistant, the searching tool that appears when you choose Search from the Start menu or display the Search Explorer bar in Windows Explorer. With the Indexing Service thus married to the operating system, you can now use the same powerful query language to locate files on your local and remote hard disks as Webmasters use to set up search forms on Internet or intranet sites.

The Indexing Service extends the power of the Search Assistant in several ways. First, it speeds up searching dramatically. How much performance gain you'll see depends on many circumstances. But in tests for this chapter, we found that content searches consistently ran on the order of a hundred times faster with the Indexing Service than without it.

Second, the Indexing Service's query language lets you find files on the basis of many different properties in addition to the size, date, and file-type properties that the native Search Assistant understands. With the Indexing Service, you can locate a file on the basis of word count, most recent editor, most recent printing time, and many other attributes. (*For a list of the most useful properties available to Indexing Service queries, see Table 6-1, page 104].*)

In addition, the query language offers Boolean and proximity operators as well as the ability to find inflected forms of search strings. The Boolean operators allow you to specify more than one criterion in a search (all files written by Bill containing the words "Windows 2000," for example). The proximity operator lets you search for files in which one word or string appears close to another (although it did not work reliably in our tests). And the ability to find inflected word forms means that, for example, a search for "swim" will turn up "swimming," "swam," and "swum" as well as "swim."

Because the Indexing Service is integrated with the Search Assistant, you can enter your queries, simple or complex, directly on the Search Assistant's Containing Text line. You don't need a special query form. (As you'll see, a query form is included in Ciadv.msc, the MMC console used for managing the Indexing Service. But you don't need to use this form—and, in fact, you can't unless you're logged on as an administrator.) You do need to ensure that the service is running and that it has had time to build a catalog of your disks' contents. Provided that the disks and folders you're searching have been indexed and the service is running, the Search Assistant lets the Indexing Service do the searching.

Security and the Indexing Service

The Indexing Service obeys the rules of NTFS file security. If a *catalog* (the collection of files used by the Indexing Service to record the contents and properties of your files) resides on a local NTFS volume, the access privileges of the user executing a search determine the results of that search. The service will not return the names of files for which the user does not have at least Read access permission. If the catalog is stored on a network share accessed via a UNC path, the user might see the names of files for which he or she lacks Read permission but will not be able to open any such files.

By default, the Indexing Service creates its catalogs in folders to which only the System account has access. This precaution prevents accidental deletion. More important, it helps maintain security. As long as the default access permissions for the catalog folder are not changed by an administrator, you can be assured that the catalog files themselves are not subject to unauthorized inspection.

The Indexing Service never indexes encrypted documents. If a file is encrypted after being indexed, the service removes it from the catalog. Because such files won't appear in searches performed by the Indexing Service, even if those searches are carried out by the owner of the files, it's best to exclude folders containing encrypted files from the catalog. *(See "Changing the Folders Included in a Catalog," page 113.)* Folders excluded from the catalog can be searched in the normal way by the Search Assistant.

Limitations of the Indexing Service

Does using the Indexing Service have drawbacks? Not many. But here are some things you should know:

- **The Indexing Service requires disk space.** Because the Indexing Service catalogs your disks in the background, during periods when your computer is idle, you don't pay a performance penalty for having the service running. You do, however, sacrifice some disk space. Microsoft estimates that the catalog will consume from 15 to 30 percent of the size of the indexed files. Prudence suggests assuming that the higher figure is more accurate.
- **The Indexing Service catalogs the content of only certain kinds of files.** By default, the Indexing Service catalogs the content of the following document types:
  - HTML files (their textual contents)
  - Text files, including files with the extensions .ini, .reg, .inf., .bat, and .txt
  - Documents created by Microsoft Office (version 95 and later)
  - Internet mail and news files (if IIS is installed)
  - Any other document type for which a suitable filter is installed

  A *filter* tells the Indexing Service how to separate meaningful text from file headers, formatting information, and all other nontextual elements. Microsoft provides filters for HTML, text, Office, and mail and news documents. Third parties might provide filters for their own documents. (For example, Adobe Systems provides a filter for its popular .pdf format. You can download that filter from *www.adobe.com*.) If you use a non-Microsoft office suite, you might want to check with that product's vendor to see whether an Indexing Service filter (an *ifilter*, to use the programmer's jargon) is available.

  With an optional setting available via the Indexing Service MMC console, you can set the service to index files with unknown extensions. *(To learn how to do this, see "Indexing Files with Unknown Extensions," page 112.)* If you index files with unknown extensions, the service tries to extract meaningful content from file types other than the ones it catalogs by default. For more reliable content searching of unfiltered file types, however, we recommend the command-line utility Findstr. You can open a Command Prompt session and type *findstr /?* to obtain information about this command. *(See Chapter 11, "Using the Command Prompt.")*
- **The Indexing Service ignores "noise" words.** The list of words ignored by the Indexing Service appears in the file %SystemRoot%\System32\Noise.*xxx*, where *xxx* is a three-letter abbreviation for the language you use. The file is plain text, and you can edit it with Notepad or another plain-text editor. The noise

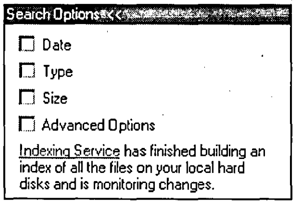
file for the English language, Noise.eng, includes common prepositions and conjunctions, articles, relative pronouns, various forms of the verb *to be* and other common verbs, individual numerals (1, 2, 3, and so on), individual letters (*a, b, c*), and a handful of other words that occur so frequently in text that they're generally not useful in search strings.

If you include a noise word in a search string, the service treats that word as a placeholder. For example, in the search string "age before beauty," "before" is a noise word. The Indexing Service will treat this string as equivalent to "age after beauty," "age with beauty," and so on.

- **The Indexing Service ignores case.** In the native Search Assistant, searches are case insensitive by default, but you can override that default. Indexing Service searches, on the other hand, are always case insensitive. If you need a case-sensitive search, simply click Advanced Options in the Search Options section of the Search Explorer bar, and select the Case Sensitive check box. The Search Assistant will then ignore the Indexing Service catalog.

Activating the Indexing Service

Before you can use the Indexing Service, the service must be running. It must also have some time to generate a catalog. To learn the current status of the service, open the Search Assistant (Start | Search | For Files And Folders) and check the text that appears at the bottom of the Search Options section. (If the Search Options section is collapsed, click Search Options to expand it.)



Search Options <<

□ Date

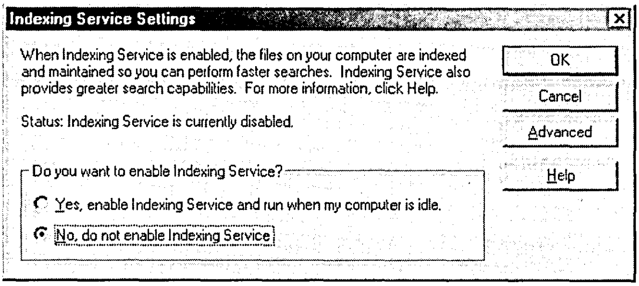
□ Type

□ Size

□ Advanced Options

Indexing Service has finished building an index of all the files on your local hard disks and is monitoring changes.

If the Indexing Service is not currently running, the text will indicate that the service is disabled. To enable it, you must be logged on as a member of the Administrators group. If you click Indexing Service without being logged on as an administrator, you'll be taken to the Help documents for the Indexing Service, where you can read all the many reasons you should find an administrator to start the service! If you are logged on as an administrator, the Indexing Service Settings dialog box, shown in Figure 6-1, appears. Here you can turn on the service by selecting Yes, Enable Indexing Service And Run When My Computer Is Idle.



When Indexing Service is enabled, the files on your computer are indexed and maintained so you can perform faster searches. Indexing Service also provides greater search capabilities. For more information, click Help.

Status: Indexing Service is currently disabled.

Do you want to enable Indexing Service?

○ Yes, enable Indexing Service and run when my computer is idle.

● No, do not enable Indexing Service

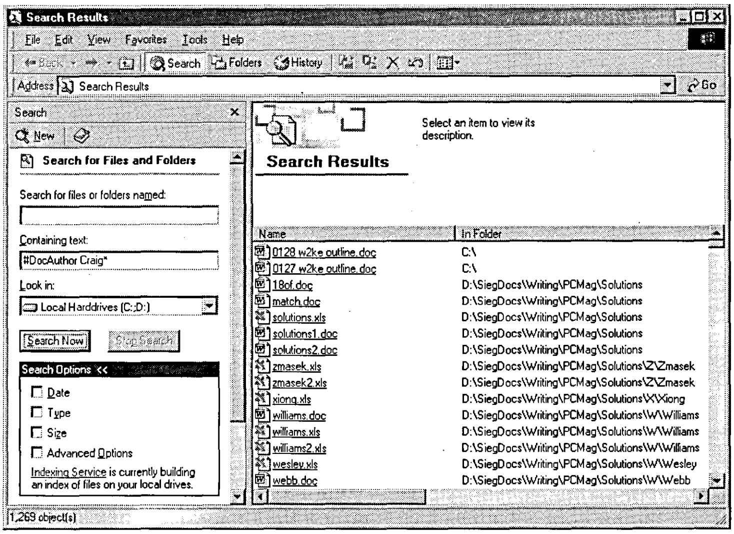
Figure 6-1
Click Yes to turn on the Indexing Service. You must be logged on as an administrator to reach this dialog box.

The Advanced button in the Indexing Service Settings dialog box provides one route to the Indexing Service MMC console, where (if you have administrative privileges) you can tailor the service to your needs. The options available there are described later in this chapter. *(See "Administering the Indexing Service," page 110.)* By default, the service creates a catalog called System that incorporates all of your local hard disk storage except for %HomeDrive%\Documents And Settings\Default User\ Application Data and %HomeDrive%\Documents And Settings\Default User\Local Settings (and the subfolders of these two folders).The first time you activate the Indexing Service, it has quite a bit of work to do to create this catalog. You will probably need to leave your machine on and idle overnight before the catalog is complete. After the initial work is finished, however, the Indexing Service is a low-maintenance feature. Changes that you make to your files are quickly incorporated into the catalog. *For more details about how the Indexing Service maintains its catalog(s), see "Administering the Indexing Service," page 110.*

Submitting Queries

To submit a query, simply open a Search Assistant window (choose Start | Search | For Files And Folders, or click Search in Windows Explorer) and type on the Containing Text line. Your query can be up to 256 characters in length. As Figure 6-2 shows, the results appear in the Search Results window, which is an ordinary Windows Explorer window. You can manipulate files there exactly as you would in any other Windows Explorer context.

Note that you can still use all the other fields in the Search Assistant to restrict your query. For example, typing *#docauthor Craig** on the Containing Text line generates a search for all documents whose author's name begins with Craig. To restrict the search to Microsoft Excel documents, you could type **.xls* on the Search For Files Or Folders Named line. To limit the search to documents last modified within the most recent month, you could click Date, choose Files Modified, and so on. You could add these restrictions to your query by using Boolean operators on the Containing Text line, but why bother? If the Search Assistant provides the parameters you need, you might as well take advantage of them—and save your Boolean prowess for more complex queries that require it.


Search Results
File Edit View Favorites Tools Help
Back Search Folders History
Address Search Results
Go
Search
New
Search for Files and Folders
Search Now
Stop Search
Search Options <<
Select an item to view its description.
Search Results

Search for files or folders named:

Containing text: #DocAuthor Craig*

Look in: Local Harddrives (C:;D:)

□ Date
□ Type
□ Size
□ Advanced Options

Indexing Service is currently building an index of files on your local drives.

Name	In Folder
0128 w2ke outline.doc	C:\
0127 w2ke outline.doc	C:\
18of.doc	D:\SiegDocs\Writing\PCMag\Solutions
match.doc	D:\SiegDocs\Writing\PCMag\Solutions
solutions.xls	D:\SiegDocs\Writing\PCMag\Solutions
solutions1.doc	D:\SiegDocs\Writing\PCMag\Solutions
solutions2.doc	D:\SiegDocs\Writing\PCMag\Solutions
zmasek.xls	D:\SiegDocs\Writing\PCMag\Solutions\Z\Zmasek
zmasek2.xls	D:\SiegDocs\Writing\PCMag\Solutions\Z\Zmasek
xiong.xls	D:\SiegDocs\Writing\PCMag\Solutions\X\Xiong
williams.doc	D:\SiegDocs\Writing\PCMag\Solutions\W\Williams
williams.xls	D:\SiegDocs\Writing\PCMag\Solutions\W\Williams
williams2.xls	D:\SiegDocs\Writing\PCMag\Solutions\W\Williams
wesley.xls	D:\SiegDocs\Writing\PCMag\Solutions\W\Wesley
webb.doc	D:\SiegDocs\Writing\PCMag\Solutions\W\Webb

1,269 object(s)

Figure 6-2
To submit a query, simply type on the Containing Text line.

The Short Form and the Long Form

You can express queries in either of two "dialects," known as the short form and the long form. Figure 6-2 shows an example of a short-form query.

The short form is compatible with earlier versions of the query language; the long form is the basis for all future versions. In other words, if training and preparation for the future are important to you, you should learn and use the long form. For the sake of maintainability, it would also be wise to focus on the long form if you're developing applications that use the Indexing Service APIs. On the other hand, the long form requires a lot more typing.

If extra typing is not an insurmountable burden for you, however, you might come to prefer the long form, simply because it is more internally consistent and easier to learn. The short form relies on mode symbols that don't always work in an intuitive way.

In the current version of the Indexing Service, you can do everything with the short form that you can do with the long.

The Syntax of the Short Form

Short-form queries look like this:

```
@|$|#property-name query-expression
```

That is, they begin with a property name, prefixed by one of the following mode symbols:

Mode Symbol	Query Type
@	Phrase query
$	Free-text query
#	UNIX-style regular-expression query

If you're searching for file content (as opposed to, say, looking for files by a particular author or files created within a particular date range), the property in question is Contents. Thus a short-form content query might look like this:

```
@contents query-expression
```

or

```
$contents query-expression
```

In short-form queries that involve multiple properties, each property name must be preceded by one of the three mode symbols. *For an explanation of the difference between free-text and phrase queries, see "Phrase and Free-Text Query Expressions," below.*

The Syntax of the Long Form

The long-form syntax resembles that of Hypertext Markup Language (HTML):

```
{query-tag attribute1=value1, attribute2=value2, ...} query-expression {closing-tag}
```

For example, a long-form query for documents whose subject is "taxes" might look like this:

```
{prop name=docsubject} taxes {/prop}
```

A space character following the query tag's closing brace is optional, as are space characters surrounding an operator name (such as AND). Examples in this chapter include space characters for readability and typographical convenience.

Closing tags are sometimes optional. Because they are required in many queries, however, you might want to acquire the habit of using them. (The Indexing Service displays an error message if you omit a required closing tag.)

Phrase and Free-Text Query Expressions

Query expressions involving text can take either of two forms, called *phrase* and *free-text*. In a phrase expression, the service looks for exact matches. For example, given the query

```
{phrase} John's debugger eats bugs {/phrase}
```

the service returns only those files that include exactly that four-word string.

In a free-text expression, the service treats the text as though each word were separated from the next by a Boolean OR—that is, it returns files that match any of the words. It also looks for inflected forms of verbs. So the query

```
{freetext} John's debugger eats bugs {/freetext}
```

would cause the service to look for files that contain any of following words: "John's," "debugger," "eats," "bugs," "ate," "eating," "eaten."

When you perform a free-text query, the Relevance column in the Search Results window becomes relevant. The numbers there reflect the Indexing Service's estimate of the relative utility of the files returned. Files in which all the words in the search string are found in immediate proximity to one another and in the order submitted receive the highest rankings. Note, however, that Indexing Service does not perform any natural-language processing when it carries out a free-text search. It simply looks for word matches.

Query expressions in the current version of Indexing Service are free-text by default. This is a change from earlier versions.

Submitting Content Queries

When you look for files containing particular words or sequences of words, you're asking the Indexing Service to look at your documents' Contents property. Because Contents is the service's default property and free-text is its default text mode, you can perform a free-text content search simply by typing on the Search Assistant's Containing Text line—that is, without using either the short form or the long form of the query language. You can also submit a phrase query directly on the Containing Text line by enclosing your phrase in quotation marks.

It's not a particularly good idea to submit your content queries in this manner, however. If your catalog is not completely up to date, the Search Assistant might begin a laboriously slow file-by-file, bit-by-bit search of your hard disk, rather than consulting the catalog. Worse, if it launches into a phrase search in this manner, it will look for the quotation marks right along with the words they contain.

To avoid misunderstandings, it's better to do a little extra typing. For a free-text query, type

```
$contents text
```

or

```
{freetext} text {/freetext}
```

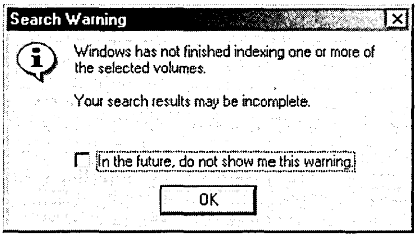
For a phrase query, type

```
@contents text
```

or

```
{phrase} text {/phrase}
```

If the catalog is not current when you do this, the following message appears:



Search Warning

Windows has not finished indexing one or more of the selected volumes.

Your search results may be incomplete.

To bail out, click the X in the upper right corner of the dialog box to close it. (Someone neglected to put a Cancel button in this dialog box.) Unless you've had the Indexing Service turned off for a long time, though, the chances are good that your catalog is nearly complete and that going ahead with the search will produce the file names you're looking for.

Note the following about query expressions that include text:

- Free-text and phrase expressions cannot be mixed in a single query. That is, you cannot use a Boolean or proximity operator to connect a free-text expression to a phrase expression.
- Enclose your text in quotation marks if it contains any of the following characters: % | ^ # @ $
- Enclose your text in quotation marks if you're using the long form and if *query-expression* contains any of the following words: "and," "or," "not," "near," "equals," "contains."
- The Indexing Service always ignores case.
- You can't use relational operators in content queries. Therefore, do not put an equal sign in short-form queries for text. Results for queries of the form @contents=*text* are erratic. Sometimes the service displays an error message; sometimes it returns nothing.

Working with Properties

Technically, all queries are property queries. When you look for files that contain particular words, you're searching on the basis of the Contents property. Contents is the Indexing Service's default property. Table 6-1 lists the most important additional properties that you can use in your queries. Note that not all of these properties are available for every document type.

Table 6-1. Useful Document Properties Available for Indexing Service Queries

Property Name	Description
Access	The last time the document was accessed
All	All properties, including Contents; works only for text queries, not numeric queries
AllocSize	The amount of disk space allocated to the document
Created	The time the document was created
Directory	The physical path to the document, not including the document name
DocAppName	The name of the application that created the document
DocAuthor	The author of the document
DocByteCount	The number of bytes in the document
DocCategory	The document type
DocCharCount	The number of characters in the document
DocComments	Comments about the document
DocCompany	The name of the company for which the document was written
DocCreatedTm	The time the document was created
DocEditTime	The total time spent editing the document
DocHiddenCount	The number of hidden slides in a Microsoft PowerPoint document
DocKeywords	Key words associated with the document
DocLastAuthor	The user who most recently edited the document
DocLastPrinted	The time the document was last printed
DocLastSavedTm	The time the document was last saved
DocManager	The name of the manager of the document's author
DocNoteCount	The number of pages with notes in a PowerPoint document
DocPageCount	The number of pages in the document
DocParaCount	The number of paragraphs in the document
DocPartTitles	The names of document parts, such as worksheet names in a Microsoft Excel document or slide titles in a PowerPoint document
DocRevNumber	The current version number of the document
DocSlideCount	The number of slides in a PowerPoint document DocSubject The subject of the document
DocTemplate	The name of the template used by the document
DocTitle	The title of the document

(continued)

Table 6-1. Useful Document Properties Available for Indexing Service Queries *(cont.)*

Property Name	Description
DocWordCount	The number of words in the document
Filename	The name of the document
Path	The physical path to the document, including the document name
ShortFileName	The 8.3-format name of the document
Size	The size of the document, in bytes
Write	The date and time the document was last modified

In addition to the properties listed in Table 6-1, the Indexing Service can catalog custom properties associated with a document.

Specifying Property Names

To specify a property name using the short form, simply prefix the property name with @ or #. Use # for pattern-matching queries *(for details, see "Pattern-Matching Queries," page 108),* such as

```
#directory *\PressReleases\*
```

Otherwise, use @.

To specify a property via the long form, use the {prop} tag, like this:

```
{prop name=directory} MyDocs\LPCO\PressReleases\00 {/prop}
```

If your query expression includes wildcard characters, you must also use the {regex} tag. The long-form equivalent of the short-form query #directory *\PressReleases* would be

```
{prop name=directory} {regex} *\PressReleases\* {/regex} {/prop}
```

If your property name includes spaces, use quotation marks:

```
{prop name="Number of exasperating revisions requested"} >10 {/prop}
```

The EQUALS and CONTAINS Operators

In query expressions involving text, use the EQUALS operator when you require an exact match. The short form of the EQUALS operator is = (an equal sign). For example, the following queries

```
@doctitle  Queen's Gambit Declined
```

```
{prop name=docTitle} equals Queen's Gambit Declined {/prop}
```

locate all files whose DocTitle property value is exactly "Queen's Gambit Declined."

When you care only whether a particular word appears in a property value (no matter what else may be there), use the CONTAINS operator (or no operator; CONTAINS is the default). For example, to find documents in which the words "Queen's Gambit Declined" appear somewhere within any property (including the contents), you could write any of the following:

```
@all Queen's Gambit Declined
```

```
{prop name=all} contains {phrase} Queen's Gambit Declined {/phrase} {/prop}
```

```
{prop name=all} {phrase} Queen's Gambit Declined {/phrase} {/prop}
```

Note that the short form does not include a CONTAINS operator.

To find documents in which any of those words (or any of the inflected forms of "declined") appear, express the text in free-text mode:

```
$all Queen's Gambit Declined
```

```
{prop name=all} contains {freetext} Queen's Gambit Declined {/freetext} {/prop}
```

```
{prop name=all} {freetext} Queen's Gambit Declined {/freetext} {/prop}
```

The Relational Operators

The Indexing Service offers the following relational operators:

Operator	Description
=	Equal to
!=	Not equal to
<	Less than
<=	Less than or equal to
>	Greater than
>=	Equal to or greater than

Both the long form and the short form use the same set of relational operators.

Date and Time Expressions

Dates and times should be expressed in one of the following formats:

```
yyyy/mm/dd hh:mm:ss
```

```
yyyy-mm-dd hh:mm:ss
```

The first two year digits are optional. If you omit them, the Indexing Service regards all years as falling between 1930 and 2029. You can add an optional three-digit millisecond value to the time value (for example, 2000/04/12 14:54:23.456). All times are recorded in coordinated universal time format (UTC, or Universal Time Coordinate), which is essentially the same as Greenwich mean time.

In conjunction with relational operators, you can express times as offsets relative to the current time, using the following abbreviations:

Abbreviation	Meaning
y	Year
q	Quarter (three months)
m	Month
w	Week
d	Day
h	Hour
n	Minute
s	Second

For example, the query

```
@Write >-1d12h
```

returns files last saved within the most recent 36 hours.

The Boolean Operators

The Indexing Service offers the following Boolean operators:

Operator	Short Form	Long Form
AND	&	AND
OR	|	OR
Binary NOT	&!	AND NOT
Unary NOT	!	NOT

The binary NOT operator is used between two properties. For example, in the query

```
@DocAuthor Carl &! @DocSubject Windows
```

the binary NOT operator returns documents that match @DocAuthor Carl but not @DocSubject Windows.

The unary NOT operator is used to negate a single query expression. For example, the query

```
{prop name=size} not > 1000
```

returns documents whose size is not greater than 1000 bytes. The only reason the distinction matters is that the unary NOT is permitted only in queries in which the query expression is a numeric value.

Note that it's okay to use the short-form operator symbols in long-form queries—that is, you can substitute & for AND, | for OR, and so on. More important, be aware that the Indexing Service Help text (as well as some documents posted at Microsoft's MSDN Web site) erroneously indicates that the unary NOT operator should go before the property name in the short form, like this:

```
!@Size > 1000
```

Unfortunately, the Indexing Service will not reject this query. Instead it will ignore the NOT operator, returning results that are the opposite of what you intend.

The Proximity Operator

The proximity operator allegedly lets you look for files in which two text expressions fall within 50 words of each other. In numerous tests for this chapter, however, the service returned files in which the two expressions appeared only at significantly larger separations. (In one file, the two expressions were more than 1000 words apart.) Even assuming that noise words are disregarded in the calculation, we have to conclude that the proximity operator might better be described as a Boolean AND.

In fact, we compared the effects of the AND operator and the proximity operator, and in every test the Indexing Service returned the same set of documents with each operator. The operators differed in terms of the relevance rankings given to the files returned, but we found no consistent pattern to the differences in these rankings. We suggest that you regard the proximity operator with a degree of skepticism!

The long form of the proximity operator is NEAR; you can use either NEAR or ~ in the short form.

The Order of Operator Precedence

The Boolean and proximity operators are evaluated in the following order:

1. NOT
2. AND and NEAR
3. OR

Operators at the same precedence level are evaluated in left-to-right order. You can use parentheses to override the default precedence.

Pattern-Matching Queries

The Indexing Service supports three types of pattern-matching queries:

- Queries that use MS-DOS-style wildcard characters (* and ?)
- UNIX-style regular-expression queries
- Queries that look for alternative word forms

Queries That Use MS-DOS-Style Wildcard Characters

The Indexing Service recognizes both of the standard MS-DOS wildcard characters, * and ?. The asterisk represents any number of characters, and the question mark represents any single character.

In the short form, you can express this kind of query using either the @ or the # mode symbol. For example, both

```
#filename=*.do?
```

and

```
@filename=*.do?
```

will deliver file names whose extensions start with the characters *do* and end with at most one additional character.

Do not, however, omit the equal sign in short-form queries of this type. If you do, the Indexing Service assumes a CONTAINS operator instead of an EQUALS operator. The query

```
#filename *.do?
```

returns file names that include the characters *do* anywhere—before or after the period.

To find file names with the pattern **.do?* using the long form, write this query:

```
{prop name=filename} {regex} *.do? {/regex} {/prop}
```

Do not omit the {regex} tag. If you do, the Indexing Service returns only those files with the characters *do?* before the extension!

Queries That Use UNIX-Style Regular Expressions

The Indexing Service supports the UNIX regular-expression syntax. A full treatment of the possibilities this affords is beyond the scope of this chapter. (You can read details in the Indexing Service Help text, or at *msdn.microsoft.com/library/psdk/indexsrv/ixqlang_1n1v.htm.*) Here, however, is one potentially useful example. The query

```
{prop name=filename} {regex} *.|(do?|,xl?|,mdb|) {/regex} {/prop}
```

returns all files with any of the following extensions: .do?, .xl?, or .mdb.

Here is the equivalent short-form query:

```
#filename *.|(do?|,xl?|,mdb|)
```

Notice that in this case, as distinguished from the simple MS-DOS-style query, you must use the # mode symbol, and you must *omit* the equal sign.

Queries That Look for Alternative Word Forms

If you want to use the short form to find words that begin with particular letters, use the @ mode symbol, no equal sign, and a single asterisk. For example, the query

```
@contents dog*
```

returns documents with "dog," "doghouse," "doggerel," "dogmatic," "doggone," and so forth. Note that if you mistakenly use the # mode symbol, you get nothing!

To perform the same query using the long form, write either of the following:

```
{prop name=contents} dog* {/prop}

{prop name=contents} {generate method=prefix} dog {/generate}{/prop}
```

The {generate} tag provides finger exercise, but no more. Its method attribute currently supports only two values—*prefix* and *inflect*. As you'll see, the *inflect* value is also superfluous in the current version. (Future versions of the query language presumably will support additional kinds of alternative word forms.)

To find inflected forms of verbs, use the double-asterisk wildcard. For example,

```
@contents swim**
```

locates files containing "swim," "swam," and "swum"—but not "swimmer." Short-form users, *nota bene*: Use @, not #, and do not write an equal sign.

In the long form, the equivalent query is either of the following:

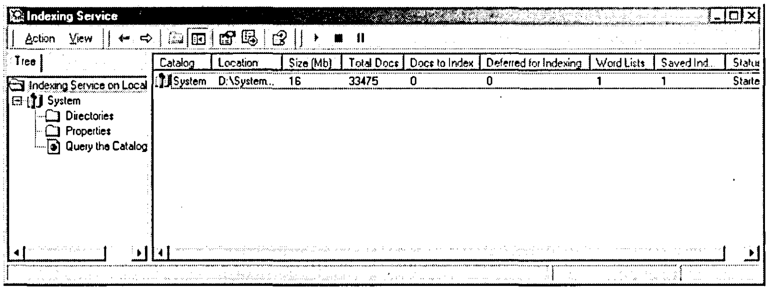
```
{prop name=contents} {generate method=inflect} swim {/generate} {/prop}

{prop name=contents} swim** {/prop}
```

Administering the Indexing Service

The MMC console for administering the Indexing Service is Ciadv.msc, shown in Figure 6-3. You can get there by any of the following routes:

- Type *ciadv.msc* at a command prompt.
- Right-click My Computer and choose Manage. In Computer Management, open Services And Applications. Under Services And Applications, select Indexing Service.
- In the Search Assistant (or the Search Explorer bar), click the Indexing Service link. (Click Search Options first if you don't see the Indexing Service link.) In the Indexing Service Settings dialog box (see Figure 6-1, page 99), click Advanced.

You must be logged on as an administrator to use the Indexing Service console. You can get there without administrative privileges (if you use one of the first two methods just described), but you can't do anything useful—or even see the status of the service.



Catalog	Location	Size (Mb)	Total Docs	Docs to Index	Deferred for Indexing	Word Lists	Saved Ind..	Statu
System	D:\System...	16	33475	0	0	1	1	Starte

Figure 6-3
If you log on as an administrator, you can use this MMC console to administer the Indexing Service.

If the Indexing Service console does not display the console tree (the left pane), you might want to do the following to display it:

1. Choose View | Customize.
2. Select the Console Tree check box and click OK.

If the Console Tree check box is already selected but the console tree is not visible, clear the check box, click OK, choose View | Customize again, and then select the check box and click OK. (This is a bug in MMC.)

The console tree displays an entry for each catalog created by the Indexing Service. By default, that includes a System catalog and, if IIS is installed, a Web catalog. You can also create additional catalogs or delete existing ones in the Indexing Service console.

Opening the entry for a catalog reveals the three subentries shown in Figure 6-3: Directories, Properties, and Query The Catalog. Directories shows which folders are indexed by the selected catalog (and lets you make changes to that list). Properties shows which properties are being indexed, and Query The Catalog provides a query form that you can use as an alternative to the Search Assistant. Queries submitted with this query form generate the same list of files as queries submitted via the Search Assistant, but the files arrive as hyperlinks rather than as Windows Explorer entries.

When you select a catalog name in the console tree, the details pane of the Indexing Service provides status information about the selected catalog.

An Overview of the Indexing Process

The Indexing Service creates and maintains its catalogs through the following processes:

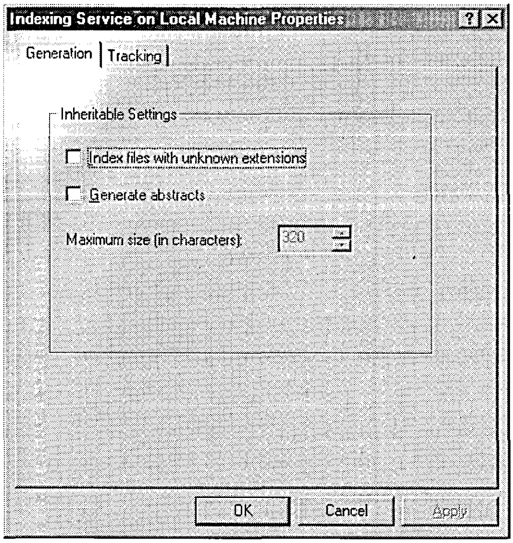
1. **Scanning.** The service scans the disks and folders to be indexed to determine which files have changed and thus need to be reindexed. A full scan takes place the first time you turn on the service, whenever you add a folder to a catalog, and whenever a serious error occurs. Incremental scans take place whenever

the service is restarted (for example, when you restart your computer) and at least once a day.

2. **The creation of word lists.** A word list is a small temporary index maintained in memory. Documents in a word list are automatically reindexed whenever the service is restarted.
3. **The creation of saved indexes.** A saved index is a highly compressed temporary disk file optimized for fast response to searches. The service combines word list data into saved indexes whenever a large enough number of word lists have accumulated.
4. **Merging.** Merging is the combining of data from multiple word lists and saved indexes into a permanent master index.

Indexing Files with Unknown Extensions

To include files with unknown extensions in all your catalogs, right-click Indexing Service On Local Machine, at the top of the console tree, and choose Properties from the shortcut menu. The dialog box shown in Figure 6-4 appears.



□ Index files with unknown extensions

□ Generate abstracts

Maximum size (in characters): 320

Figure 6-4
Use this properties dialog box to add unknown file types to your catalog.

On the Generation tab, select the Index Files With Unknown Extensions check box. The Indexing Service will then do its best to extract meaningful content from file types for which it lacks a filter. After you've made this change, you need to stop and restart the Indexing Service to have your change take effect.

To index unknown file types only in a particular catalog, right-click that catalog's name in the console tree and then choose Properties. On the Tracking tab, clear the Inherit Above Settings From Service check box. Then go to the Generation tab and select Index Files With Known Extensions. (If you don't first clear Inherit Above Settings From Service, your catalog uses whatever setting you've applied to the service as a whole.) After making this change, stop and restart the catalog to have your change take effect.

Supplying an Alias for a Folder Name

By default, the Indexing Service identifies remote folders by their share names and their full UNC paths. The UNC paths appear in the Alias column in the details pane of the Indexing Service console. If this default alias is not to your liking, right-click Indexing Service On Local Machine, choose Properties from the shortcut menu, go to the Tracking tab, and clear the Add Network Share Alias Automatically check box. You can then supply your own alias (if you want) by expanding the catalog entry in the console tree, selecting Directories in the console tree, double-clicking the directory (folder) name in the details pane, and filling out the ensuing dialog box.

You can also clear the alias default at the catalog level rather than the service level. To do so, right-click the catalog name, choose Properties, go to the Tracking tab, clear the Inherit Above Settings From Service check box, and then clear Add Network Share Alias Automatically.

Stopping, Pausing, and Restarting

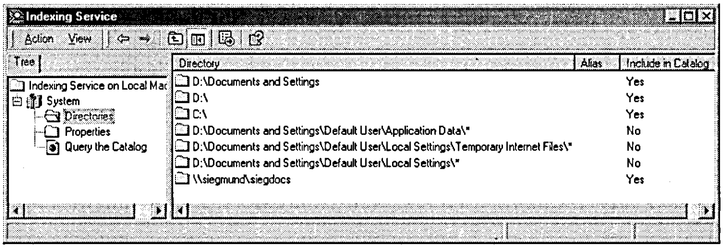
To stop the service, right-click Indexing Service On Local Machine and choose Stop from the shortcut menu. To stop a particular catalog, right-click that catalog's name, choose All Tasks from the shortcut menu, and then choose Stop.

To pause the service or a catalog, follow the same steps, but choose Pause instead of Stop. While the service or a catalog is paused, you can still execute queries, but no further catalog processing occurs. To restart after a pause or a stop, retrace your steps and choose Start.

Changing the Folders Included in a Catalog

To see which folders are included in a catalog, open the catalog's entry in the console tree and select Directories. Figure 6-5 shows a sample of what you might see.

Folders with a Yes in the Include In Catalog column are part of that catalog—as are all their subfolders, with the exception of subfolders explicitly excluded by entries that have a No in the Include In Catalog column.



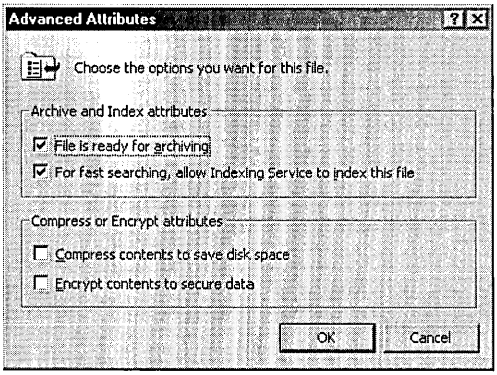
Directory	Alias	Include in Catalog
D:\Documents and Settings		Yes
D:\		Yes
C:\		Yes
D:\Documents and Settings\Default User\Application Data*		No
D:\Documents and Settings\Default User\Local Settings\Temporary Internet Files*		No
D:\Documents and Settings\Default User\Local Settings*		No
\\siegmund\siegdocs		Yes

Figure 6-5
The Directories list shows which folders a catalog includes.

To add a folder to the catalog, right-click Directories in the console tree, choose Add, and then choose Directory. In the ensuing dialog box, supply the path and alias of the folder you want to add. To delete a folder, right-click it in the details pane and choose Delete from the shortcut menu. To change a folder's status—from included to excluded, or vice versa—double-click the folder in the details pane. In the ensuing dialog box, select Yes or No as appropriate.

Excluding Specific NTFS Files

To explicitly include or exclude an NTFS file from your catalog(s), right-click the file in a Windows Explorer window and choose Properties from the shortcut menu. On the General tab of the properties dialog box, click the Advanced button to display the Advanced Attributes dialog box, shown in Figure 6-6. Clear the For Fast Searching, Allow Indexing Service To Index This File check box to exclude this file from all catalogs.



Choose the options you want for this file.

Archive and Index attributes

☑ File is ready for archiving
☑ For fast searching, allow Indexing Service to index this file

Compress or Encrypt attributes

□ Compress contents to save disk space
□ Encrypt contents to secure data

Figure 6-6
You can use this Advanced Attributes dialog box to explicitly exclude a file from your catalog(s).

Manually Rescanning a Folder

You can manually initiate an incremental or full scan of any folder by right-clicking the folder name in the details pane, choosing All Tasks, and then choosing Rescan (Full) or Rescan (Incremental). Microsoft recommends that you do a full rescan if you install a new filter, start or stop the indexing of unknown file types, or edit the noise word file.

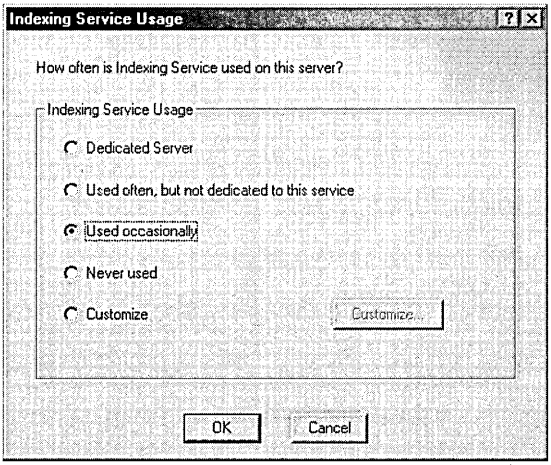
Creating and Deleting Catalogs

To create a new catalog, right-click Indexing Service On Local Machine (in the console tree), choose New from the shortcut menu, and then choose Catalog. You'll be asked to supply a name and storage location for the new catalog.

To delete a catalog, first stop the Indexing Service. Then right-click the catalog's name in the console tree, choose Delete from the shortcut menu, and answer the confirmation prompt.

Adjusting the Indexing Service's Performance Parameters

To adjust the Indexing Service's performance parameters, first stop the service. Right-click Indexing Service On Local Machine in the console tree, choose All Tasks, and then choose Tune Performance. These steps take you to the Indexing Service Usage dialog box, shown in Figure 6-7.



Indexing Service Usage

How often is Indexing Service used on this server?

Indexing Service Usage

○ Dedicated Server

○ Used often, but not dedicated to this service

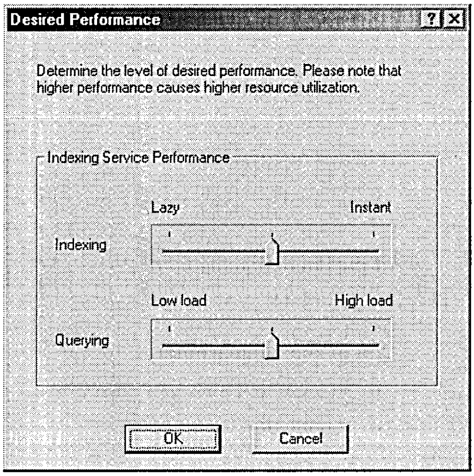
● Used occasionally

○ Never used

○ Customize

Figure 6-7
The Indexing Service Usage dialog box lets you choose a broad performance category.

If none of the first four options listed in this dialog box quite describes your situation, choose Customize, and then click the Customize button. The Desired Performance dialog box, shown in Figure 6-8, appears.



Desired Performance

Determine the level of desired performance. Please note that higher performance causes higher resource utilization.

Figure 6-8
The Desired Performance dialog box allows further fine-tuning.

The sliders here control the processing priority that Windows 2000 will give to the service's catalog building (Indexing) and query processing (Querying). Moving either slider to the right makes the service more responsive while reducing the performance of whatever applications you might be running concurrently with the Indexing Service.

Chapter 7

The Windows 2000 Shell: Beyond the Basics

In This Chapter

Removing Impediments 117
Using Cascading Folder Names 123
Using Windows Explorer's Command-Line Syntax 124
Relocating Shell folders 126
Adding or Changing Shortcut Menu Commands 128
Using Third-Party Shell Tools 130

Getting Windows Explorer and the other components of the Microsoft Windows 2000 shell to look and work in a manner congruent with your level of expertise is critical to your satisfaction with Windows 2000. Fortunately, Microsoft made the shell highly customizable, so with a modicum of effort you *can* tailor it to your comfort. Unfortunately, the system's default behavior is designed to serve a user whose preferences probably differ considerably from your own. Therefore you'll almost certainly need to mold the shell in a variety of ways to get it working the way you want.

To assist you in that effort, this chapter provides a brief power user's tour of Windows Explorer and other elements of the Windows 2000 shell.

Removing Impediments

The default design of Windows Explorer promotes simplicity at the expense of expert users' convenience. Ordinarily, the shell opens without the invaluable Folders bar, providing an elementary display but making navigation among folders more difficult than it needs to be. System files and files with the hidden attribute are not normally displayed, paths are suppressed from folder address and title bars, file name extensions are excluded, and a potentially obnoxious HTML template discourages exploration of particular folders, such as %SystemRoot% and System32. One of the first things you might want to do to streamline your work in Windows Explorer is to make the shell a little less protectively simple.

Including the Folders Bar by Default

Windows Explorer can open in either of two modes, with or without the Folders bar. If you right-click any folder name, you'll see these two modes identified on the shortcut menu as *Open* and *Explore.* Open, the factory default, provides a single-pane display, without the Folders bar. Explore generates a two-pane display, including the Folders bar.

If you like using the Folders bar for navigation or for moving and copying items between folders, you'll probably want to make explore mode the default action for folders:

1. In any Windows Explorer window, choose Folder Options from the Tools menu.
2. On the File Types tab of the Folder Options dialog box, scroll down and select Folder (not File Folder!). Because the Folder entry has an N/A extension, the easiest way to find it is to click the File Types heading first. Doing so sorts the list by type rather than by extension.
3. Click the Advanced button.
4. In the Actions list, select Explore.
5. Click Set Default; then click OK and Close to get out of the dialog box.

Now, any time you open a Windows Explorer window, you'll get the Folders bar. On those occasions when you want to see folder contents without the namespace outline, you can simply click Folders on the Windows Explorer toolbar. Or, if you want to navigate by history (returning to a folder or a Web site you've recently visited), you can click the History button to replace the Folders bar with the History bar.

"De-Personalizing" the Start Menu

Like the Office Assistant—that cute little animated figure that periodically descends upon your Microsoft Word or Microsoft Excel document—the "personalized" Start menu introduced with Windows 2000 is more apt to provoke love or hate than feelings of neutrality. Those who love it are relieved not to have to scroll their Programs and Favorites menus. Those who feel the opposite chafe at the erratic positioning of menu items and the disappearance of items they happen not to have used in a week or two.

If the little double-headed arrows at the bottoms of menus annoy you, don't despair. Simply "de-personalize":

1. Choose Start | Settings | Taskbar & Start Menu.
2. On the General tab, clear the Use Personalized Menus check box.

Adding Good Stuff to Your Start Menu

While you're in the Taskbar And Start Menu Properties dialog box, click over to the Advanced tab. The list at the bottom of this dialog box includes eight check boxes, the first seven of which you'll almost certainly want to select. These add valuable items to your Start menu—a cascading Control Panel submenu, for example, that saves you the trouble of opening the entire Control Panel when all you need is one item. (See Figure 7-1.)

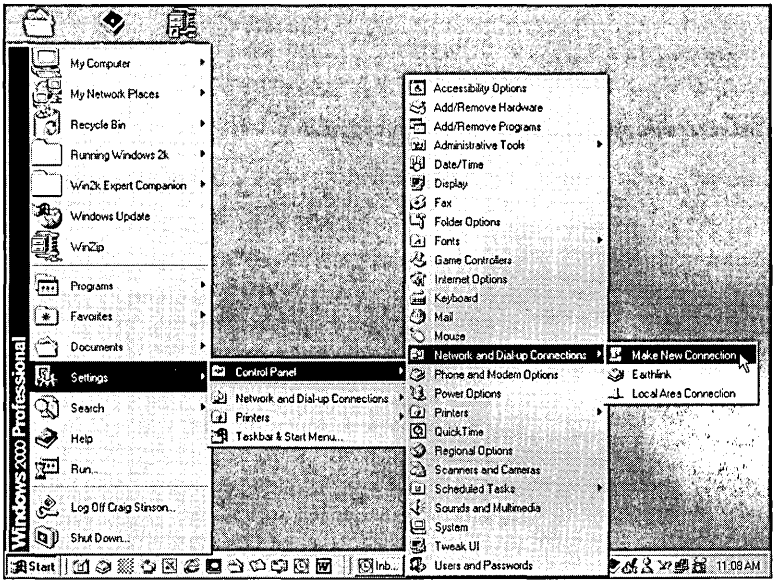


Figure 7-1
A cascading Control Panel menu is a great time-saver.

The last option in this dialog box, Scroll The Programs Menu, doesn't add anything to the Start menu, but it does change the menu's behavior. If your Programs menu becomes too tall for your screen, Windows 2000 by default displays the spillover in one or more adjacent columns. If you'd rather scroll to get the whole Programs menu, select this check box.

Revealing Hidden and System Items

By default, Windows Explorer hides files and folders that have either the hidden attribute or the system attribute set. Such files not only don't show up in folder windows; they're also invisible to the Search command. The operating system keeps these things out of sight, on the assumption that what you can't see you can't delete, rename, or corrupt.

To make hidden files and folders visible, choose Tools | Folder Options in Windows Explorer, click the View tab, and select Show Hidden Files And Folders. To make visible files and folders with system and hidden attributes (the so-called "superhidden" items), clear Hide Protected Operating System Files (Recommended).

If you want hidden and system files and folders to stay invisible most of the time, but you occasionally need to search for such items, you can open a Search window, use the Tools menu to reveal the hidden stuff, perform your search, and then use the Tools menu again to put things back in their original state. Alternatively, if you know the folder in which a hidden item resides, you can open a Command Prompt window, navigate to that folder, and then use the Dir command with the /Aswitch. Typing the command *dir /ash,* for example, generates a list of items with the system and hidden attributes.

Displaying or Hiding Extensions

Windows Explorer normally displays file name extensions only for file types unknown to the registry, leaving you to discern the type of most files by their icons or their entries in the Type column (if you're using Details view). If you find this level of feedback inadequate—if you long for the full *filename.extension* presentation of an MS-DOS directory listing, for example—you can go to the View tab of the Folder Options dialog box and clear Hide File Extensions For Known File Types.

If you need to see extensions only for certain registered file types, however, there's a better solution:

1. Choose Tools | Folder Options, and click the File Types tab.
2. Select the file type whose extension you want to see.
3. Click Advanced.
4. Select Always Show Extension.

These steps add the string value AlwaysShowExt to the class definition registry subkey for the selected file type. You could achieve the same result by opening a registry editor and adding this subkey by hand, but we recommend that you make direct changes to the registry only when the Windows user interface doesn't provide an indirect method.

You do need to modify the registry directly if you want to make extensions visible for a file type that doesn't appear in the Windows Explorer File Types list. Here's the procedure:

1. Run Regedit or Regedt32.
2. Look for the subkey HKCR\.*ext,* where *ext* is the extension of your file type.
3. If that subkey doesn't exist, create it.
4. To the subkey HKCR\.*ext,* add the string value AlwaysShowExt. Do not add any data to the value AlwaysShowExt.

5. Log off and then log back on to have this change take effect. (This is necessary only for file types that don't appear in the File Types list.)

For information about using Regedit and Regedt32, see Chapter 39, "Working with the Registry."

Note that if you want to know a file name's extension on an ad hoc basis, you can't simply right-click the file and look at its properties dialog box. You could do this in earlier versions of Windows, but Windows 2000 doesn't do you the courtesy of showing the extension in the properties dialog box. What you can do is right-click the file and choose Open With. The full file name, including extension, appears at the top of the Open With dialog box. It's kludgy, but it works.

It's possible to achieve the opposite effect of AlwaysShowExt—to *suppress* the extension for a particular file type, even if you've cleared Hide File Extensions For Known File Types in the Windows Explorer Folder Options dialog box. Presumably because the designers of Windows considered this an unlikely request, they did not provide a UI switch for this purpose. So here's another case in which a direct registry edit is required.

To hide a file type's extension when all other extensions are displayed:

1. Run Regedit or Regedt32.
2. Navigate to the key HKCR\\.*ext*, where *ext* is the extension of the file type in question.

   In most cases, the subkey for the extension you're interested in will have, as its default data, a plain-English program identifier. For example, if you go to HKCR\\.bmp in Regedit, you will see

   ```
   (Default)     REG_SZ     PaintPicture
   ```

   in the right pane. In Regedt32, you will see

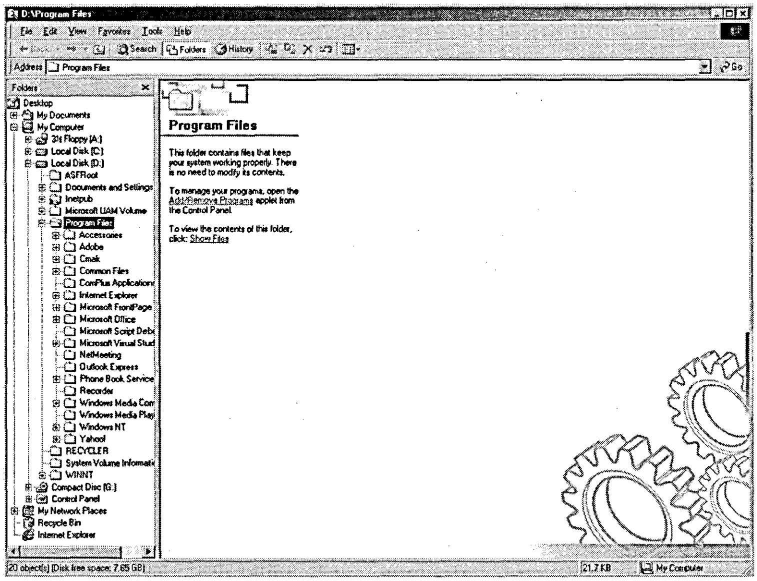
   ```
   <NoName>:REG_SZ:PaintPicture
   ```

3. Navigate to HKCR\programidentifier, where *programidentifier* is this plain-English descriptor.
4. To the subkey HKCR\programidentifier, add the string value NeverShowExt. Do not add any data to the value NeverShowExt.
5. Log off and then log back on to make this change effective.

Chapter 7

Removing the "Nag" Screens

If you've selected Enable Web Content In Folders in the Windows Explorer Folder Options dialog box, it's possible you've encountered a screen similar to the one shown in Figure 7-2. It's equally possible that you've felt vexed by the operating system's presumption that you ought not to be looking at the contents of certain folders, such as Program Files, %SystemRoot%, and System32.



This folder contains files that keep your system working properly. There is no need to modify its contents.

To manage your programs, open the Add/Remove Programs applet from the Control Panel.

To view the contents of this folder, click: Show Files

Figure 7-2
It's easy to get rid of "nag" screens like the one shown here.

In reality, the requirement that you click the Show Files link to see the contents of such folders is not *that* onerous, because you don't have to do this every time you visit the affected folder. After you've done it once, Windows Explorer remembers, and for the duration of your session in Windows 2000 the nag screen stays out of your way.

But if you hate being nagged even once, you can easily do away with the thing, without giving up your preference to show Web content in folders:

1. Open the file Desktop.ini in the folder where you want to remove the nag screen.
2. Put an apostrophe at the beginning of the line that starts

   ```
   WebviewTemplate.NT5=
   ```

3. Save the Desktop.ini file.

Commenting out the line that specifies the HTML template for this folder is the least destructive and most easily reversible solution to the problem. If you change your mind, you can simply go back into the .ini file and take out the apostrophe.

Using Cascading Folder Menus

Earlier in this chapter, we mentioned the so-called "advanced" options available via Start | Settings | Taskbar & Start Menu. Along with offering other valuable options, the Advanced tab of the Taskbar And Start Menu Properties dialog box lets you add a cascading Control Panel submenu to your Start menu.

Windows 2000 also lets you add other cascading folders to the Start menu. For example, to create a cascading My Computer item at the top of the menu, simply right-drag My Computer to the Start button, wait until the menu opens, drag to the top of the menu, release the mouse button, and choose Create Shortcut(s) Here. You can then rename the item to get rid of the "Shortcut to" verbiage. As Figure 7-3 shows, such a menu makes it easy to open just about any folder on your system. (For amusement, you can even cascade that menu around in circles, since Start Menu is itself a folder subordinate to My Computer.)

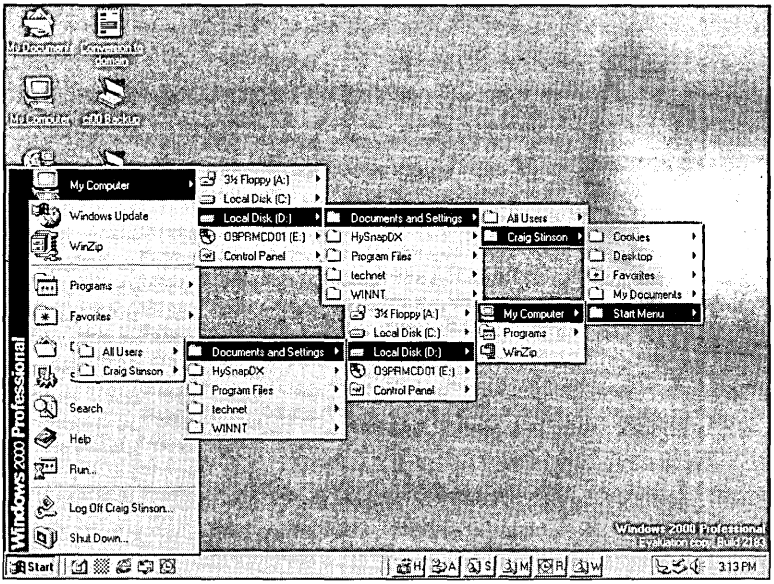


Figure 7-3
Adding My Computer to the Start menu lets you navigate easily to distant realms.

Any system folder or ordinary file folder can be added to the Start menu in this fashion. If you regularly visit subfolders nested within My Network Places, for example, you might find it helpful to put My Network Folders on the Start menu. If the project you're currently working on takes you repeatedly to a particular document folder on your server, adding that folder to the Start menu could be a step-saver for you. When you complete the project, you can simply delete the folder shortcut from the menu.

As an alternative to piling onto your Start menu, consider adding a folder to your taskbar as a toolbar. Drag the folder to an unoccupied spot on the taskbar. Windows 2000 creates a new toolbar for your folder. Then drag the toolbar as far to the right as possible (if your taskbar is at the top or bottom of the screen) so that only the name shows. Now you can click the chevron at the right side of the toolbar (folder) name to create a cascading pop-up menu.

Using Windows Explorer's Command-Line Syntax

Cascading folder menus, whether on the Start menu or in the form of a toolbar, make it easy to open Windows Explorer with a particular folder in view. But this might not be the ideal way. Compare the two views of D:\Winnt shown in Figure 7-4. The one on the left was generated by a Start menu item, subordinate to My Computer. The one on the right was produced by a command-line string.

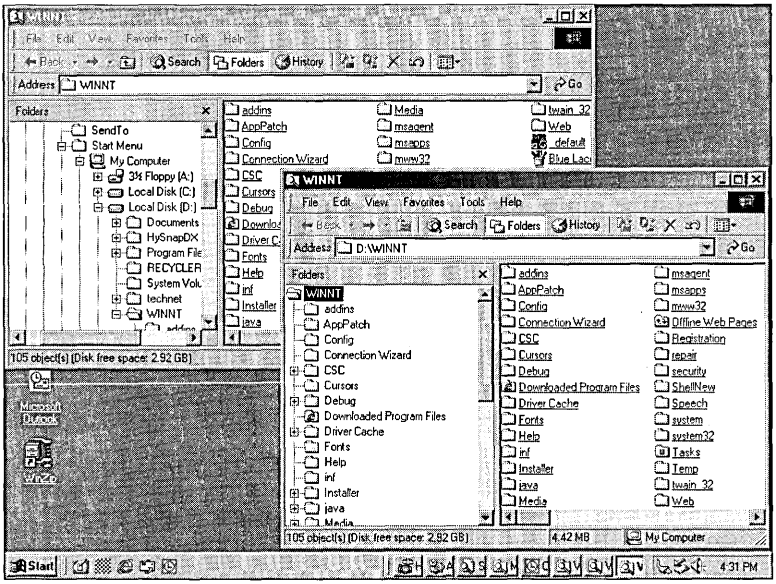


Figure 7-4
The view on the right, generated by a command-line string, restricts the Folders bar to a particular namespace node.

The difference between the two views is all in the left pane, the Folders bar. The command-line string in this case puts the selected folder (Winnt) at the top of the namespace hierarchy, eliminating all of Winnt's ancestry and letting you focus your attention on Winnt's subfolders.

This is one example of the potential utility of the Windows Explorer command-line syntax. You can probably find others in your own work. You can use Windows

Explorer command strings in shortcuts, with the Start menu's Run command, at the command prompt, or in batch files. The syntax is as follows:

```
explorer [/n|/e][,/root,object][[,/select],subobject]
```

/N Opens without displaying the Folders bar.

/E Opens with the Folders bar displayed.

/Root,*object* Restricts Windows Explorer to *object* and all folders contained within *object*.

/Select,*subobject* Gives the initial focus to the parent folder of *subobject* and selects *subobject*. If /select is omitted, *subobject* specifies the folder that gets the initial focus.

Let's look at some examples. To begin,

```
explorer /e,/root,d:\winnt
```

opens Windows Explorer and displays the Folders bar, restricting the namespace to D:\Winnt and its subfolders. (This is the syntax used to generate the window on the right side of Figure 7-4.)

To open D:\Winnt\Cursors in Windows Explorer, with the Folders bar displayed and the file Appstart.ani selected, you must include the file name and extension in the command string, as shown here:

```
explorer /e, /select,d:\winnt\cursors\appstart.ani
```

Typing the following opens D:\Winnt without the Folders bar:

```
explorer d:\winnt
```

The folder is loaded as the subobject focus, not as the root folder.

This simple string opens My Documents, with the Folders bar displayed:

```
explorer
```

The string

```
explorer /n
```

opens the drive on which Windows 2000 is installed without displaying the Folders bar, while

```
explorer /e,.
```

opens the current folder in Windows Explorer. This is particularly handy if you've used the CD command in a Command Prompt window to navigate to a folder and you then want to use Windows Explorer to manipulate files in that folder.

You're probably wondering why typing *explorer*, by itself, opens My Documents, whereas typing *explorer /n* opens the drive on which Windows 2000 is installed. We wonder, too. Microsoft changed the default behavior of Windows Explorer in Windows 2000. Formerly, the shell opened My Computer by default; now it opens My

Documents. But typing the command string *explorer /n* opens neither My Computer nor My Documents. Go figure.

Using GUIDs to Open Shell Folders in Windows Explorer

A GUID, or *globally unique identifier,* is a string of 32 hexadecimal digits enclosed within braces, with hyphens separating the digits into groups of eight, four, four, four, and twelve—like this:

```
{nnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnn}
```

Windows 2000 uses GUIDs to identify all kinds of objects, including certain system folders. You can open the following GUIDs in Windows Explorer:

{208D2C60-3AEA-1069-A2D7-08002B30309D}	My Network Places
{20D04FE0-3AEA-1069-A2D8-08002B30309D}	My Computer
{2227A280-3AEA-1069-A2DE-08002B30309D}	Printers
{645FF040-5081-101B-9F08-00AA002F954E}	Recycle Bin
{7007ACC7-3202-11D1-AAD2-00805FC1270E}	Network And Dial-Up Connections
{D6277990-4C6A-11CF-8D87-00AA0060F5BF}	Scheduled Tasks

When you include a GUID in a command string, precede it with two colons, like this:

```
explorer ::{208D2C60-3AEA-1069-A2D7-08002B30309D}
```

If typing all 38 characters of the GUID, including the braces and hyphens, isn't your idea of fun, you can copy the string out of the registry:

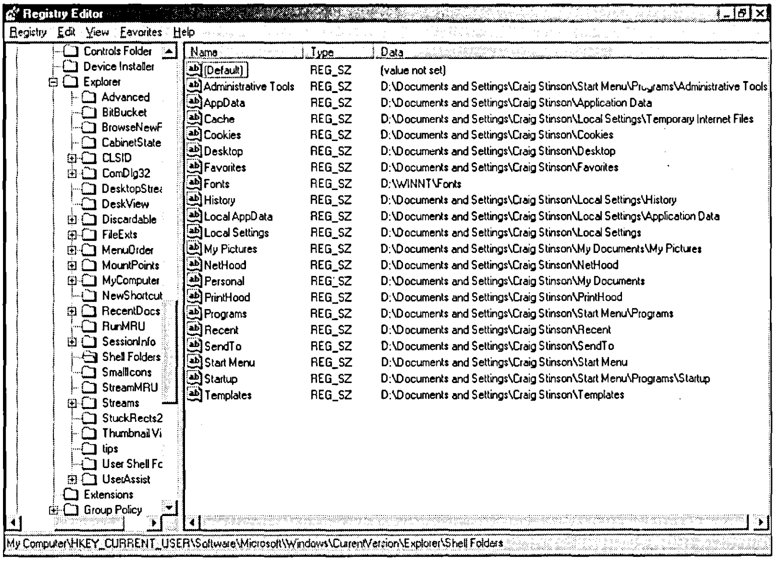
1. Run Regedit.
2. Select HKCR.
3. Press Ctrl+F and search for the name of the folder you want.
4. When Regedit finds your folder, make sure that the key name displayed on the Status bar ends with the GUID listed in this book. (Use the View menu to make the Status bar visible if it isn't already.) If the GUID doesn't match, press F3 to find the next occurrence of your search string.
5. In Regedit's left pane, right-click the subkey marked by the open folder (which should be near the bottom of the pane) and choose Copy Key Name.
6. Paste the key name into your command string, and then delete everything up to the opening brace.

Relocating Shell Folders

Certain shell folders—for example, My Network Places and Printers—are constructs of Windows 2000 that do not correspond to traditional disk directories. You can display them as folders in Windows Explorer, but you can't display them with a Dir command at the command prompt. You also can't change their locations, because they're not located anywhere!

Others, such as your Start Menu folder, are ordinary disk folders. These you can relocate if the need arises. Both you and a colleague, for example, might want to move your Favorites folder to a network share so that you can enjoy each other's latest Web discoveries. Or you might want to move one or more such folders to a different partition if the one where they're currently located is running out of space.

To change the location of a shell folder, you need to edit the registry key HKCU \Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders. Figure 7-5 shows what this key looks like on a typical system. To make the change, simply double-click the appropriate value in the right pane of Regedit or Regedt32 and supply the new path and folder name.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Administrative Tools	REG_SZ	D:\Documents and Settings\Craig Stinson\Start Menu\Programs\Administrative Tools
AppData	REG_SZ	D:\Documents and Settings\Craig Stinson\Application Data
Cache	REG_SZ	D:\Documents and Settings\Craig Stinson\Local Settings\Temporary Internet Files
Cookies	REG_SZ	D:\Documents and Settings\Craig Stinson\Cookies
Desktop	REG_SZ	D:\Documents and Settings\Craig Stinson\Desktop
Favorites	REG_SZ	D:\Documents and Settings\Craig Stinson\Favorites
Fonts	REG_SZ	D:\WINNT\Fonts
History	REG_SZ	D:\Documents and Settings\Craig Stinson\Local Settings\History
Local AppData	REG_SZ	D:\Documents and Settings\Craig Stinson\Local Settings\Application Data
Local Settings	REG_SZ	D:\Documents and Settings\Craig Stinson\Local Settings
My Pictures	REG_SZ	D:\Documents and Settings\Craig Stinson\My Documents\My Pictures
NetHood	REG_SZ	D:\Documents and Settings\Craig Stinson\NetHood
Personal	REG_SZ	D:\Documents and Settings\Craig Stinson\My Documents
PrintHood	REG_SZ	D:\Documents and Settings\Craig Stinson\PrintHood
Programs	REG_SZ	D:\Documents and Settings\Craig Stinson\Start Menu\Programs
Recent	REG_SZ	D:\Documents and Settings\Craig Stinson\Recent
SendTo	REG_SZ	D:\Documents and Settings\Craig Stinson\SendTo
Start Menu	REG_SZ	D:\Documents and Settings\Craig Stinson\Start Menu
Startup	REG_SZ	D:\Documents and Settings\Craig Stinson\Start Menu\Programs\Startup
Templates	REG_SZ	D:\Documents and Settings\Craig Stinson\Templates

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

Figure 7-5
You can move any of these shell folders to a new location by modifying this and one other registry key.

After changing HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer \Shell Folders, move on down to HKCU\Software\Microsoft\Windows\Current Version\Explorer\User Shell Folders. If the shell folder you're relocating also appears in this key, make the same change here as well.

You'll notice that your My Documents folder appears in both registry keys under the name Personal. You can relocate My Documents by changing these keys, but it's not necessary or advisable. Rather, to store your documents somewhere new—on a network share, for example—right-click My Documents on the desktop and choose Properties from the shortcut menu. Then fill out a new path on the Target line. (The advantages of changing My Documents this way are that you don't have to open the registry—something you should avoid doing when safer methods are available—and that Windows 2000 will give you the option of moving your current documents to the new location.)

When moving shell folders, be careful that you don't assign two folders to the same disk location.

Adding or Changing Shortcut Menu Commands

When you right-click a file or folder in Windows Explorer, you get the familiar shortcut menu of commands available for that object. The commands that appear on this menu are derived from the following registry locations:

- HKCR*class*\Shell (where *class* is a class definition for a file type)
- HKCR*\Shell
- HKCR\Unknown\Shell
- HKCR*class*\Shellex\ContextMenuHandlers
- HKCR*\Shellex\ContextMenuHandlers
- Shell32.dll

Those that appear under HKCR*class*\shell are file-type specific. You can easily add new commands here or delete or edit existing ones. Those that appear under HKCR*\Shell and HKCR\Unknown\Shell work just like the ones under HKCR*class*\Shell except that they apply to all file types (*) or to unregistered file types (Unknown). You can change these, too.

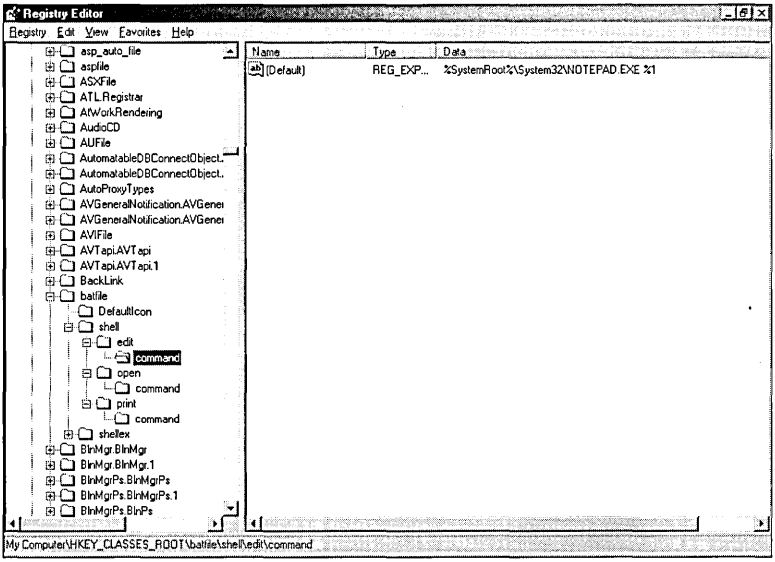
Those that appear under HKCR*class*\Shellex\ContextMenuHandlers or HKCR* \ContextMenu Handlers are shell extensions provided by .exe or .dll files. Don't mess with these.

The ones that come from Shell32.dll are the so-called *canonical verbs*—Cut, Copy, Paste, Delete, Rename, and Properties. A few class definitions include ShellFolder subkeys with Attributes values that disable particular canonical verbs. The Attributes value is an eight-digit hexadecimal number that, when converted to binary, produces a bit field that specifies which canonical verbs should appear, according to the following scheme:

Bit Number(Rightmost is bit 0)	Canonical Verb
16	Paste
24	Copy
25	Cut
28	Rename
29	Delete
30	Properties

You can disable a command by changing its bit from 1 to 0 or reenable it by changing it back to 1. It's probably not worth the bother.

An example of how the HKCR*class*\Shell commands work is shown in Figure 7-6. Batfile is the class definition for files with the extension .bat. Three commands are defined under HKCR\Batfile\Shell: Edit, Open, and Print. Each has its own subkey, and each subkey has a subkey called Command. The default value of Command provides the string that executes the command. The %1 at the end of the command string is a placeholder for the name of the file that you right-click.



Name	Type	Data
(Default)	REG_EXP...	%SystemRoot%\System32\NOTEPAD.EXE %1

My Computer\HKEY_CLASSES_ROOT\batfile\shell\edit\command

Figure 7-6
This registry subkey defines the Edit command that appears on the shortcut menu for .bat files.

To create your own shell command:

1. Run Regedit or Regedt32.
2. Navigate to the key HKCR\\.*ext*, where *ext* is the extension of the file type in question.
3. Navigate to HKCR\programidentifier\shell, where *programidentifier* is the plain-English descriptor that appears as the default value for HKCR\\.*ext*.
4. Create a subkey for the command you want to create.
5. Under this subkey, create the subkey Command.
6. As the default value for Command, type the command string you want to execute.

It's a good idea to enclose the %1 placeholder in quotation marks. Doing this ensures that if the file name to which you apply your command includes spaces, the command string won't mistake the file name for two or more separate arguments.

Using Third-Party Shell Tools

The following tools, which are available from other vendors, offer some additional flexibility, convenience, and capabilities. For more information about these programs and links to the vendors, see the companion CD.

TweakUI

TweakUI is not exactly a third-party item, because it comes from Microsoft. But it's not part of Windows 2000 and is no longer included with the Windows Resource Kits. When added to Control Panel, TweakUI lets you modify your environment in a large number of ways. You can change the behavior of your mouse, modify the appearance of shortcut icons, change the animation associated with menus and dialog boxes, and do a great deal more. As this book went to press, the download site for the Windows 2000 version of TweakUI had not yet been determined. Search for it within *www.microsoft.com*, and be sure to get the Windows 2000 version.

Tweaki for Power Users

JerMar Software's Tweaki for Power Users provides a busy dialog box full of customizing options, including items for Windows 2000, Windows 9x, and Microsoft Office. Tweaki is shareware. You can download it from *www.jermar.com*.

Part 3

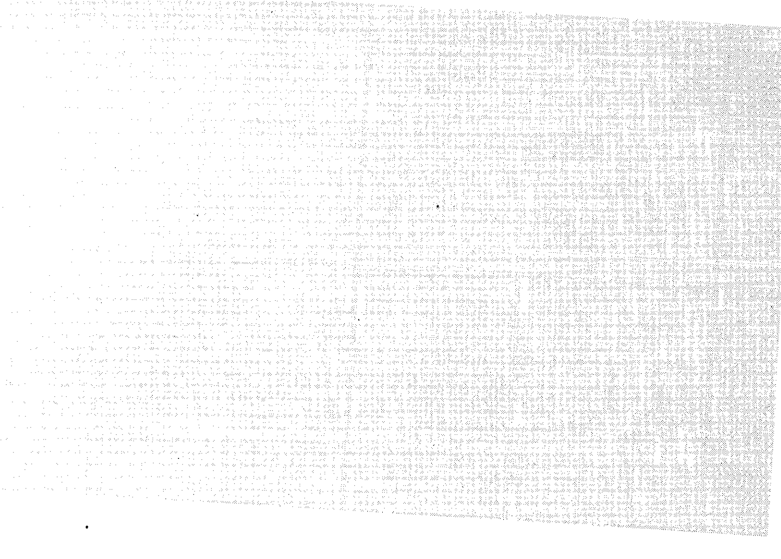
Managing Programs

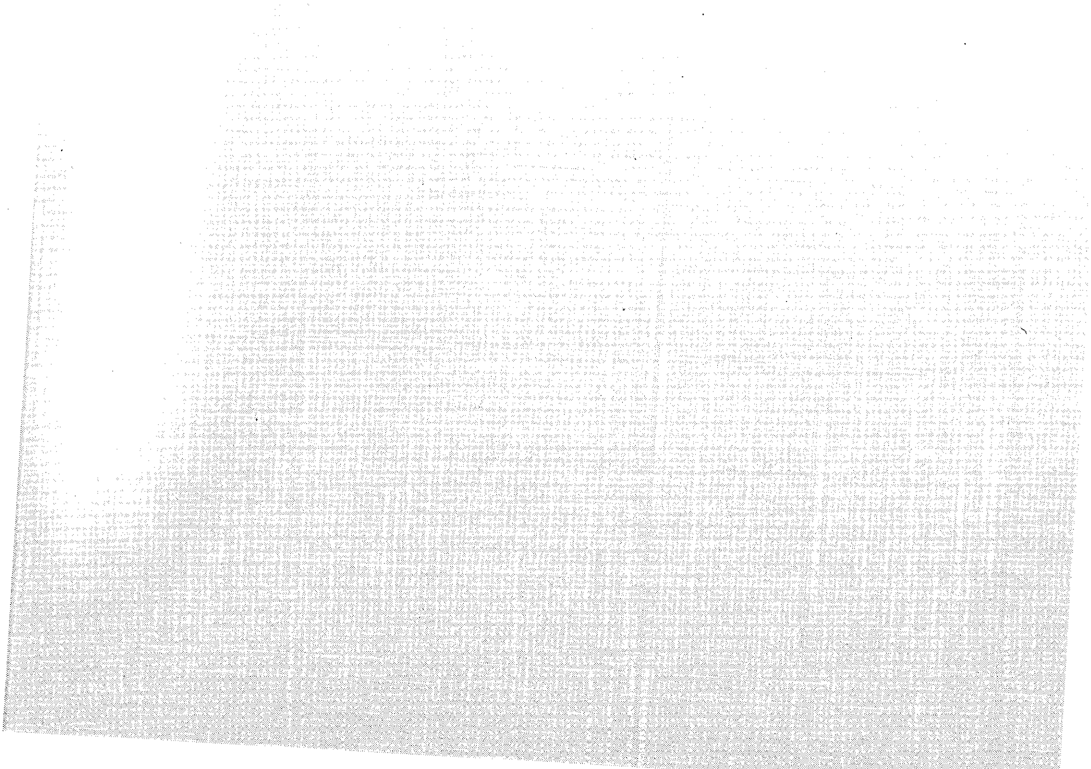
Chapter 8
Running Programs 133

Chapter 9
Installing and Removing Programs and System Components . 145

Chapter 10
Using Programs Written for Other Operating Systems 153

Chapter 11
Using the Command Prompt 171





Chapter 8

Running Programs

In This Chapter

Using Command Lines, Paths, and MRUs 133

Controlling Programs and Services that Start at Logon 135

Scheduling Tasks 137

Running a Program Under a Different User Account 142

Downloading Compatibility Updates 143

Using Apcompat to Solve Compatibility Problems 143

Probably nothing in Microsoft Windows is more self-evident than running programs. Thanks to the Start menu, most recently used (MRU) lists, file-type associations, the Documents menu, and the Favorites menu, even the greenest beginner is unlikely to have difficulty getting his or her favorite application or document aloft. But a few fine points need to be considered, and this chapter considers them. In particular, we discuss scheduled (and startup) program execution, ways to run a program under a different user account, and applications that present compatibility issues with Microsoft Windows 2000. We also take a brief look at command-line execution of Windows-based programs (saving non-GUI programs for Chapter 10).

Using Command Lines, Paths, and MRUs

You can execute command strings in a variety of places: on the Run command line (the command line that appears when you choose Run from the Start menu), on the Target line of a shortcut's properties dialog box, in a Command Prompt window, on the Address toolbar, on the Address bar in Internet Explorer, and even on the Address bar in Windows Explorer. Several of these venues maintain lists of your most recently executed command strings.

Command strings can specify the name of an .exe file, a .lnk file (a shortcut), a batch file or script, or a document whose file type is associated with a program (for example, a .bmp file). If any file name in the string includes spaces, you should enclose that file name within quotation marks.

Like MS-DOS, Windows 2000 uses the Path environment variable to find executables. To inspect your Path variable, choose Run from the Start menu and type *msinfo32*. That launches the System Information console in MMC. Expand Software Environment in the console tree, click Environment Variables in the console tree, click Path in the details pane, and then rest your mouse on the part of the variable text that appears to the right of the variable name. The full text then becomes visible as a ScreenTip.

To edit the Path variable, choose Settings | Control Panel | System. On the Advanced tab, click Environment Variables. Under System Variables, select Path and click Edit. You must be logged on as an administrator to edit any system variable. (You can also use the System Properties dialog box to simply inspect the Path variable, of course, but the dialog box is severely scrunched, and you can't read the entire contents of the variable unless you scroll horizontally.)

Some executables that don't reside along the path can nevertheless be executed from command strings without a full path specification. That's because their registry data includes path information. The simplest way to find out whether the program you're interested in can be run that way is to try invoking it without the path and see what happens.

Windows facilitates command reexecution by maintaining separate MRU lists for command strings entered via the Run command, the Address toolbar, and the Address bar in Internet Explorer. The MS-DOS subsystem also records an MRU list, good only for the life of a Command Prompt session. (To reexecute a command in a Command Prompt window, press F7 and select from the menu.)

In addition to these MRU lists, Windows helps you reenter commands in a variety of other ways. The History bar in Windows Explorer and Internet Explorer, for example, keeps a record of your activities that covers the most recent three weeks. The Documents menu maintains a list of your 15 most recently used documents (shortcuts to many more than 15 are kept in your Recent folder), and the common dialog boxes (the File Open dialog box in Microsoft Word, for example) have their own built-in historians.

All this convenience might occasionally prove inconvenient—particularly if you're reluctant to have your colleagues know about every Web site you happen to visit. You can hide your tracks from casual onlookers by locking your workstation whenever you leave your desk. (Press Ctrl+Alt+Delete and choose Lock Computer.) Under ordinary circumstances you can make your history invisible to other user accounts by putting the sensitive data on an NTFS volume and using file and folder permissions settings to ward off intruders. For good measure, you can also apply NTFS file encryption to folders you're concerned about. Encrypting and restricting access to your %UserProfile% folder and all its subfolders will keep casual snoopers out of your History, Temporary Internet Files, and Recent folders—provided, of course, that you haven't moved those folders from their default locations.

Note If you choose Start | Settings | Taskbar & Start Menu and then click the Advanced tab, you will find a Clear button that promises to "remove records of recently accessed documents, programs, and Web sites." Although clicking this button erases your Documents menu and three MRU lists—those of the Start menu, the Address toolbar, and Internet Explorer—it does not affect the contents of the History bar.

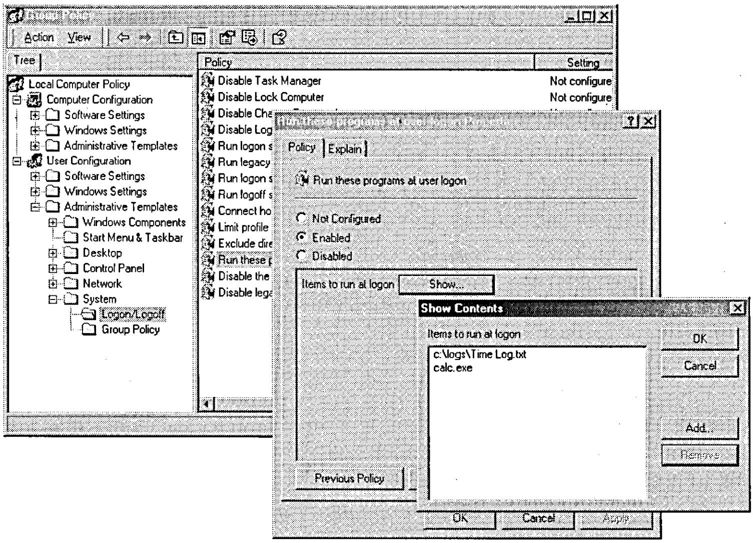
You should be aware, however, that it is possible for someone with administrative privileges for your computer to run a background process on your system that can monitor every keystroke and mouse click you make. Make it invisible to Windows 2000 Task Manager, so the target user has no way to know that he or she is being watched. It is also possible for an administrator to take ownership of your NTFS files and even—with a bit of effort—to decrypt them. All of Windows 2000's security features notwithstanding, a user with administrative privileges for your system is potentially omniscient! *For more about the NTFS file system and file encryption, see Chapter 32, "Using the NTFS File System," and Chapter 33, "Using Encryption."*

Controlling Programs and Services that Start at Logon

After Windows 2000 starts, it can automatically launch any number of programs and services. You can find—and add or delete, if desired—the programs that start in any of the following places:

- **Startup folder on the Start menu (current user).** To remove any of these programs, you can edit the Start menu directly, or you can use Windows Explorer to navigate to %UserProfile%\Start Menu\Programs\Startup.
- **Startup folder on the Start menu (all users).** Unlike the situation in Windows NT, the content of the Start menu for all users is merged with the one for a particular user, so it's not possible to tell by looking at the Start menu which profile a particular entry belongs to. You can modify these entries in Windows Explorer by navigating to %AllUsersProfile%\Start Menu\Programs\Startup.
- **Run key in the registry (current user).** The HKCU\Software\Microsoft \Windows\CurrentVersion\Run key contains a value for each program to be run whenever you log on. The name of each REG_SZ value in the Run key represents the "friendly" name of the program, and the data specifies the name of the executable and any command-line options.
- **Run key in the registry (all users).** The HKLM\Software\Microsoft \Windows\CurrentVersion\Run key contains a value for each program to be run whenever anyone logs on. The format of the values is the same as for the comparable HKCU key.

- **RunOnce key (all users).** The HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce key contains the names of programs that will run at startup the next time anyone logs on. When the programs run, their values are automatically deleted from the RunOnce key so that they don't run again. The format of the values is the same as for the Run key.
- **RunOnce key (current user).** The HKCU\ Software\Microsoft\Windows\CurrentVersion\RunOnce key is structured just like its counterpart under HKLM, and it works the same way except that it affects only the current user.
- **Your Scheduled Tasks folder.** You can use Scheduled Tasks to specify per-user startup tasks (as well as tasks that occur on other kinds of schedules).
- **An administrator's Scheduled Tasks folder.** A user who has administrative privileges for your computer can use Scheduled Tasks to set up a startup task for your user account. By default, that task will not be listed in your own Scheduled Tasks folder.
- **Another user's Scheduled Tasks folder.** Strange as it might seem, users who do not have administrative privileges for your computer can still schedule tasks that will run when you log on. Such tasks run as background processes only.
- **Group Policy.** Group Policy contains two policies (both called Run These Programs At User Logon) that contain a list of programs to be run whenever anyone logs on. You can find these lists in the Group Policy console (Gpedit.msc) by navigating to Computer Configuration\Administrative Templates\System or User Configuration\Administrative Templates\System\Logon/Logoff. To review or edit either list, select Enabled and click Show. See Figure 8-1.



Run these programs at user logon

○ Not Configured
● Enabled
○ Disabled

Items to run at logon Show...

Items to run at logon

c:\logs\Time Log.txt
calc.exe

Figure 8-1
You can use Group Policy to specify the names of programs or documents that should be run. You must include the path if the file is not stored in %SystemRoot%.

A program that launches at startup can be located in any of these places. If you're trying to determine why a particular program starts, you'll need to check each place until you find it. Note that the Scheduled Tasks folder displays only those tasks that your own user account has established. If an administrator uses Scheduled Tasks to create a startup task for your account, you will not see that task listed in your own Scheduled Tasks folder.

If you want to add a program to the startup routine, the place where you choose to add it depends on whether you want the program to run only when you log on or when anyone logs on; how familiar you are with registry editing; whether you're concerned about hiding menu items from users; and whether you're concerned about forcing users to run certain programs. As with so many tasks in Windows, you'll find many ways to achieve the same result.

Note You're probably familiar with the trick of holding down a Shift key while Windows starts (that is, beginning when you press Enter or click OK in the Log On To Windows dialog box) to prevent startup programs from running. That trick works in Windows 2000, but it affects only the programs in the Startup folders. Programs in the registry's Run keys run regardless.

To review and change the services that start during startup, you can use the Services console. *For more information, see Chapter 20, "Managing Services."*

Scheduling Tasks

Windows 2000 includes a flexible, easy-to-use scheduling tool that allows you to automate chores that need to be performed at regular intervals. To set up a scheduled task on your own system, choose Start | Settings | Control Panel | Scheduled Tasks | Add Scheduled Task. If you have appropriate privileges, you can schedule tasks for a remote system by opening that system's ADMIN$ share and navigating to its %SystemRoot%\Tasks folder.

The Scheduled Tasks Wizard that appears when you choose Add Scheduled Task is mostly, but not entirely, self-evident. Here are some points to note:

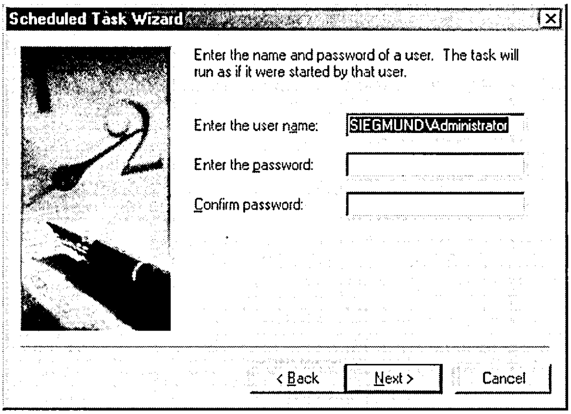
- You can schedule any application, script, batch file, shortcut, or linked document—anything that you could execute on a command line. You can also specify command-line arguments, but doing so requires a visit to the task's properties dialog box after you have created the task.
- If you schedule a task to run "when my computer starts," that task will run as a noninteractive process when the computer starts and will continue to run, regardless of who is logged on, until the system is shut down or you terminate

the task. (Because you are the task's owner, only you can terminate it. To terminate a noninteractive process, press Ctrl+Alt+Delete, choose Task Manager, click the Processes tab, select the process, and then click End Process.)

- If you schedule a task to run "when I log on," the task will actually run when *anyone* logs on. If you log on, the task runs interactively (provided, of course, that it was designed to run that way). If someone else logs on, the task runs as a noninteractive process. Note the following peculiarity: if you set up a logon task for your own use, expecting it to run interactively, and someone else logs on before you, that task will run noninteractively when you log on. Windows 2000 leaves the task running when the other user logs off (because you own it) and declines to start a second, interactive, instance when you log on.
- The screen shown in Figure 8-2 prompts you for a user account name and a password. If you're logged on as a member of the Administrators group, you can specify a user account and password other than your own here, thereby creating an interactive task for another user. Even if you're merely scheduling a task for your own account, however, you must supply your account name and password (the latter twice) in this dialog box—notwithstanding the fact that you've already given your password at logon.
- If you schedule a recurring task or one that will run at some distant point in the future, be aware that the password you specify must be valid at the time the task runs. If you change your password periodically, or if you set up a task for a user account that changes its password periodically, you might need to reenter the password down the line. You can do that by right-clicking the task in the Scheduled Tasks folder and choosing Properties from the shortcut menu.
- The wizard's last page includes a check box that gives you the opportunity to open the new task's Advanced Properties dialog box when you click Finish. This dialog box provides some important additional scheduling options, but you can always come back to it later by right-clicking the task in the Scheduled Tasks folder and choosing Properties from the shortcut menu.

A Note About Security

The behavior of the Windows 2000 Scheduled Tasks facility points up a fact that you should always keep in mind when working on a network or sharing your own machine with other user accounts: it's possible for someone else to start a process that runs invisibly while you're logged on to your own account. Even though a process started by someone else is limited by the privileges available to that other user, it's possible for such a process to monitor your activities. If you work with data you don't want others to see, keep that data on an NTFS volume and use NTFS file security to restrict others' access.



Enter the name and password of a user. The task will run as if it were started by that user.

Enter the user name: SIEGMUND\Administrator

Enter the password:

Confirm password:

Figure 8-2
If you're an administrator, you can use this screen to schedule interactive tasks for other accounts.

Working with Scheduled Task Objects

A scheduled task becomes a task object (a .job file). In the Scheduled Tasks folder, such an object is denoted by an icon with a little clock in its lower left corner. You can copy and move task objects, as you can any other kind of file objects. So, for example, you can copy a task object to another system or even e-mail one to another user. Outside someone's Scheduled Tasks folder, you can modify the object's properties (including its schedule), but the task will not run unless the object is returned to a Scheduled Tasks folder.

Be aware that the user credentials associated with a task object do not travel with the object. If you relocate a task object to another system, you will need to reenter the user credentials (account name and password) on that system.

Monitoring Scheduled Tasks

You can get useful information about the status of a scheduled task by displaying the Scheduled Tasks folder in Details view. Among other things, you can learn when the task last ran (or was scheduled to run), when it's scheduled to run again, and who created the task.

If a task fails to run, Details view will tell you so but won't tell you why. To get diagnostic information, choose View Log from the Scheduled Tasks folder's Advanced menu. The log appears as a plain-text file in Notepad.

Tasks that fail to run because the computer is off at the appointed hour, or because the computer is on battery power and you've stipulated that the task shouldn't run in that condition, are recorded as missed tasks. You can get notification of missed tasks by choosing Notify Me Of Missed Tasks from the Scheduled Tasks folder's

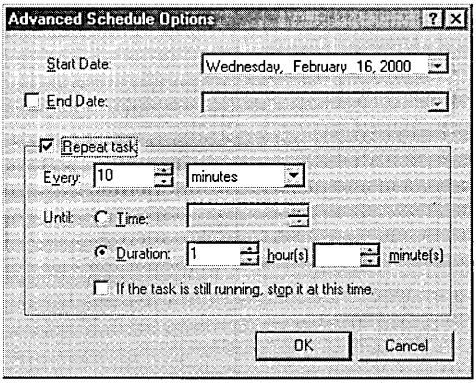
Advanced menu. If you miss a task because your computer is off, a message to that effect appears at your next logon.

Advanced Scheduling Options

Visiting the properties dialog box for a task lets you modify the task's schedule, change the password or user name associated with the task, add command-line arguments for the task, or even change the application that is scheduled to run. The properties dialog box also provides some useful advanced scheduling options.

The Show Multiple Schedules check box, on the Schedule tab, lets you assign more than one schedule to the same task. You could, for example, arrange to have your task run every Friday at 5 P.M. and also at 5 P.M. on the 30th day of every month. When you select this check box, a New button appears. Click New to enter a second or subsequent schedule.

Figure 8-3 shows the dialog box that is displayed when you click Advanced on the Schedule tab. Here you can specify an end date for a recurrent task or specify a repeat interval for a recurrent task. If you select Repeat Task, you can use the Time or Duration option to tell the system when to quit repeating. To repeat every two hours until 11 P.M., for example, you could select Repeat Task, set the Every fields to 2 and Hours, select Time, and specify 11 P.M. To run at 30-minute intervals for four hours, you could set the Every fields to 30 and Minutes, select Duration, and then specify 4 hours and 0 minutes.



Advanced Schedule Options

Start Date: Wednesday, February 16, 2000

☐ End Date:

☑ Repeat task

Every: 10 minutes

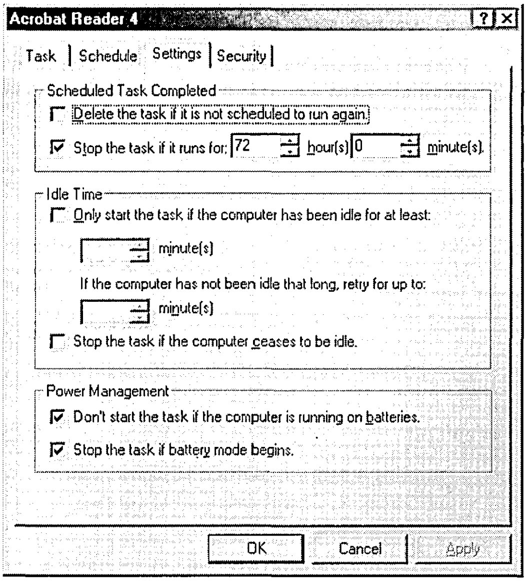
Until: ○ Time:

● Duration: 1 hour(s) minute(s)

☐ If the task is still running, stop it at this time.

Figure 8-3
Click Advanced on the Schedule tab to produce this dialog box, where you can set up end dates and recurrence parameters.

On the Settings tab, shown in Figure 8-4, you can provide a termination order for a task that has run too long, stipulate that a task not run if the computer is in use at the scheduled time (or stop running if someone begins using the computer), and tell the system not to run a task if the computer is running on battery power. You can also select a check box that will remove the task object from the Scheduled Tasks folder if, on the current schedule, it's never going to run again.


Acrobat Reader 4

Task | Schedule | Settings | Security

Scheduled Task Completed

□ Delete the task if it is not scheduled to run again.

☑ Stop the task if it runs for: 72 hour(s) 0 minute(s).

Idle Time

□ Only start the task if the computer has been idle for at least:

minute(s)

If the computer has not been idle that long, retry for up to:

minute(s)

□ Stop the task if the computer ceases to be idle.

Power Management

☑ Don't start the task if the computer is running on batteries.

☑ Stop the task if battery mode begins.

OK | Cancel | Apply

Figure 8-4
The Settings tab of a task's properties dialog box provides power-management control and other useful options.

On the Security tab, you can control who's allowed to do what with your scheduled tasks. Task objects use standard NTFS file-system security descriptors: Full Control, Modify, Read & Execute, Read, and Write. Note that the security descriptors that appear in the task object's properties dialog box apply only to the task object. The programs and documents specified by the task object have their own separate security descriptors. You can use Windows Explorer to modify those. *For information about using NTFS security descriptors, see "Securing Folders and Files," page 544.*

Scheduling Tasks with the At Command

The Scheduled Tasks facility is a friendly and versatile extension of the At command that was included with previous versions of the Windows NT platform. You can continue to enter At commands at the command prompt or in batch files; tasks that you set up this way appear in the Scheduled Tasks folder, identified as At*n*, where *n* is a task ID supplied by the system. If you edit an At task in Scheduled Tasks, however, the task is upgraded to a "normal" scheduled task. At that point, you can no longer delete the task from the command prompt, and you must supply user credentials (account name and password) before the task can run.

The At command has two alternative syntaxes:

```
at [\\computername] time [/interactive] [/every:date[,...] | /next:date[,...]]
    "command"
```

and

```
at [\\computername] [id] [/delete] | /delete [/yes]]
```

Use the first to create a task or the second to delete a task you've already created. When you create a task, the system responds with the task number. You can use that number as the ID argument to delete the task.

Note that At tasks run as background tasks by default; to run an interactive application, use the /interactive switch.

Here are some examples of using the At command. For instance,

```
at 15:45 "myapp.exe"
```

runs Myapp as a background task on the local computer, at 3:45 P.M., either on the current day or the next day (if it's already past 3:45 P.M.).

You could use this command to run Yourapp interactively on the local computer at 8:00 A.M. next Tuesday:

```
at 8:00 /interactive /next:tuesday "yourapp.exe"
```

To run Thisapp in the background on Fafner at 5:00 P.M. every Monday, Wednesday, and Friday, use the following:

```
at \\fafner 17:00 /every:monday,wednesday,friday "thisapp.exe"
```

Enter the command

```
at 1234 /delete /yes
```

to delete At task number 1234 without requiring user confirmation. (Omitting /yes would generate a confirmation prompt.)

Tasks scheduled via the At command run under the System account by default. To make them run under a different user account, choose AT Service Account from the Advanced menu in the Scheduled Tasks folder. Then supply an account name and password. You must be logged on as a member of the Administrators group to do this.

Running a Program Under a Different User Account

There may be times when a program you want to run is not accessible to the account under which you're currently logged on. If your program is accessible to another account and you're able to log on to that account, you could log off the current account, log back on to the other account, and then run the program. But Windows 2000 offers a simpler solution: the Run As command.

The Run As command is particularly valuable for administrators who want to do their nonadministrative work on nonadministrative accounts. Microsoft strongly recommends that you avoid logging on as an administrator, because a system running with full administrative permissions is vulnerable to Trojan horses and other forms of mischief. To be safe, log on as a member of the Power Users group and use Run As to perform administrative chores.

To run a program under a different account, hold down the Shift key while you right-click the item or a shortcut to it (on the Start menu, for example) and then choose Run As from the shortcut menu. (MMC applications and Control Panel items—files with the extension .msc or .cpl—have Run As on their normal shortcut menus. But you can always make Run As appear by holding down Shift while you right-click.) In the dialog box that appears, specify a user account and password.

You can create a shortcut that always runs a program or opens a document via Run As. Simply create a normal shortcut and then open the shortcut's properties dialog box. On the Shortcut tab, select the Run As Different User check box.

Using RunAs at the Command Prompt

You can use the RunAs command in a Command Prompt window or in a batch file. The syntax is as follows:

```
runas [/profile][/env][/netonly] /user:useraccountname program
```

in which */profile* specifies the name of the user's profile, if it needs to be loaded; /Env stipulates that the current network environment rather than the user's local environment should be used; /Netonly indicates that the user information specified is for remote access only; and /User:*useraccountname* supplies the name of a user account, in the format *user@domain*.

Downloading Compatibility Updates

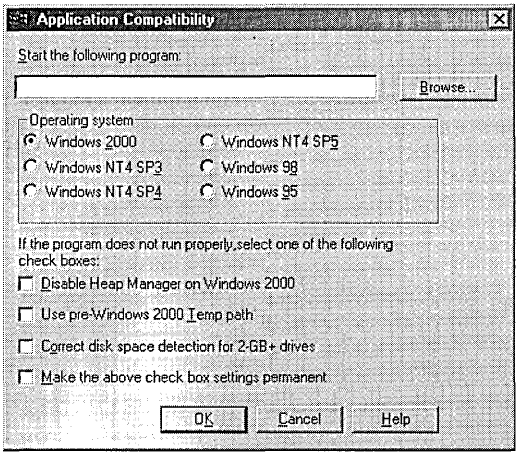
From time to time, Microsoft publishes updates to Windows 2000 that provide compatibility with additional applications. You can download these updates from the Windows Update site. Choose Start | Windows Update, or navigate to *windowsupdate.microsoft.com*. After you click Product Updates, you'll find the compatibility updates patch listed under Recommended Updates.

The first compatibility update appeared in February 2000, at the time the operating system itself was shipped. This update addressed minor issues affecting 48 game programs.

If a program you need doesn't run under Windows 2000, be sure to check this Web site to see whether a compatibility patch is available. If no patch is available, try using Apcompat, described next.

Using Apcompat to Solve Compatibility Problems

Apcompat, shown in Figure 8-5, is a tool designed to overcome certain compatibility issues that might prevent some older programs from running under Windows 2000. Apcompat works either by persuading an older application that it's about to run under an earlier version of Windows or by circumventing some aspect of Windows 2000 that might prevent the older program from running. The utility is one of several support tools included on your Windows 2000 Professional CD. To install it (and the other support tools), navigate to *d*:\Support\Tools (where *d* is your CD-ROM drive) and run Setup. You must run it with an administrative account. If you're not logged on as a member of the Administrators group, right-click Setup, choose RunAs, and provide the name and password of an administrative account.



Application Compatibility

Start the following program:

Operating system

● Windows 2000 ○ Windows NT4 SP5
○ Windows NT4 SP3 ○ Windows 98
○ Windows NT4 SP4 ○ Windows 95

If the program does not run properly,select one of the following check boxes:

□ Disable Heap Manager on Windows 2000
□ Use pre-Windows 2000 Temp path
□ Correct disk space detection for 2-GB+ drives
□ Make the above check box settings permanent

Figure 8-5
Apcompat can solve some compatibility problems by convincing older applications that they're not really running under Windows 2000.

On the line at the top of the dialog box, name the program you're trying to run—or click Browse and find it. In the Operating System section, try selecting the earlier operating system under which the program ran successfully. If that doesn't solve the problem, one of the following options might:

- **Disable Heap Manager On Windows 2000.** Some older programs use memory in ways that conflict with Windows 2000. Disabling the Windows 2000 heap manager might enable the older program to run, although it will use memory less efficiently.
- **Use Pre-Windows 2000 Temp Path.** If the path specified by the Windows 2000 %Temp% or %Tmp% variable exceeds a length limit imposed by the older application, selecting this check box might solve the problem. The program will then use \Temp as its temporary file folder.
- **Correct Disk Space Detection For 2-GB+ Drives.** Some older applications do not use the same data type as Windows 2000 for determining the amount of free space available on hard disks. If your program reports inadequate disk space (when enough space is actually available), try selecting this check box.

If you get your program running successfully with Apcompat, return to this dialog box and select Make The Above Check Box Settings Permanent. Thereafter, you'll be able to run your program without going through Apcompat.

Chapter 9

Installing and Removing Programs and System Components

In This Chapter

The Benefits of the Windows Installer 145

Windows File Protection 147

Using Add/Remove Programs 147

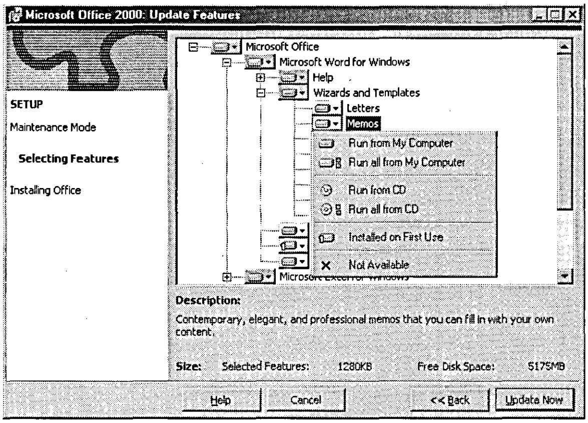
Installing Programs Under a Different User Account 151

Creating MSI Files for Legacy Applications 151

The process of installing and removing programs and system components is both simpler and safer in Microsoft Windows 2000 than in any previous version of the operating system. Three factors account for these improvements: the Windows Installer, Windows file protection, and the improved functionality of Add/Remove Programs in Control Panel.

The Benefits of the Windows Installer

If you've installed Microsoft Office 2000 or the Windows 2000 Support Tools that come with Windows 2000 Professional, you've already encountered the Windows Installer. (If you haven't installed the Support Tools, run \Support\Tools\Setup on your Windows 2000 Professional distribution media.) One component of the Windows Installer is the new Setup application shown in Figure 9-1. This Setup application lets you specify which program features you want installed on your hard disk, which you want installed at first use (installed "on demand"), which you want to run from the CD, and which you never want to be bothered with. New versions of major applications from Microsoft will all use this Setup tool, as will many future third-party programs.



Description:
Contemporary, elegant, and professional memos that you can fill in with your own content.

Size: Selected Features: 1280KB Free Disk Space: 5175MB

Figure 9-1
With the new Windows Installer Setup tool, you can stipulate that program features be installed "on demand."

Another aspect of the Windows Installer makes applications that use it "self-repairing." The Installer maintains a record of all DLLs and other critical components used by an application. If a required DLL becomes damaged, is overwritten by an unauthorized alternative version, or is deleted, the Installer detects the change and repairs the component when you try to run the application—prompting you for installation media if necessary.

A third aspect of the Installer assists administrators in Active Directory environments in deploying applications and maintaining corporate use policies. Using the Group Policy console on a server version of Windows 2000, an administrator can *publish* or *assign* applications to users or computers.

An application published to a user is made available to that user via Add/Remove Programs in Control Panel. If the administrator chooses an auto-install option, documents associated with the published application are recorded in the registry in advance; then, if the user opens an associated document, the published software is automatically installed from the network server.

An application assigned to a user appears on the user's Start menu or as a shortcut on the user's desktop, and the application's documents are pre-associated. As soon as the user chooses the menu item, activates the shortcut, or opens an associated document, the application is installed. An application assigned to a specific user is available to that user wherever he or she might log on. An application can also be assigned to a computer, in which case the application is automatically installed when anyone logs on to that computer. (And if someone uninstalls the assigned application, it is automatically reinstalled at the next logon.)

The Windows Installer is implemented as an operating-system service in Windows 2000 and is available via service pack for Windows 95, Windows 98, and Windows NT 4. To use the Windows Installer, an application must describe itself in an .msi file. On the .msi file's shortcut menu, you'll find Install, Repair, and Uninstall options. Thus you can use the shortcut menu to go directly to an aspect of the program's setup functionality, if you prefer not to use Control Panel's Add/Remove Programs.

The Windows Installer also has a command-line executable, Msiexec.exe. Msiexec's elaborate syntax is beyond the scope of this book. You can read about it by choosing Help from the Start menu, clicking the Search tab, and searching for *msiexec*.

Windows File Protection

As mentioned, one of the benefits of the Windows Installer is run-time resiliency—the ability to repair damaged applications on the fly. Windows file protection provides comparable resiliency to the operating system itself. Copies of critical DLLs are maintained in the super-hidden folder %SystemRoot%\System32\Dllcache. If any of these protected DLLs is deleted or changed by an unauthorized agent, a change notification event occurs. If the DLL was deleted, Windows 2000 supplies a fresh copy from the cache. If the DLL was overwritten, Windows 2000 checks to see whether the new copy has a valid digital signature. If it doesn't, the new copy is overwritten from the cache.

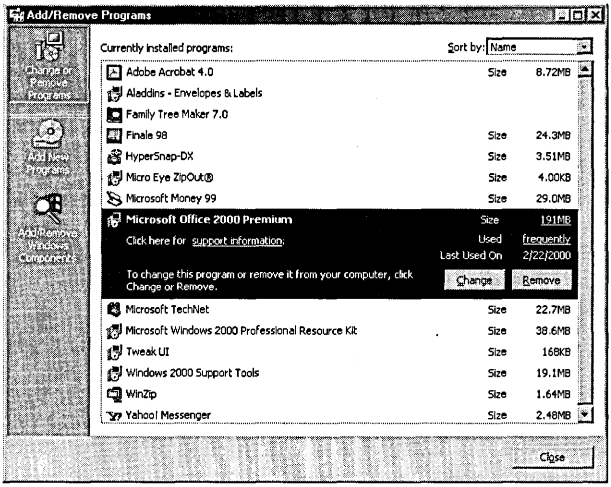
Windows file protection prevents applications (including Microsoft's) from changing system DLLs. Only service packs and new versions of the operating system can change critical files.

The System File Checker application (Sfc.exe) that was included with Windows 98 is still present (for compatibility purposes) in Windows 2000, but you don't need to use it, because the operating system looks after the health of your system files automatically. Nevertheless, if you're curious—or mistrustful of the system's automatic checking—you can run System File Checker by typing *sfc* in a Command Prompt window. Sfc will respond with a list of available command-line arguments.

Using Add/Remove Programs

Control Panel's Add/Remove Programs was once widely regarded as a tool for novices. Many expert users didn't bother with it, preferring to execute Setup or Uninstall programs directly from CDs or other media. But Add/Remove Programs is so improved that you might want to consider creating a shortcut to it on your Quick Launch toolbar. Figure 9-2 shows the refurbished Add/Remove Programs.

As the button bar on the left makes clear, Add/Remove Programs divides its functionality into a maintenance section (Change Or Remove Programs) and an installation section (Add New Programs), with a third section devoted to the installation and removal of Windows components. This arrangement is not quite as logical as it might first appear, because, as you'll see, the installation section includes a link to the Windows Update Web site, which is an important maintenance resource.



Currently installed programs:

Sort by: Name

Adobe Acrobat 4.0	Size	8.72MB
Aladdins - Envelopes & Labels		
Family Tree Maker 7.0		
Finale 98	Size	24.3MB
HyperSnap-DX	Size	3.51MB
Micro Eye ZipOut®	Size	4.00KB
Microsoft Money 99	Size	29.0MB
Microsoft Office 2000 Premium	Size	191MB
Click here for support information:	Used	frequently
	Last Used On	2/22/2000
To change this program or remove it from your computer, click Change or Remove.		
Microsoft TechNet	Size	22.7MB
Microsoft Windows 2000 Professional Resource Kit	Size	38.6MB
Tweak UI	Size	168KB
Windows 2000 Support Tools	Size	19.1MB
WinZip	Size	1.64MB
Yahoo! Messenger	Size	2.48MB

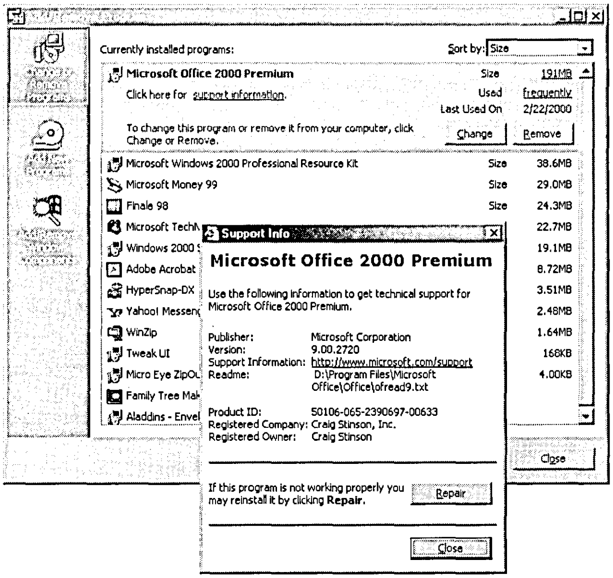
Figure 9-2
Add/Remove Programs is considerably more useful now than it was in earlier versions.

Changing or Removing Programs

Figure 9-2 shows the Change Or Remove Programs section, with installed programs sorted by name. The displayed list provides information about disk space and usage for the selected program. Usage is characterized as "frequently," "occasionally," or "rarely" and reflects your activity over the most recent 30 days. For example, if you use a program every day, but you've been on safari the last two months, Add/Remove Programs reports your use of that program as "rarely" until you reestablish your normal work habits.

Below the usage characterization, you'll find the date on which you last opened the selected program. If you want to uninstall the programs you use least, you might find this data point more relevant than the usage category. You can use the Sort By list in the upper right corner to sort your programs by date of most recent use (with the oldest date at the top). Alternatively, if you want to unload the item that's consuming most of your disk space, you can sort by size, with hogs on top and piglets below.

In addition to Change and Remove buttons, some applications display a Support Information link when you select them. When you click this link, you might see an additional link to the vendor's Web site and the name and location of a readme file. Some Microsoft applications also display a Repair button when you click the support link. (See Figure 9-3.) The Repair button allows you to reinstall an application that has stopped working correctly (although the Windows Installer's run-time resiliency makes that less likely).



Currently installed programs:

Sort by: Size

Microsoft Office 2000 Premium	Size	191MB
Click here for support information.	Used	frequently
	Last Used On	2/22/2000

To change this program or remove it from your computer, click Change or Remove.

Microsoft Windows 2000 Professional Resource Kit	Size	38.6MB
Microsoft Money 99	Size	29.0MB
Finale 98	Size	24.3MB
Microsoft TechN		22.7MB
Windows 2000 S		19.1MB
Adobe Acrobat		8.72MB
HyperSnap-DX		3.51MB
Yahoo! Messeng		2.48MB
WinZip		1.64MB
Tweak UI		168KB
Micro Eye ZipOu		4.00KB
Family Tree Mak		
Aladdins - Envel		

Support Info

Microsoft Office 2000 Premium

Use the following information to get technical support for Microsoft Office 2000 Premium.

Publisher:	Microsoft Corporation
Version:	9.00.2720
Support Information:	http://www.microsoft.com/support
Readme:	D:\Program Files\Microsoft Office\Office\ofread9.txt
Product ID:	50106-065-2390697-00633
Registered Company:	Craig Stinson, Inc.
Registered Owner:	Craig Stinson

If this program is not working properly you may reinstall it by clicking **Repair.**

Figure 9-3
Clicking Support Information provides a Web link, directions to a readme file, and a Repair button that the Windows Installer promises you'll never need.

Installing New Programs

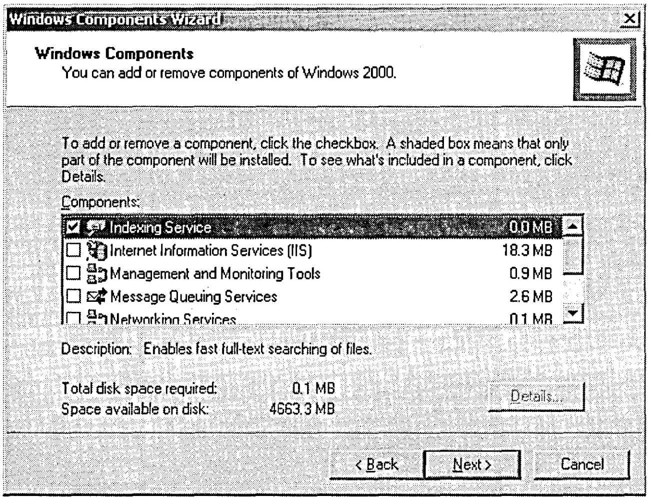
When you click Add New Programs in the button bar, Add/Remove Programs displays two or three additional buttons, depending on your circumstances. The first of these lets you install a program from local media—CD or floppy. The second takes you to the Windows Update site. The third, if present, displays a list of applications published by your network administrator.

The options for installing from local or network media are self-explanatory. *For information about the Windows Update option, which relates to system maintenance, see "Using Windows Update to Maintain Driver and System Files," page 676.*

Adding and Removing Windows Components

Clicking Add/Remove Windows Components on the button bar lets you install pieces of Windows that you neglected to install earlier or unload ones that you don't need. You need to be logged on as a member of the Administrators group to use this part of Add/Remove Programs.

If you've used earlier versions of Windows, you'll almost certainly notice on your first visit to Add/Remove Windows Components that the list of items that can be installed and/or uninstalled (shown in Figure 9-4) is considerably shorter than it used to be. For reasons quite unclear, Microsoft has made it difficult to uninstall the accessory programs, games, and multimedia clips that come with Windows. Fortunately, there's a way around the difficulty.



Windows Components
You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Indexing Service	0.0 MB
□	Internet Information Services (IIS)	18.3 MB
□	Management and Monitoring Tools	0.9 MB
□	Message Queuing Services	2.6 MB
□	Networking Services	0.1 MB

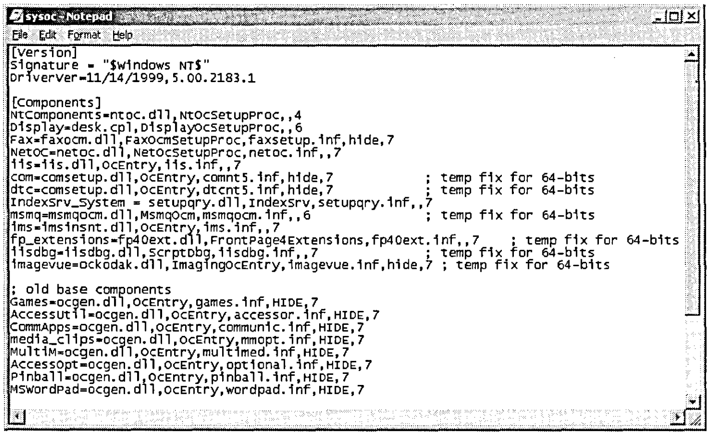
Description: Enables fast full-text searching of files.

Total disk space required: 0.1 MB
Space available on disk: 4663.3 MB

Figure 9-4
The initial list of removable Windows components no longer includes accessories or games, although you can remedy that difficulty.

To add items to the list of removable Windows components:

1. Make a backup copy of the hidden file %SystemRoot%\Inf\Sysoc.inf.
2. Open the original copy of the file for editing in Notepad or WordPad, as shown here.



```
[Version]
Signature = "$Windows NT$"
DriverVer=11/14/1999,5.00.2183.1

[Components]
NtComponents=ntoc.dll,NtOcSetupProc,,4
Display=desk.cpl,DisplayOcSetupProc,,6
Fax=faxocm.dll,FaxOcmSetupProc,faxsetup.inf,hide,7
NetOC=netoc.dll,NetOcSetupProc,netoc.inf,,7
iis=iis.dll,OcEntry,iis.inf,,7
com=comsetup.dll,OcEntry,comnt5.inf,hide,7            ; temp fix for 64-bits
dtc=comsetup.dll,OcEntry,dtcnt5.inf,hide,7            ; temp fix for 64-bits
IndexSrv_System = setupqry.dll,IndexSrv,setupqry.inf,,7
msmq=msmqocm.dll,MsmqOcm,msmqocm.inf,,6               ; temp fix for 64-bits
ims=imsinsnt.dll,OcEntry,ims.inf,,7
fp_extensions=fp40ext.dll,FrontPage4Extensions,fp40ext.inf,,7    ; temp fix for 64-bits
iisdbg=iisdbg.dll,ScrptDbg,iisdbg.inf,,7              ; temp fix for 64-bits
imagevue=ockodak.dll,ImagingOcEntry,imagevue.inf,hide,7 ; temp fix for 64-bits

; old base components
Games=ocgen.dll,OcEntry,games.inf,HIDE,7
AccessUtil=ocgen.dll,OcEntry,accessor.inf,HIDE,7
CommApps=ocgen.dll,OcEntry,communic.inf,HIDE,7
media_clips=ocgen.dll,OcEntry,mmopt.inf,HIDE,7
MultiM=ocgen.dll,OcEntry,multimed.inf,HIDE,7
AccessOpt=ocgen.dll,OcEntry,optional.inf,HIDE,7
Pinball=ocgen.dll,OcEntry,pinball.inf,HIDE,7
MSWordPad=ocgen.dll,OcEntry,wordpad.inf,HIDE,7
```

3. Remove the word *HIDE* from each line below the "_;_old base components" comment. (For each item you edit, be sure to remove both the word *HIDE* and the comma that follows it.)
4. Save the file and reopen Add/Remove Programs. The edited items now appear on the list.
5. If anything goes awry (though it won't, unless you've made a mistake in your editing), restore your backup of Sysoc.inf.

Installing Programs Under a Different User Account

If installing the application you need requires administrative privileges and you're not currently logged on as an administrator, the simplest approach is to skip Add/Remove Programs and go straight to the application's Setup.exe, using RunAs:

1. Hold down the Shift key while you right-click Setup.exe.
2. Choose RunAs from the shortcut menu, and supply the necessary credentials.

For more information about the RunAs command, see "Running a Program Under a Different User Account," page 142.

Creating MSI Files for Legacy Applications

As mentioned at the beginning of this chapter, applications must describe their setup functionality in an .msi file to take advantage of the Windows Installer. On the Windows 2000 Professional CD, in the folder \Valueadd\3rdParty\Mgmt\Winstle, you'll find a product called WinINSTALL LE, which you can use to create .msi files for legacy applications. If you're an administrator who needs to create consistent and robust setup procedures for all your applications, you might find WinINSTALL LE invaluable. WinINSTALL LE (the LE stands for Limited Edition) is supplied by Veritas Software and is based on the same vendor's WinINSTALL product. You can read about both WinINSTALL and WinINSTALL LE at *www.veritas.com/products/wile.*

To install WinINSTALL LE, right-click the file Swiadmle.msi in your Windows 2000 CD's Winstle folder, and choose Install. WinINSTALL LE consists of two components: a Discover program and a Software Console program. You use the first to create an .msi file and the second to edit or customize one. You'll find shortcuts for both programs under Start | Programs | VERITAS Software. You should read the extensive Help files that come with each of these components before diving in to create your first .msi file.

Chapter 10

Using Programs Written for Other Operating Systems

In This Chapter

Running Windows 3.x–Based Programs 154
Running MS-DOS-Based Applications 157
Running POSIX-Based Applications 169

With Microsoft Windows 2000, you can run programs written for certain other operating systems as easily as you can run programs written for Windows 2000. Because Windows 2000 runs these programs seamlessly, you generally don't need to know a program's origin or type to run it. Specifically, you can run applications written for:

- **Windows 9x.** Except for programs that can violate Windows 2000 security (by directly accessing the disk, for example), programs written for Windows 95 or Windows 98 work exactly the same in Windows 2000. Therefore, they are not discussed in any detail in this chapter.
- **Windows 3.x.** On the surface, programs written for Windows 3.x act much like Windows 2000–based programs, but you'll find a few differences under the hood. This chapter explains those differences.
- **MS-DOS.** You can run most MS-DOS-based programs inside windows that make them look and behave much like Windows-based applications. This chapter explains how to do that, and more, with MS-DOS-based programs.
- **OS/2.** In a tip of the hat to Microsoft's role in the development of early versions of OS/2, Windows 2000 runs 16-bit character-based programs written for OS/2 versions 1.x and 2.x.
- **POSIX.** Windows 2000 supports character-based POSIX applications, which are typically UNIX-based applications that are recompiled to the POSIX standard using Windows NT or Windows 2000.

In this chapter, we survey the ins and outs of running programs written for these other operating systems, with particular emphasis on the two most widely used classes: programs for Windows 3.x and programs for MS-DOS.

Running Windows 3.x–Based Programs

Because Windows 3.x is a 16-bit operating system and Windows 2000 is a 32-bit operating system, programs for the two systems are written and compiled differently. To bridge the gap, Windows 2000 includes a subsystem for running Windows 3.x–based applications. The environment presented by this Win16 subsystem to applications written for Windows 3.x is comparable to "enhanced mode" in Windows 3.x.

Although Windows 2000 allows you to run older Windows 3.x–based programs, using these 16-bit applications under Windows 2000 has some drawbacks:

- Most 16-bit programs do not support long file names. (Windows 2000 does provide long file name information to all applications that understand it, however, allowing these particular 16-bit applications to use the names.)
- In general, 16-bit applications do not run as fast as comparable 32-bit applications. The 16-bit programs are restricted to using a single thread, even on a multithreaded operating system such as Windows 2000. And calls made by a 16-bit application must be translated for the 32-bit operating system. This translation process, called *thunking*, adds to execution time.
- Some 16-bit applications require 16-bit device drivers, which are not supported in Windows 2000. Applications that directly access hardware must supply a Windows 2000 virtual device driver and a Windows 2000 32-bit device driver, or they won't run.
- DLLs written for 16-bit applications cannot be used by 32-bit applications, and vice versa. Because the setup program for most applications installs all the DLLs needed by the application, you won't be aware of this distinction most of the time. But if, for example, you have a macro written for Microsoft Word 6 (a 16-bit application) that accesses one or more DLLs, it won't work with Word 2000 (a 32-bit application).

How Can You Tell?

Because Windows 3.x–based applications run effortlessly under Windows 2000, it's sometimes difficult to know whether you're using a 16-bit or a 32-bit application. All programs that bear the "Designed for Windows 98" or "Designed for Windows 2000" logo on their packaging are supposed to be 32-bit. A better indicator, though, is to look at the application itself. In Windows Explorer, right-click a shortcut to the program in question and choose Properties. (If there's no shortcut, create one.) Click the Shortcut tab. If the Run In Separate Memory Space check box is available, the application is a 16-bit, Windows 3.x–based program.

Compatibility with Win.ini and System.ini

Windows 3.x uses two text files, Win.ini and System.ini, to store configuration information for Windows itself and for applications you run. In later versions of the operating system, this configuration information is stored in the registry (some programs use their own private .ini files, in addition to the registry), and Win.ini and System.ini are no longer required. Some Windows 3.x–based applications depend on the existence of those files, however, so Windows 2000 retains copies of Win.ini and System.ini. You'll find them in your %SystemRoot% folder. Don't delete them!

Avoiding Crashes

By default, Windows 2000 treats each running 16-bit application as a thread within Ntvdm.exe, a process that establishes a virtual DOS machine (an environment that mimics in every detail a 640-KB computer that has access to extended memory). After you've started one or more 16-bit applications, if you open Windows Task Manager (press Ctrl+Shift+Esc) and click the Processes tab, you'll find an entry there for Ntvdm.exe, with indented subentries for your 16-bit programs. (See Figure 10-1.) You'll also find a subentry for Wowexec.exe, the Windows 2000 16-bit subsystem.

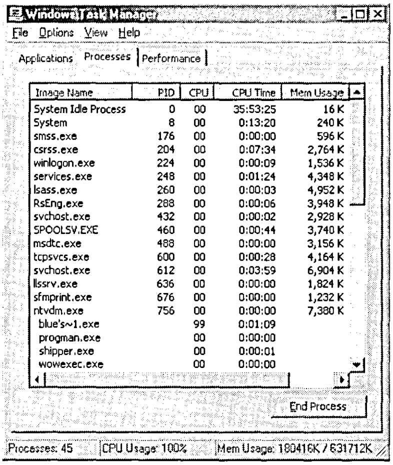


Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	00	35:53:25	16 K
System	8	00	0:13:20	240 K
smss.exe	176	00	0:00:00	596 K
csrss.exe	204	00	0:07:34	2,764 K
winlogon.exe	224	00	0:00:09	1,536 K
services.exe	248	00	0:01:24	4,348 K
lsass.exe	260	00	0:00:03	4,952 K
RsEng.exe	288	00	0:00:06	3,948 K
svchost.exe	432	00	0:00:02	2,928 K
SPOOLSV.EXE	460	00	0:00:44	3,740 K
msdtc.exe	488	00	0:00:00	3,156 K
tcpsvcs.exe	600	00	0:00:28	4,164 K
svchost.exe	612	00	0:03:59	6,904 K
llssrv.exe	636	00	0:00:00	1,824 K
sfmprint.exe	676	00	0:00:00	1,232 K
ntvdm.exe	756	00	0:00:00	7,380 K
blue's~1.exe		99	0:01:09	
progman.exe		00	0:00:00	
shipper.exe		00	0:00:01	
wowexec.exe		00	0:00:00	

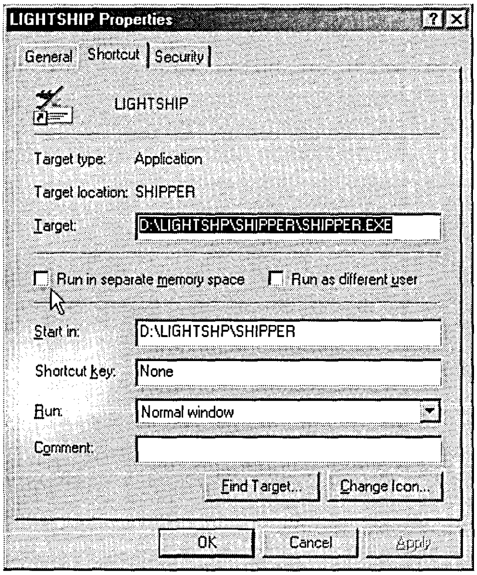
Processes: 45 | CPU Usage: 100% | Mem Usage: 180416K / 631712K

Figure 10-1
By default, each running 16-bit program appears as a subentry (a thread) under Ntvdm.exe.

In this default scheme of things, all 16-bit applications share a common memory space. Sharing memory is efficient and works fine for most 16-bit applications. However, if one Windows 3.x–based program in a shared memory space hangs or crashes, it's likely to bring down all the others with it—and you'll lose any unsaved information in all the applications.

If you have an application that occasionally hangs or crashes, you should run it in a separate memory space. To set up a Windows 3.x–based application to run in a separate memory space:

1. On the Start menu, right-click the application and choose Properties.
2. Click the Shortcut tab.
3. Select the Run In Separate Memory Space check box. (See Figure 10-2.)



Target type: Application
Target location: SHIPPER
Target: D:\LIGHTSHP\SHIPPER\SHIPPER.EXE
□ Run in separate memory space □ Run as different user
Start in: D:\LIGHTSHP\SHIPPER
Shortcut key: None
Run: Normal window
Comment:

Figure 10-2
Select Run In Separate Memory Space if your Windows 3.x–based program is prone to hanging or crashing.

If you launch your program from a shortcut outside the Start menu, make this change in that shortcut. If you launch it directly from its .exe file and don't have a shortcut, you need to create one. Select Run In Separate Memory Space, and then launch from the new shortcut.

Alternatively, you can start a 16-bit application in a separate memory space from the command prompt, using the syntax

```
start /separate filespec
```

From the Start menu's Run command line, the equivalent syntax would be

```
cmd /k start /separate filespec
```

In addition to preventing an application from disrupting others, running Windows 3.x–based programs in separate memory spaces confers other benefits:

- You get preemptive multitasking of Windows 3.x–based programs. When two or more programs share a virtual DOS machine, they multitask cooperatively (which means that programs are dependent on each other's good behavior for equitable time-sharing). When they run in separate spaces, they multitask preemptively, as native Windows 2000–based programs do.
- Applications in separate memory spaces are more responsive, because each application has its own input queue.
- You can run multiple instances of applications that normally do not allow you to do so.
- If you have an SMP (symmetric multiprocessor) computer, Windows 2000 can allocate processes in separate memory spaces among multiple processors.

The only apparent downside to running 16-bit applications in separate memory spaces is that this approach uses additional memory. If you have plenty of memory, you might consider running all your 16-bit programs in separate spaces.

Running MS-DOS-Based Applications

You can run any character-based program written for MS-DOS either in full-screen mode or in a window. (Graphics-based programs run only in full-screen mode.) If you run a program in full-screen mode, it looks exactly like it does when you run it under MS-DOS. If you run it in a window, it has a title bar, a Control menu, and all the other standard window paraphernalia.

One advantage of running in full-screen mode is that the program gets the maximum amount of screen real estate—the same amount of display space it would have if you were running it in MS-DOS. If you run the application in a window, you can maximize the window, but the presence of the window title bar means that you'll still have something less than the full screen to work with. A second advantage of full-screen mode is that it gives you faster video performance.

You might find that some programs' features work only in full-screen mode. For example, WordPerfect for DOS has a graphics display mode that provides a WYSIWYG view of your document. If you choose that view while WordPerfect is running in a window, the application is frozen until you switch to full-screen mode.

Provided your MS-DOS-based program is not one of the few that run only in full-screen display, and provided you have not disabled the Alt+Enter shortcut key, you can switch from full-screen display to windowed display by pressing Alt+Enter.

If you want to switch from full-screen to windowed display, but you've disabled the Alt+Enter shortcut key (because it's used for another purpose by your application), press Alt+Tab or Ctrl+Esc to switch to another program. Then right-click the taskbar button for the program you switched away from. Choose Properties from the shortcut menu, click the Options tab in the properties dialog box, and then select the Window option button.

Mouse Options

If your MS-DOS-based program supports a mouse, and you run the program in full-screen mode, the MS-DOS-based program "owns" the mouse. That is, you can choose commands, make selections, or do anything else with the mouse that you could do if you were running the program in MS-DOS.

If you run the program in a window, you have a choice about mouse ownership. You can let the MS-DOS-based program own the mouse as in full-screen mode, or you can let Windows own it. If the program owns the mouse, you need to use the Mark command on the Control menu to copy anything to the clipboard. If you let Windows own your mouse, you can use the mouse to select information and copy it to the clipboard, exactly as you can in a Windows-based program. But you won't be able to use the mouse for choosing commands in the MS-DOS-based program.

Whichever mouse mode you choose, you can use the mouse to change the window's size or position or to choose commands from the Control menu. In other words, the issue of who owns the mouse arises only when the mouse pointer lies within the client area of the program's window. On the borders or the title bar, Windows always retains control of the mouse.

Two settings control mouse ownership—and neither one is available through an application's properties dialog box (as they are in Windows 9x). The QuickEdit setting determines whether the mouse performs its usual program functions (such as selecting commands) or selects text for copying to the clipboard. The Hide Mouse Pointer command resolves a conflict that causes certain applications to display *two* mouse pointers—one for Windows and one for the application itself.

QuickEdit Mode

QuickEdit mode, when selected, causes Windows to take ownership of the mouse so that you can use it to easily select, copy, and paste text. Because it prevents the MS-DOS-based program from using the mouse for any other purpose, it's most useful in programs that don't use a mouse. To select QuickEdit mode:

1. Run your MS-DOS-based program.
2. Press Alt+Spacebar or click the program's Control menu icon to open the Control menu, and then choose Properties.
3. Click the Options tab.
4. Select QuickEdit Mode and click OK.
5. Select whether you want your change to affect only the current session or the current session and all future sessions of this program.

Hide Mouse Pointer Command

With most MS-DOS-based applications that support a mouse, the mouse functions the same way in both full-screen and windowed display mode. The only difference is the shape of the mouse pointer: in full-screen mode it's a rectangular block, and in a window it's an arrow.

However, some applications—WordPerfect for DOS is an example—display two mouse pointers when you run the application in a window. Moving the mouse moves the arrow-shaped Windows mouse pointer, but clicking and dragging has no effect on your application. Meanwhile, the application's block-shaped mouse pointer sits motionless, anxious but unable to help. The solution for such applications is to open the Control menu and choose Hide Mouse Pointer. When you do so, the Windows arrow pointer disappears, and the block pointer leaps around the window at your every mouse movement, enjoying its newfound freedom.

Freedom has its limits, of course, and you'll quickly find that your mouse pointer is constrained to its application window, unable to cross the window border to select another application—or even to open the active application's Control menu. When you're ready to escape this mousetrap, do one of the following:

- Press Alt+Tab to switch to another application.
- Press Ctrl+Esc to open the Start menu.
- Press Alt+Spacebar to open your application's Control menu, and then choose Display Mouse Pointer.
- Quit your application.

Using Copy and Paste

Windows 2000 provides basic copy-and-paste services for MS-DOS-based applications, just as it does for Windows-based programs. The procedures for copying and pasting are nearly the same in both kinds of applications.

Copying from an MS-DOS-Based Application

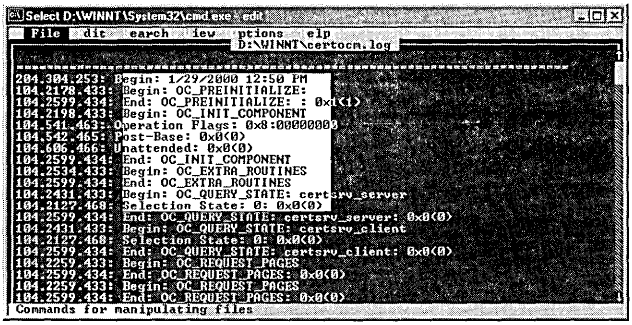
To copy a block of data from a windowed MS-DOS-based application:

1. Right-click the title bar, choose Edit from the Control menu, and then choose Mark on the submenu that appears.
2. Drag the mouse to select the data you want to copy.
3. Press Enter or right-click anywhere in the window.

Once you've copied your data to the clipboard, you can paste in the normal way.

If you've turned on the QuickEdit option for your MS-DOS-based application, you can omit step 1. How do you know whether the QuickEdit option is on? Simply drag with the mouse and see what happens. If QuickEdit is on, the word *Select* appears in the program's title bar as soon as you start dragging. If the word doesn't appear, you are not in QuickEdit mode, and you need to choose the Mark command before making your selection.

Note one important difference between selecting text in an MS-DOS-based application and selecting text in a Windows-based application: in an MS-DOS-based program, your selection is always rectangular, even if that means that lines of text are truncated on the left, the right, or both. Figure 10-3 shows an example of a text selection in an MS-DOS window. In contrast, when you select text in a Windows-based application, your selection follows the flow of your text, whether or not that produces a rectangular block.


Select D:\WINNT\System32\cmd.exe - edit
File
dit
earch
iew
ptions
elp
D:\WINNT\certocm.log
Commands for manipulating files

```
204.304.253: Begin: 1/29/2000 12:50 PM
104.2178.433: Begin: OC_PREINITIALIZE:
104.2599.434: End: OC_PREINITIALIZE: : 0x1(1)
104.2198.433: Begin: OC_INIT_COMPONENT
104.541.463: Operation Flags: 0x8:00000008
104.542.465: Post-Base: 0x0(0)
104.606.466: Unattended: 0x0(0)
104.2599.434: End: OC_INIT_COMPONENT
104.2534.433: Begin: OC_EXTRA_ROUTINES
104.2599.434: End: OC_EXTRA_ROUTINES
104.2431.433: Begin: OC_QUERY_STATE: certsrv_server
104.2127.468: Selection State: 0: 0x0(0)
104.2599.434: End: OC_QUERY_STATE: certsrv_server: 0x0(0)
104.2431.433: Begin: OC_QUERY_STATE: certsrv_client
104.2127.468: Selection State: 0: 0x0(0)
104.2599.434: End: OC_QUERY_STATE: certsrv_client: 0x0(0)
104.2259.433: Begin: OC_REQUEST_PAGES
104.2599.434: End: OC_REQUEST_PAGES: 0x0(0)
104.2259.433: Begin: OC_REQUEST_PAGES
104.2599.434: End: OC_REQUEST_PAGES: 0x0(0)
```

Figure 10-3
When you select text in an MS-DOS-based application, your selection is rectangular, even if that means that lines are truncated.

Selecting Text with the Keyboard

You can also select data in an MS-DOS-based application using the keyboard. Open the Control menu by pressing Alt+Spacebar. Press the E key to open the Edit submenu, and then press K to choose the Mark command. A rectangular cursor appears in the upper left corner of the application's window. This is your (unexpanded) selection. Use the Up, Down, Left, and Right Arrow keys to position this cursor in one corner of the area you want to select. Then hold down the Shift key while you use arrow keys to expand the selection. When you have made your selection, press Enter to copy it to the clipboard.

Pasting into an MS-DOS-Based Application

To paste data into an MS-DOS-based application, simply position the cursor where you want the pasted data to appear. Then open the Control menu, choose Edit, and choose Paste. If you have QuickEdit turned on, you can right-click anywhere in the window to paste at the cursor location.

Note that the Paste command in an MS-DOS-based application is always active, even if the clipboard is empty or contains data in a format that's not appropriate for your application. If you try to paste graphics data into a text-based application, you get an error message when you paste. A different error message appears if the clipboard is empty when you try to paste.

Also be aware that when you paste text into an MS-DOS-based application, Windows feeds characters to the application exactly as if you had typed them yourself at the keyboard. That is, the program itself cannot tell that the characters aren't coming directly from the keyboard. If you paste into a program that performs some kind of validation—for example, a spreadsheet that checks cell entries for correct formulation, or a program editor that verifies correct programming code—your paste might be interrupted by error messages from the application.

If you experience other kinds of problems with pasting into an MS-DOS-based program, try disabling the Fast Pasting option. With this option on (as it normally is), Windows feeds character data to your program as fast as it can. Most, but not all, programs can accept this fast transfer. If yours cannot, open the Misc tab of your program's properties dialog box and clear the Fast Pasting check box.

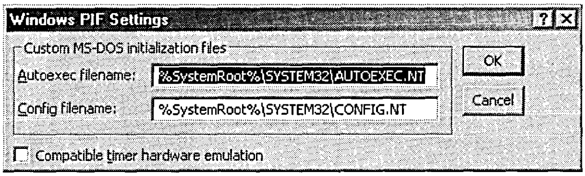
Setting the MS-DOS Configuration

The files Autoexec.nt and Config.nt set the configuration used by MS-DOS-based programs. These two files serve a purpose similar to that of Autoexec.bat and Config.sys in MS-DOS, but they also have important differences:

- Autoexec.bat and Config.sys must be located in the root directory of your boot drive. Autoexec.nt and Config.nt must be located in the %SystemRoot%\System32 folder.
- Autoexec.bat and Config.sys are the only configuration files needed or available under MS-DOS. In Windows 2000, Autoexec.nt and Config.nt are the default configuration files, but you also have the option of specifying different files with settings tailored for the application you're planning to run. In other words, you can have default Config.nt and Autoexec.nt files that are applied to all your normal MS-DOS-based programs and different versions for certain programs with special requirements.

Don't confuse MS-DOS configuration files with command prompt initialization or logon initialization files. Autoexec.nt and Config.nt affect only MS-DOS-based programs. The command interpreter, Cmd.exe, is a Windows 2000–based program and is not affected by anything in these configuration files.

To specify custom Config and Autoexec files to be used by a particular application, click the Advanced button on the Program tab of the application's properties dialog box. In the resulting dialog box, like the one shown here, you can specify the custom files.



Windows PIF Settings

Custom MS-DOS initialization files

Autoexec filename: %SystemRoot%\SYSTEM32\AUTOEXEC.NT

Config filename: %SystemRoot%\SYSTEM32\CONFIG.NT

□ Compatible timer hardware emulation

Note that this dialog box includes a Compatible Timer Hardware Emulation check box. This option imposes a performance penalty, so you should select it only if your application won't run with the box cleared.

If you create custom Config and Autoexec files, you should base them on the default Config.nt and Autoexec.nt files. That way, you'll be sure to include the basic information required to configure an MS-DOS session.

Using Config

In MS-DOS, the Config.sys file contains commands to load device drivers and set configuration parameters. In order to be compatible with all versions of MS-DOS, Windows 2000 does not validate commands in Config.nt. It executes the commands that it recognizes in Config.nt and ignores anything it doesn't understand.

You probably won't need to modify Config.nt unless you acquire new programs for MS-DOS. If the manual for your MS-DOS-based program recommends a particular setting for Config.sys, put it in Config.nt. The setting might not be used by Windows 2000, but usually it won't do any harm.

Device drivers are the exception. If your Config.sys loads a device driver with a Device= or DeviceHigh= statement, you might not be able to load the same driver in Config.nt. Table 10-1 suggests how you should handle device drivers commonly used with MS-DOS.

You can usually experiment safely with Config.nt settings. Windows 2000 protects the rest of the operating system from your MS-DOS-based programs, so failures won't harm the system. Naturally, you don't want to do much experimenting with valuable data in your MS-DOS-based programs, but usually the questionable device drivers you test will fail when loading—before the program even starts.

To see output from device drivers in Config.nt and from programs in Autoexec.nt, put the EchoConfig statement at the start of Config.nt. Use the Rem statement to add comments or to comment out statements during testing. Comment out the EchoConfig statement when you finish testing.

Table 10-1. MS-DOS Device Drivers

Device Driver	Comments
Himem.sys	Use the Windows 2000 version if you have programs that require it or if you use it in MS-DOS. Windows 2000 installs this in Config.nt by default.
Ansi.sys	Use the Windows 2000 version if you have MS-DOS-based programs that require it. The Windows 2000 command interpreter is not an MS-DOS-based program and does not recognize ANSI escape sequences. Therefore, you can't use them with the Prompt or Echo commands.
Country.sys and Setver.exe	Use the Windows 2000 versions as you would the MS-DOS versions if you have MS-DOS-based programs that need them.
Emm386.exe	Don't use it. Windows 2000 automatically provides equivalent functionality and more.
Smartdrv.sys	Don't use it. Windows 2000 has built-in disk caching.
Ramdrive.sys	Don't use it. Windows 2000 doesn't support (and generally doesn't need) RAM drives.
Dblspace.sys and Drvspace.sys	Don't use them. Windows 2000 can't recognize or set up DoubleSpace or DriveSpace drives on a local hard drive, although it can use compressed drives shared from a networked MS-DOS computer.
Network drivers	Don't use them. Windows 2000 has built-in networking.
Drivers for hardware devices	You generally won't be able to use the MS-DOS versions. Some vendors might provide Windows 2000 versions of device drives.

Using Autoexec

In your Autoexec file, you should load any programs that your MS-DOS-based applications need. The default Autoexec.nt file loads Mscdexnt.exe, Redir.exe, and Dosx.exe. These programs enable CD-ROM extensions, network services, and extended MS-DOS services needed by some MS-DOS-based programs.

Your Autoexec.bat file, if you have one, is used by Windows 2000 for only one purpose: when you start your system, Windows 2000 scans Autoexec.bat for any environment variables set by Set or Path commands and adds them to the system environment variables. All other statements in Autoexec.bat are ignored. *For more information, see "Using Environment Variables," page 185.*

Don't use the standard Autoexec.nt to start a memory-resident program. If you do, another instance of the program gets launched with each MS-DOS-based program, which wastes memory. If you must use a memory-resident program with a certain application, create a custom Autoexec file and specify that Autoexec in the application's properties dialog box.

Working with Your Programs' Properties

Each of your MS-DOS-based programs has a properties dialog box that spells out everything Windows 2000 needs to know to run the program. Windows 2000 records the property settings in a Program Information File, or PIF. (If you never modify the properties for an MS-DOS-based program, Windows 2000 uses the settings recorded in %SystemRoot%_default.pif. As soon as you make any property changes for a program, Windows 2000 creates a PIF for that program. The PIF that's created becomes a shortcut for the application.) You can use the properties dialog box to adjust the amount of memory allocated to a program, the program's initial display mode (full-screen or windowed), the icon associated with the program, and so on. To make changes to Windows 2000's defaults, modify _default.pif.

To get to a program's properties dialog box, right-click its entry in Windows Explorer. Then choose Properties from the shortcut menu. As you'll see, some of the settings in your programs' PIFs are present only for the sake of compatibility with Windows 9x.

When you choose Properties from a running application's Control menu, you see the program's console properties dialog box. Console properties dialog boxes provide a similar group of settings, but changes you make there are not saved as part of the program's PIF. *For information about console properties, see "Customizing Command Prompt Windows," page 174.*

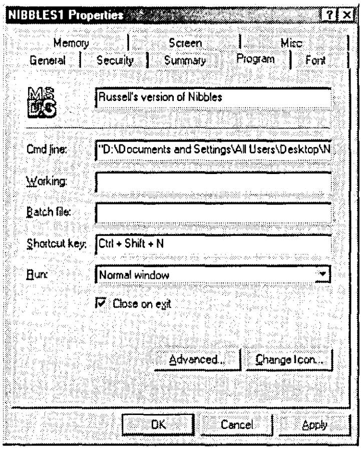
The General tab of the properties dialog box includes information about the size of the program, its creation and most-recent-access dates, and so on. The Security tab, which appears only for PIFs stored on NTFS volumes, lets you view and set permissions and monitor use of the PIF.

Options on the Program Tab

The Program tab of an MS-DOS-based program's properties dialog box, shown in Figure 10-4, includes basic information about a program. Most of this tab is self-explanatory, but here are a few points to note:

- The top line on the tab specifies the text that appears on the program's title bar when the program runs in a window. The default is the program's file name.
- You can add command-line parameters in the Cmd Line field. If you specify a question mark as a command-line parameter, Windows 2000 prompts for parameters at run time.

- The Working field lets you specify a default data folder for your program. If you leave this blank, Windows 2000 uses the folder in which the program resides.
- The Batch File and Run fields are provided for compatibility with Windows 9x. They have no effect in Windows 2000.
- In the Shortcut Key field, you can specify a keyboard shortcut for switching to this program. The shortcut key you assign must include the Ctrl key and/or the Alt key plus one character key (a letter, number, or symbol). If the shortcut key you assign is one that's used by a Windows-based application, it won't work in that application while the MS-DOS-based application is running. Note that this shortcut does not launch the program; it's useful only for switching from another program to this program.



Russell's version of Nibbles

Cmd line: "D:\Documents and Settings\All Users\Desktop\N

Working:

Batch file:

Shortcut key: Ctrl + Shift + N

Run: Normal window

☑ Close on exit

Figure 10-4
Use the Program tab to specify your program's title, working directory, keyboard shortcut, and other parameters.

The Program tab includes an Advanced button, which lets you select Config and Autoexec files that set up your MS-DOS configuration before the program runs. *For information about using the Advanced button, see "Setting the MS-DOS Configuration," page 161.*

Options on the Font Tab

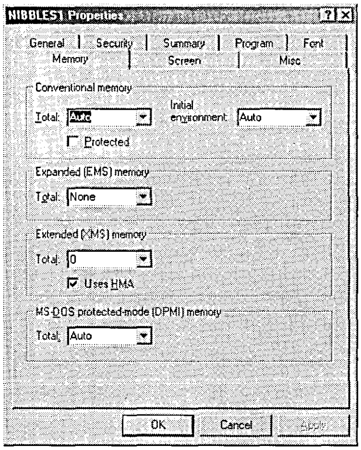
The Font tab looks as though it allows you to choose alternative display fonts to be used when an MS-DOS-based program is running in a window. Unfortunately, it does not. Selecting a font here is effective only when you run the program under Windows 9x, not while you're running Windows 2000.

To select a different font for use with Windows 2000, visit the console properties dialog box instead. *For details, see "Selecting a Font," page 176.*

Options on the Memory Tab

The Memory tab, shown in Figure 10-5, allows you to allocate memory to your applications in particular amounts and in various categories. Those categories are as follows:

Conventional	Memory in the range 0–640 KB
Expanded (EMS)	Physical memory above 1024 KB that is mapped into ranges between 640 KB and 1024 KB
Extended (XMS)	Memory above 1024 KB



Conventional memory

Total: Auto

Initial environment: Auto

□ Protected

Expanded (EMS) memory

Total: None

Extended (XMS) memory

Total: 0

☑ Uses HMA

MS-DOS protected-mode (DPMI) memory

Total: Auto

Figure 10-5
Use the Memory tab to allocate memory, in various categories, to your MS-DOS-based application.

In all three cases, the default setting, Auto, should work for most programs. For conventional memory, Auto means that Windows supplies your application with as much memory as it can. Unless you're running a particularly small-scale MS-DOS-based application and you need to conserve memory for other programs, you probably won't find a good reason to change the Auto setting.

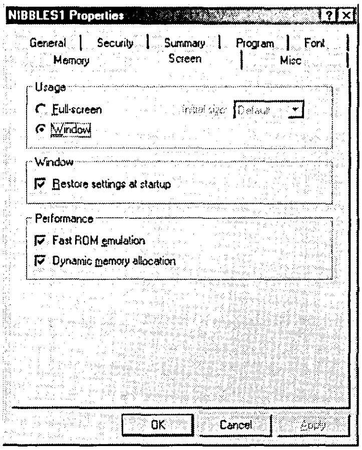
Auto also means "as much as possible" in the EMS and XMS drop-down lists. In rare cases, an MS-DOS-based program might have trouble handling an unlimited amount of EMS or XMS memory. If your program is one of the exceptional few, use these drop-down lists to reduce the available EMS or XMS memory.

The Initial Environment and MS-DOS Protected-Mode (DPMI) Memory settings on this tab have no effect in Windows 2000. They are effective only when you run the PIF under Windows 9x.

Options on the Screen Tab

The Screen tab of an MS-DOS-based program's properties dialog box, shown in Figure 10-6, lets you choose between full-screen and windowed display mode and also allows you to override two performance defaults found in Windows. The Initial

Size, Display Toolbar, and Restore Settings At Startup settings are present for compatibility purposes and have no effect in Windows 2000.



Usage

○ Full-screen

● Window

Initial size: Default

Window

☑ Restore settings at startup

Performance

☑ Fast ROM emulation

☑ Dynamic memory allocation

Figure 10-6
Use the Screen tab to specify windowed or full-screen display.

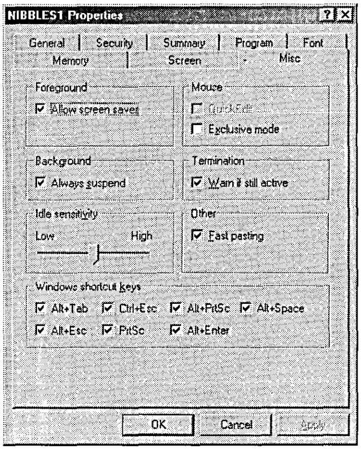
To achieve faster screen performance, Windows normally uses volatile memory (RAM) to emulate video routines that are stored in read-only memory (ROM). If you experience any abnormal screen behavior in an MS-DOS-based program, try turning off this emulation by clearing the Fast ROM Emulation check box on the Screen tab.

Programs use considerably less video memory when displaying text than when displaying graphics. When an MS-DOS-based program switches from a graphics display to a text display, Windows normally takes advantage of the "memory dividend" so that more memory is available for other programs. When an MS-DOS-based program switches back to a graphics display, Windows reallocates memory to the MS-DOS session. If you experience any problems switching from text mode to graphics mode in an MS-DOS-based program, try turning off this "dynamic memory allocation" by clearing the Dynamic Memory Allocation check box on the Screen tab.

For fastest video performance, it's best to select Full-Screen in the Usage section of this tab. While your program is running, you can press Alt+Enter to toggle between full-screen and windowed display.

Options on the Misc Tab

Options on the Misc tab of an MS-DOS-based program's properties dialog box, shown in Figure 10-7, provide control over shortcut keys and other matters. Settings in the Foreground, Mouse, Background, and Termination boxes have no effect in Windows 2000; they appear here for compatibility with Windows 9x.



Foreground
☑ Allow screen saver

Mouse
□ QuickEdit
□ Exclusive mode

Background
☑ Always suspend

Termination
☑ Warn if still active

Idle sensitivity
Low High

Other
☑ Fast pasting

Windows shortcut keys
☑ Alt+Tab ☑ Ctrl+Esc ☑ Alt+PrtSc ☑ Alt+Space
☑ Alt+Esc ☑ PrtSc ☑ Alt+Enter

Figure 10-7
Use the Misc tab to make Windows keystroke combinations, such as Alt+Tab, available to your MS-DOS-based program.

When an MS-DOS-based program running in the foreground sits idle—for example, while it's waiting for your next keystroke—Windows makes some of the resources it normally allocates to that program available to other running programs. The Idle Sensitivity slider on the Misc tab gives you some control over how much idle time Windows tolerates before reallocating resources. If your program seems less responsive than you want it to be, or if it appears to pause periodically, move the slider to the left. If you want other programs to run more quickly while your MS-DOS-based program has the focus, move the slider to the right.

If Windows doesn't correctly paste data from the clipboard into an MS-DOS-based program, try clearing the Fast Pasting check box on the Misc tab. This slows the rate at which Windows feeds clipboard data to the program.

Windows normally reserves certain keystroke combinations for itself, even while an MS-DOS-based program has the focus. For example, if you press Alt+Enter while working in an MS-DOS-based program, Windows assumes that the keystroke combination is intended for it rather than for the MS-DOS-based program. The normal effects of the reserved keystroke combinations that appear on this tab are listed here:

Alt+Tab	Lets you switch to a different program
Ctrl+Esc	Displays the Start menu
Alt+PrtSc	Copies the current window to the clipboard as a bitmap
Alt+Space	Displays the current program's Control menu
Alt+Esc	Switches the focus to another program
PrtSc	Copies the desktop to the clipboard as a bitmap
Alt+Enter	Switches between full-screen and windowed display

To make any of these keyboard shortcuts available to an MS-DOS-based application, clear the appropriate check box in the Windows Shortcut Keys section of the Misc tab.

Printing from an MS-DOS-Based Application

If you plan to print from your MS-DOS-based application, it's best to configure it to print to LPT*n* (where *n* is the number of your parallel printer port) rather than to PRN. When you print to LPT*n*, your application most likely uses calls to Interrupt 17. If you configure it to print to PRN, it prints directly to the printer port. The latter approach is considerably slower in Windows 2000.

Running POSIX-Based Applications

For full compliance with the POSIX standard, you should save any files created by POSIX-based applications on an NTFS volume. NTFS supports POSIX with the following features:

- **Case-sensitive file names.** NTFS preserves the case with which file names are saved, so that POSIX-based applications can distinguish between, say, Myfile.doc and MyFile.doc.
- **Hard links.** A POSIX file can be given more than one name, allowing two different file names (in different folders, for example) to point to the same data.
- **Additional time stamps.** POSIX-based applications can recognize such time stamps as time of last access or modification.

Note that even if you don't use POSIX-based applications yourself, if you upload files to a UNIX-based Web server, you need to be aware of case distinctions. Your server will treat variants such as Calendar.htm and calendar.htm as distinct files. Because NTFS preserves case, even though Windows 2000–based applications are case insensitive, you should store files that are to be uploaded to a UNIX-based Web server on NTFS volumes.

Chapter 11

Using the Command Prompt

In This Chapter

Starting and Ending a Command Prompt Session 172
Customizing Command Prompt Windows 174
Starting Programs 178
Using Commands 179
Using Environment Variables 185
Starting Command Prompt and Running a Command 187
Using AutoRun to Execute Commands When Command Prompt Starts 188
Using File and Folder Name Completion 189
Using Command Extensions 190
Using Cmd's Command-Line Syntax 190
Using Network Commands 191

Microsoft Windows 2000 allows you to enter commands, run batch programs, and run applications by typing commands at the command prompt. If you're accustomed to performing file management and disk management operations at the command line, you don't need to change your ways in Windows 2000. In Windows 2000, you can open multiple command prompts, each in its own separate session, protected from any failures that might occur in other sessions.

You can run any supported command or application at the command prompt, regardless of which operating system it was designed for—Windows 2000, Windows 9x, Windows 3.x, MS-DOS, OS/2 1.x, or POSIX. In addition to starting programs, you can use the command prompt to

- Issue Windows 2000 commands, which include almost all commands from MS-DOS 5 plus many new commands

- Copy and paste information between applications
- Administer or use network resources
- Communicate on a TCP/IP-based network, such as the Internet
- Pipe or redirect data between subsystems

You can customize your Command Prompt sessions in various ways, and Windows 2000 includes tools such as Doskey and batch programs that make using Command Prompt sessions easier. *For information about using Doskey, see Chapter 36, "Using Doskey Macros." For information about automating tasks with batch files, see Chapter 37, "Using Batch Programs."*

Starting and Ending a Command Prompt Session

To get to the command prompt, do any of the following:

- Choose Start | Programs | Accessories | Command Prompt.
- Choose Start | Run and type *cmd,* with or without any optional command-line arguments. *(For more about Command Prompt's command-line syntax, see "Using Cmd's Command-Line Syntax," page 190.)*
- Double-click the Cmd icon in your %SystemRoot%\ System32 folder.
- Double-click any shortcut for Cmd.exe.

You can open as many Command Prompt windows as you like. With each additional window, you start another Command Prompt session. For example, you might want to open two Command Prompt windows to see two directories in side-by-side windows. To open another Command Prompt window, type *start* or *start cmd* at the command prompt. (These commands produce the same result. If you don't type a program name after *start,* Windows 2000 assumes that you want to start Cmd.exe.)

When the Command Prompt window is active, you can end a Command Prompt session in any of the following ways:

- Type *exit* at the command prompt.
- Click the Close button.
- Click the Control-menu icon and choose Close from the Control menu.
- Double-click the Control-menu icon.

If you are running a character-based program in the Command Prompt window, you should use the program's normal exit command to terminate the program before attempting to close the window and end the Command Prompt session. However, if you are sure that the program doesn't have any unsaved files, you can safely and quickly close it using one of the last three methods in the preceding list. A dialog box appears asking whether you really want to terminate the program.

Starting Command Prompt at a Particular Folder

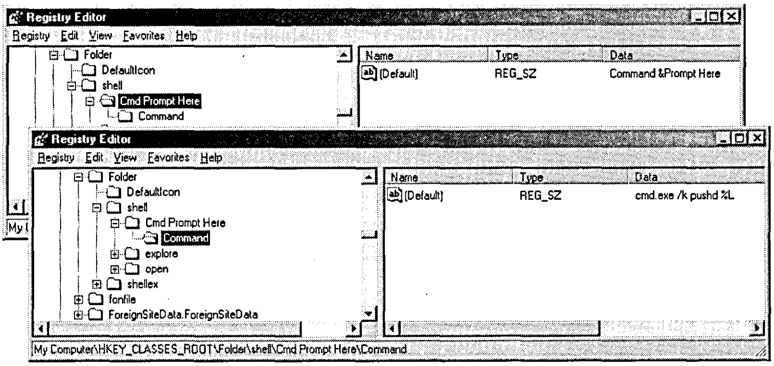
You can add a nifty shortcut-menu command to the folder file type that will allow you to right-click any folder in Windows Explorer and start a Command Prompt session with that folder as the current folder:

1. In Notepad or another plain-text editor, create a file with the following data:

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\Folder\shell\Cmd Here]
@="Command &Prompt Here"
[HKEY_CLASSES_ROOT\Folder\shell\Cmd Here\command]
@="cmd.exe /k pushd %L"
```

2. Save the file as Cmdhere.reg.
3. Double-click Cmdhere.reg and answer the confirmation prompt.

These steps create the new registry values shown in Figure 11-1. *For more information about editing the registry, see Chapter 39, "Working with the Registry."*



Name	Type	Data
(Default)	REG_SZ	Command &Prompt Here

Name	Type	Data
(Default)	REG_SZ	cmd.exe /k pushd %L

My Computer\HKEY_CLASSES_ROOT\Folder\shell\Cmd Prompt Here\Command

Figure 11-1
These new subkeys of HKCR\Folder\Shell create a shortcut-menu command that starts Command Prompt at the current folder.

Cmd.exe vs. Command.com

Cmd.exe is Windows 2000's command processor. Command.com, the 16-bit command processor of MS-DOS days, is still supported, but unless you have a legacy application that requires it, you should stick with Cmd.exe. You can run external MS-DOS commands, batch files, and other executables with either processor, but Cmd includes a few internal commands not available in Command.com, and some of the internal commands common to both have additional options in Cmd. Moreover, most of the command-line syntax described later in this chapter is available only with Cmd.

Customizing Command Prompt Windows

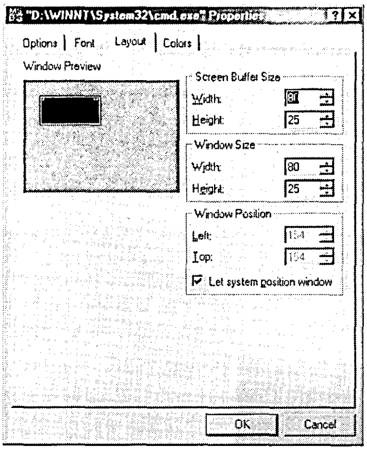
You can customize the appearance of a Command Prompt window in several ways: you can change its size, select a font, and even use eye-pleasing colors. And you can save these settings independently for each shortcut that launches a Command Prompt session, so you can make appropriate settings for different tasks.

To customize a Command Prompt window, you make settings in a properties dialog box that you can reach in any of three ways:

- Right-click a shortcut that opens a Command Prompt window and choose Properties from the shortcut menu. Changes you make here affect all future Command Prompt sessions launched from this shortcut.
- Click the Control-menu icon on a Command Prompt window and choose Properties from the Control menu. (If Command Prompt is running in full-screen mode, press Alt+Enter to switch to windowed display.) Changes you make here affect the current session. When you leave the properties dialog box, you'll be given the option of propagating your changes to the shortcut from which this session was launched. If you accept, all future sessions launched from that shortcut will have the new properties.
- Click the Control-menu icon on a Command Prompt window and choose Defaults from the Control menu. (If Command Prompt is running in full-screen mode, press Alt+Enter to switch to windowed display.) Changes here *do not* affect the current session. They affect all future Command Prompt sessions except those launched from a shortcut whose properties you have modified. They also affect future sessions in character-mode, MS-DOS-based applications that do not have a PIF and that do not store their own settings. *(For more information about running MS-DOS-based applications, see Chapter 10, "Using Programs Written for Other Operating Systems.")*

Setting the Window Size and Position

To change the screen position where a newly launched Command Prompt window appears, open the window's properties dialog box (using any of the methods described previously) and click the Layout tab (see Figure 11-2).



Screen Buffer Size
Width: 80
Height: 25

Window Size
Width: 80
Height: 25

Window Position
Left: 154
Top: 154
☑ Let system position window

Figure 11-2
Settings on the Layout tab control the number of lines and characters per line that a Command Prompt window can display.

The dialog box maintains two different sizes—the screen buffer size and the window size. The width for both sizes is specified in columns (characters); the height is specified in rows (text lines).

The screen buffer settings control the size of the "virtual screen," which is the maximum extent of the screen. Standard screen sizes are 80×25, 80×43, or 80×50, but you can set your Command Prompt screen to any size you want. (Some programs that you launch from a Command Prompt session, however, might work correctly only with standard screen sizes. In such cases, Windows 2000 automatically adjusts the screen buffer size to the closest size that the program understands.)

The window size settings control the size of the Command Prompt window on your screen. In most cases, you'll want it the same size as the screen buffer. But if your screen is crowded, you can reduce the window size. If you do, scroll bars are added so that you can scroll to different parts of the virtual screen. The window size settings can never be larger than the screen buffer size settings.

Because you specify a window size as a number of columns and rows of characters, the size of those characters also affects the amount of space a console occupies on your display. *For information about changing the character size, see "Selecting a Font," page 176.*

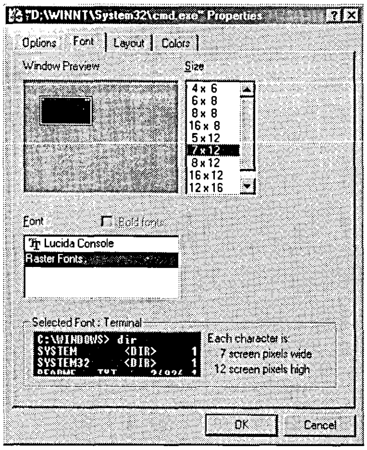
Setting the Window Size and Position Visually

Rather than guess at the settings for window size and window position, you can use the following procedure:

1. Open a Command Prompt window.
2. Drag the window's borders to adjust its size and drag its title bar to adjust its position.
3. Click the Control-menu icon and choose Properties from its menu.
4. Click the Layout tab and you'll see the settings that reflect the window's current condition.
5. Click OK to apply the settings.
6. Select Save Properties For Future Windows With Same Title to retain the settings for future sessions.

Selecting a Font

Unlike most Windows-based applications, applications in a Command Prompt window can display only one font at a time. Compared to what's available in most Windows-based applications, your choice of fonts is limited, as you'll see if you click the Font tab in the Command Prompt window's properties dialog box (see Figure 11-3).



Size: 7 x 12

Font: Raster Fonts

Selected Font : Terminal

```
C:\WINDOWS> dir
SYSTEM         <DIR>        1
SYSTEM32       <DIR>        1
```

Each character is:
7 screen pixels wide
12 screen pixels high

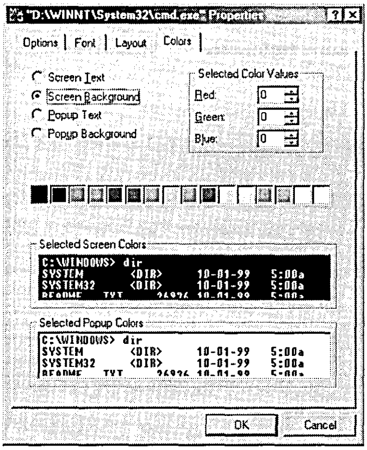
Figure 11-3
The small window at the bottom of this dialog box shows an actual-size sample of the selected font; the window at the top shows the relative size and shape of the Command Prompt window if you use the selected font.

You should make a selection in the Font list first because your choice here determines the contents of the Size list. If you select Lucida Console, you'll find point sizes to choose from in the Size list. If you select Raster Fonts, you'll find character widths and heights (in pixels, or screen dots) in the Size list, as shown in Figure 11-3.

Setting Colors

You can set the color of the text and the background of the Command Prompt window. You can also set the color of the text and the background of pop-up windows that originate from the command prompt, such as the command history.

To set colors, click the Colors tab in the Command Prompt window's properties dialog box. The dialog box is shown in Figure 11-4.



○ Screen Text
● Screen Background
○ Popup Text
○ Popup Background

Selected Color Values
Red: 0
Green: 0
Blue: 0

Selected Screen Colors

```
C:\WINDOWS> dir
SYSTEM         <DIR>        10-01-99    5:00a
SYSTEM32       <DIR>        10-01-99    5:00a
README    TXT       26926  10-01-99    5:00a
```

Selected Popup Colors

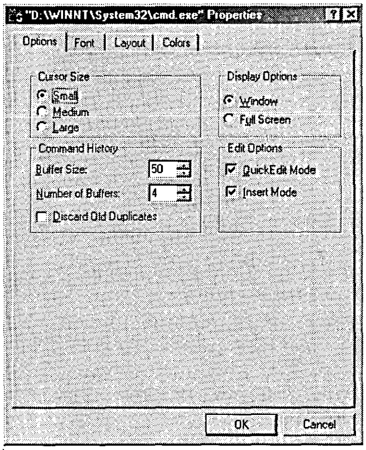
```
C:\WINDOWS> dir
SYSTEM         <DIR>        10-01-99    5:00a
SYSTEM32       <DIR>        10-01-99    5:00a
README    TXT       26926  10-01-99    5:00a
```

Figure 11-4
You can set separate foreground and background colors for the Command Prompt window and pop-up windows, such as the command history that appears when you press F7.

Setting Other Options

The Options tab in the Command Prompt window's properties dialog box, shown in Figure 11-5, offers a grab bag of options that affect how your Command Prompt window operates.

- The Cursor Size option buttons control the size of the blinking cursor in a Command Prompt window.
- The Display Options setting determines whether your Command Prompt session appears in a window or occupies the entire screen.
- The Command History options control the buffer used by Doskey.
    - Buffer Size specifies the number of commands to save in each command history.



Cursor Size
● Small
○ Medium
○ Large

Display Options
● Window
○ Full Screen

Command History
Buffer Size: 50
Number of Buffers: 4
□ Discard Old Duplicates

Edit Options
☑ QuickEdit Mode
☑ Insert Mode

Figure 11-5
You can set cursor size, the size of your command-history buffer, and other specifications on the Options tab.

  - Number Of Buffers specifies the number of command history buffers to use. (Certain character-based programs other than Cmd.exe use Doskey's command history. Doskey maintains a separate history for each such program that you start.)
  - Selecting Discard Old Duplicates uses the history buffers more efficiently by not saving duplicate commands.

- QuickEdit Mode provides a fast, easy way to copy text from (and paste text into) Command Prompt windows with a mouse. (If you don't select QuickEdit Mode, you can use commands on the Control menu for copying and pasting text.) *For details, see "Using Copy and Paste," page 159.*

Starting Programs

You can start all kinds of programs at the command prompt—programs for Windows 2000, Windows 9x, Windows NT, Windows 3.x, MS-DOS, OS/2 1.x, or POSIX—so you don't need to know a program's origin or type to run it. If it's on your disk, simply type its name (and path, if needed) followed by any parameters. It should run with no questions asked.

If you're starting a character-based program, it runs in the Command Prompt window. When you terminate the application, the command prompt returns. If you start a Windows-based program, it appears in its own window.

In early versions of Windows NT, if you ran a Windows-based program from Command Prompt, the Command Prompt session remained inaccessible until the Windows-based program ended. To continue using Command Prompt after launching a Windows-based program, you had to launch that program with the Start command. That behavior has changed in Windows 2000; the Command Prompt session now remains accessible by default. If you want the old behavior, launch your program with the Start command, using the /Wait switch, like this:

```
start /wait myprog.exe
```

The /Wait switch is probably not useful unless you need the old behavior for some reason. The Start command has other options that are useful, however. For Windows-based programs, you can use /Min or /Max to make the program open in a minimized or maximized window. For character-based programs, you can enter (in quotation marks) the title that you want to appear on the program window. Place any parameters or switches that you use with the Start command *before* the name of the program or command you want to start. Anything after the program name is passed to the program as a command-line parameter and is ignored by Start.

For more information about the Start command, type *start /?* at the command prompt.

Using Commands

In most respects, entering commands or running programs at the Windows 2000 command prompt is the same as using the command prompt of any other operating system. MS-DOS, OS/2, UNIX—if you've used one command prompt, you've used them all. Every operating system has a command to delete files, another to display lists of files, another to copy files, and so on. The names and details may be different, but it's the same cast of characters.

The commands and features available at the Windows 2000 command prompt most closely resemble those of MS-DOS 5—with some important enhancements and additions.

Getting Help

The first thing you need to know about using the command prompt is how to get help. You can get help on any command-line program or internal command supplied with Windows 2000 in two ways. You can

- Type the name of the command followed by */?*. For example,

  ```
  dir /?
  ```

- Type *help* followed by the name of the command. For example,

  ```
  help dir
  ```

For help with network-related commands, precede your help request with *net*. For example, type *net view /?* or *net help view* for information about the Net View command. (With the Net commands, "net help *command*" provides more detailed help than "net *command* /?")

You can also type *help* with no arguments to get a list of the internal commands and system utilities provided with Windows 2000.

Editing the Command Line

When working at a command prompt, you often enter the same command several times, or enter several similar commands. If you make a mistake when typing a command line, you don't want to retype the whole thing—you just need to fix the part that was wrong. Windows 2000 includes a feature that recalls previous commands and lets you edit them on the current command line. Table 11-1 shows the editing keys and what they do.

Table 11-1. Command-Line Editing Keys

Key	Function
Up Arrow	Recalls the previous command in the command history
Down Arrow	Recalls the next command in the command history
PgUp	Recalls the earliest command used in this session
PgDn	Recalls the most recent command used
Left Arrow	Moves left one character
Right Arrow	Moves right one character
Ctrl+Left Arrow	Moves left one word
Ctrl+Right Arrow	Moves right one word
Home	Moves to the beginning of the line
End	Moves to the end of the line
Esc	Clears the current command
F7	Displays the command history in a scrollable pop-up box
F8	Displays commands that start with characters currently on the command line
Alt+F7	Clears the command history

The command-line recall feature works by keeping a history of the commands entered during the Command Prompt session. To display this history, press the F7 key. A window pops up that shows the commands you have recently entered. Scroll through the history with the arrow keys to select the command you want. Then press Enter to reuse the selected command, or press the Left Arrow key to place the selected text on the command line without executing the command. (This lets you edit the command before executing it.)

Displaying the pop-up window is not necessary to use the command history. You can scroll through the history with the Up Arrow and Down Arrow keys.

The F8 key provides a useful alternative to the Up Arrow key. The Up Arrow key moves you through the commands to the top of the command buffer and then stops. The F8 key does the same, except that when you get to the top of the buffer, it cycles back to the bottom. Furthermore, F8 displays only commands in the buffer that begin with whatever you type before you press F8. Type *d* at the command prompt (don't press Enter) and then press F8 a few times. You'll cycle through recently entered commands that start with *d*, such as Dir and Del. Now type *e* (after the *d*) and press F8 a few more times. You'll cycle through Del commands along with any others that start with *de*. You can save a lot of keystrokes with F8 if you know the first letters of the command you're looking for.

Using Wildcards

Windows 2000, like MS-DOS, recognizes two wildcard characters: ? and *. The question mark represents any single character in a file name. The asterisk matches any number of characters.

In MS-DOS, the asterisk works only at the end of the file name or extension. Windows 2000 handles the asterisk much more flexibly, allowing multiple asterisks in a command string and allowing you to use the asterisk character wherever you want.

Using Command Symbols

Old-fashioned programs that take all their input from a command line and then run unaided can be useful in a multitasking system because you can turn them loose to do complicated processing in the background while you continue to work with other programs in the foreground. Windows 2000 includes features that make command-line programs easier to run and more powerful and that let you chain programs together so that later ones use the output of their predecessors as input.

To work together better, many command-line programs follow a set of conventions that control their interaction.

- By default, programs take all their input as lines of text typed at the keyboard. But input in the same format also can be redirected from a file or any device capable of sending lines of text.
- By default, programs send all their output to the screen as lines of text. But output in the same format also can be redirected to a file or another line-oriented device such as a printer.
- Programs are written to set a number called a return value when they terminate, to indicate the results of the program.

When programs are written according to these rules, you can use the symbols in Table 11-2 to control a program's input and output and to connect or chain programs together.

Table 11-2. Command Symbols

Symbol	Purpose
<	Redirects input
>	Redirects output
>>	Appends redirected output to existing data
|	Pipes output
&	Separates multiple commands in a command line
&&	Runs the command after && only if the command before && is successful
||	Runs the command after || only if the command before || fails
^	Treats the next symbol as a character
(and)	Groups commands

The Redirection Symbols

As in MS-DOS and UNIX, Command Prompt sessions in Windows 2000 allow you to override the default source for input (the keyboard) or the default destination for output (the screen).

Redirecting Input

To redirect input from a file, type the command followed by a less-than sign (<) and the name of the file. The Sort and More commands are examples of commands that can accept input from a file. The following example uses Sort to filter the file created with the Dir command shown previously:

```
sort < batch.lst
```

The input file, Batch.lst, contains a list of .bat files followed by a list of .cmd files (assuming that you have some of each in the current folder). The output to the screen has the same list of files sorted alphabetically by file name.

Redirecting Output

To redirect output to a file, type the command followed by a greater-than sign (>) and the name of the file. For example, to send the output of the Dir command to a file rather than the screen, type the following:

```
dir /b *.bat > batch.lst
```

This command line creates a file called Batch.lst that contains the names of all the .bat files in the current folder.

Using two greater-than signs (>>) redirects the output and appends it to an existing file. For example:

```
dir /b *.cmd >> batch.lst
```

This command line appends a list of .cmd files to the previously created file containing .bat files. (If you use >> to append to a file that doesn't exist, Windows 2000 creates the file.)

Redirecting Input and Output

You can redirect both input and output in a command line. For example, to use Batch.lst as input to the Sort command and send its output to a file named Sorted.lst, you can type the following:

```
sort < batch.lst > sorted.lst
```

Standard Output and Standard Error

Programs can be written to send their output to either the standard output device or the standard error device. Sometimes programs are written to send different types of output to each device. You can't always tell which is which because, by default, both devices are the screen.

The Windows 2000 Type command illustrates the difference. When used with wildcards (something you can't do with the Type command in MS-DOS or Windows 9x), Type sends the name of each matching file to standard error and sends the contents of the file to standard output. Because they both go to the screen, you see a nice display with each file name followed by its contents.

However, if you try to redirect output to a file like this:

```
type *.bat > std.out
```

the file names still appear on your screen because standard error is still directed to the screen. Only the file contents are redirected to Std.out.

Windows 2000 allows you to qualify the redirection symbol by preceding it with a number. Use 1> (or simply >) for standard output and 2> for standard error. For example:

```
type *.bat 2> err.out
```

This time the file contents go to the screen and the names are redirected to Err.out. You can redirect both to separate files with this command line:

```
type *.bat 2> err.out 1> std.out
```

The Pipe Symbol

The pipe symbol (|) is used to send, or *pipe*, the output of one program to a second program as the second program's input. Piping is commonly used with the More utility, which displays multiple screens of output one screenful at a time. For example:

```
help dir | more
```

This command line uses the output of Help as the input for More. The More command filters out the first screenful of Help output, sends it to the screen as its own output, and then waits for a keypress before sending more filtered output.

The Command Combination Symbols

Unlike MS-DOS, Windows 2000 allows you to enter multiple commands on a single command line. Furthermore, you can make later commands depend on the results of earlier commands. This feature can be particularly useful in batch programs and Doskey macros, but you might also find it convenient at the command prompt.

For information about batch programs, see Chapter 37, "Using Batch Programs." For information about Doskey macros, see Chapter 36, "Using Doskey Macros."

To simply combine commands without regard to their results, use the & symbol, like this:

```
copy a:file.dat & edit file.dat
```

But what if there is no File.dat on drive A? Then it can't be copied to the current drive, and the Edit command will fail when it can't find the file. Your screen will be littered with error messages. Windows 2000 provides two command symbols for better control over situations like this:

- The && symbol causes the second command to run only if the first command succeeds.
- The || symbol causes the second command to run only if the first command fails.

Consider this modified version of the earlier example:

```
copy a:file.dat && edit file.dat
```

With this command line, if the Copy command fails, the Edit command is ignored.

Sometimes you want the opposite effect: execute the second command only if the first fails. You can do this with the || symbol:

```
copy a:file.dat || copy b:file.dat
```

This command line tries to copy the file from drive A. If that doesn't work, it tries to copy the file from drive B.

The Escape Symbol

Some command symbols are legal characters in file names. This leads to ambiguities. You can resolve such ambiguities by using the caret (^) as an escape to indicate that whatever follows it is a character rather than a command symbol.

Consider the following command line:

```
copy f:\cartoons\Tom&Jerry
```

This copies the file F:\Cartoons\Tom to the current folder and then executes the Jerry command—probably not what you wanted. You might think that because no space comes before or after the & symbol, the system will know that you are referring to the file name Tom&Jerry. Not true. When a command symbol (such as the ampersand) appears on the command line, whatever follows it is assumed to be a command, space or no space. Use the caret as follows to indicate that you are referring to a file name:

```
copy f:\cartoons\Tom^&Jerry
```

Alternatively, rather than using the ^ symbol, you can enclose a file specification that includes command symbols (or other troublesome characters, such as spaces) within quotation marks to achieve the same effect. For example:

```
copy "f:\cartoons\Tom&Jerry"
```

Pausing or Canceling Commands

You can pause or cancel a command that you enter at the command prompt. (Keep this in mind if you accidentally request a directory of all the files—or worse, enter a command to delete all the files—on a huge network server drive!)

To pause the output of a command, press Ctrl+S or the Pause key. To resume output, press any alphanumeric key.

If you have QuickEdit mode enabled for your Command Prompt window, simply click in the window to pause command output. To resume output, right-click in the window. *For information about QuickEdit, see "QuickEdit Mode," page 158.*

To cancel a command, press Ctrl+C or Ctrl+Break. With either key, your command is canceled and the command prompt returns. Be aware, though, that any action (such as deleting files) that occurs before you cancel the command is done—and cannot be undone.

Using Environment Variables

Command-prompt operating systems traditionally use environment variables as a means for programs to share information and read global settings. (Windows 2000—and applications written for Windows 2000—uses the registry for the same purpose.)

Viewing Environment Variables

The Set command allows you to examine as well as set environment variables. To examine the current environment variables, open a Command Prompt window and type *set* (without any arguments). Windows 2000 displays a listing of all the current environment variables and their values, as the following typical example shows:

```
ALLUSERSPROFILE=D:\Documents and Settings\All Users
APPDATA=D:\Documents and Settings\Craig\Application Data
CommonProgramFiles=D:\Program Files\Common Files
COMPUTERNAME=FAFNER
ComSpec=D:\WINNT\system32\cmd.exe
HOMEDRIVE=D:
HOMEPATH=\
LOGONSERVER=\\FAFNER
```

```
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Os2LibPath=D:\WINNT\system32\os2\dll;
Path=D:\WINNT\system32;D:\WINNT;D:\WINNT\System32\Wbem;D:\Program Files\
 Support Tools\;;C:\PROGRA~1\NETWOR~1\MCAFEE~1
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 6 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=060a
ProgramFiles=D:\Program Files
PROMPT=$P$G
SystemDrive=D:
SystemRoot=D:\WINNT
TEMP=D:\DOCUME~1\Craig\LOCALS~1\Temp
TMP=D:\DOCUME~1\Craig\LOCALS~1\Temp
USERDOMAIN=FAFNER
USERNAME=Craig
USERPROFILE=D:\Documents and Settings\Craig
windir=D:\WINNT
```

Predefined Environment Variables

Many of the environment variables in the preceding example are ones that Windows 2000 automatically sets with information about your system. You can use these values in batch programs, Doskey macros, and command lines—and, if you're a programmer, in the programs you write. The system-defined environment variables include

- **Information about your place in the network.** COMPUTERNAME contains the name of your computer, USERDOMAIN contains the name of the domain you logged on to, and USERNAME contains your logon name.
- **Information about your computer.** PROCESSOR_ARCHITECTURE contains the type of processor (such as "x86"), and PROCESSOR_IDENTIFIER, PROCESSOR_LEVEL, and PROCESSOR_REVISION provide specific information about the processor version.
- **Information about Windows 2000.** SystemRoot contains the drive and folder in which Windows 2000 is installed; SystemDrive contains only the drive letter.
- **Information about your programs.** When you type a program name (to start the program) without typing its path, Windows 2000 looks first in the current folder. If the program isn't located in the current folder, Windows 2000 looks in each folder listed in the Path variable.
- **Information about the command prompt.** PROMPT contains codes that define the appearance of the command prompt itself. (For details, type *prompt /?* at the command prompt.)

Modifying Environment Variables

Command Prompt gets its environment variables from three sources:

- Any variables set in your Autoexec.bat file
- System variables, as recorded in HKLM \CurrentControlSet\Control\Session Manager\Environment
- User variables, as recorded in HKCU\Environment

When you log on, Windows 2000 scans the Autoexec.bat file in the root folder of your boot drive. At logon, the system does not actually execute Autoexec.bat; it merely scans it for environment variables initialized with Set statements. If you don't want Windows 2000 to scan your Autoexec.bat file for Set statements, open a registry editor and navigate to HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon. Then change the data associated with the ParseAutoexec value from 1 to 0.

System and user variables are both stored in the registry, but you don't need to launch a registry editor to change them. Open Control Panel | System instead. Click the Advanced tab and then the Environment button. To change system variables, you must be logged on as a member of the Administrators group.

Environment changes made via Control Panel affect your next and subsequent Command Prompt sessions (not the current ones, of course). Changes made via Autoexec.bat are not effective until your next logon. In case of conflicting assignments, user variables take precedence over system variables, which take precedence over variables declared in Autoexec.bat. The Path and OS2LibPath variables, however, are cumulative. That is, changes made in any venue are appended to any changes made in other venues. (But changes made via Autoexec.bat or HKCU\Environment are not effective until your next logon.)

Within a given Command Prompt session, you can change environment variables by means of Set statements. Such statements affect only the current session and any applications (including additional Command Prompt sessions) spawned from the current session.

Note that the Autoexec.nt file has no effect on the Command Prompt environment. Autoexec.nt affects MS-DOS-based applications only. Command Prompt, although it is the MS-DOS command interpreter, is itself a Windows 2000-based application.

Starting Command Prompt and Running a Command

The /C and /K command-line arguments allow you to start a Command Prompt session and run a command—an MS-DOS command or a batch file, for example. The difference between the two is that Cmd /C *commandstring* terminates the Command Prompt session as soon as *commandstring* has finished executing, whereas Cmd

/K *commandstring* keeps the Command Prompt session going after *commandstring* has finished. Note the following:

- You must include either /C or /K if you want to specify a command string as an argument to Cmd. If you type *cmd commandstring,* the command processor simply ignores *commandstring.*
- While *commandstring* is executing, you can't interact with the command processor. To run a command and keep the Command Prompt window interactive, use the Start command. For example, to run Mybatch.bat and continue issuing MS-DOS commands while the batch file is running, type *cmd /k start mybatch.bat.*
- If you include other command-line arguments along with /C or /K, the /C or /K must be the last argument before *commandstring.*

For more information about using Command Prompt's command-line syntax, see "Using Cmd's Command-Line Syntax," page 190.

Cmd.exe and Other Command Prompts

Cmd.exe, the application whose name is Command Prompt, is only one of several forms of command prompt available in Windows 2000. Others include the Start menu's Run command, the Address toolbar, the Address bar in Windows Explorer, and the Address bar in Microsoft Internet Explorer. In many ways, these various command prompts function alike. You can start a Windows-based application from any of them, for example. (If you do it from Internet Explorer, you need to include an explicit path specification, or else Internet Explorer will try to find a URL that matches your command string.) What's exceptional about Cmd.exe is that it lets you execute internal MS-DOS commands (commands that are not stored in discrete .exe files). To execute an internal MS-DOS command from any of the other command prompts, you need to launch Cmd.exe itself (with /K or /C) and specify your internal MS-DOS command as an argument to Cmd.

Using AutoRun to Execute Commands When Command Prompt Starts

Command Prompt's equivalent to the old MS-DOS Autoexec batch mechanism is a feature called AutoRun. By default, Command Prompt executes on startup whatever it finds in the following two registry values:

- The AutoRun value in HKLM\Software\Microsoft\Command Processor
- The AutoRun value in HKCU\Software\Microsoft\Command Processor

The AutoRun value in HKLM affects all user accounts at the current machine. The AutoRun value in HKCU affects only the current user account. If both values are present, both are executed—HKLM before HKCU.

Both AutoRun values are of data type REG_SZ, which means they can contain a single string. (You can enter a REG_MULTI_SZ value, but Windows 2000 ignores all but the first string.) To execute a sequence of separate Command Prompt statements, therefore, you must use command symbols or store the sequence as a batch program and then use AutoRun to call the batch program. *(For information about command symbols, see "Using Command Symbols," page 181. For information about batch programs, see Chapter 37, "Using Batch Programs.")*

To specify an AutoRun value, open a registry editor and navigate to the Command Processor key in either HKLM or HKCU. Create a new REG_SZ value there and name it AutoRun. Then specify your command string as the data for AutoRun, exactly as you would type it at the command prompt.

To disable AutoRun commands for a particular Command Prompt session, start Command Prompt with /D. *(For more about Command Prompt's command-line syntax, see "Using Cmd's Command-Line Syntax," page 190.)*

Using File and Folder Name Completion

Command Prompt offers an invaluable file and folder name completion feature that, remarkably, is not enabled by default. If you enable this feature, you can save yourself the trouble of typing long paths or file names. If you start a command string and then press the completion character, Command Prompt proposes the next file or folder name that's consistent with what you've typed so far. For example, to switch to a folder that starts with the letter Q, you can type *cd q* and press the folder-name completion character as many times as necessary until the folder you want appears.

You can turn on file and folder name completion for a particular Command Prompt session by starting Command Prompt with /F:on. *(For more about Command Prompt's command-line syntax, see "Using Cmd's Command-Line Syntax," page 190.)* If you do that, Command Prompt uses Ctrl+D for folder-name completion and Ctrl+F for file-name completion.

Alternatively, you can turn this feature on permanently—for either the current user account or all accounts at the current computer—by editing the registry. The REG_DWORD values CompletionChar and PathCompletionChar in HKLM\Software\Microsoft\Command Processor specify the file and folder completion characters, respectively, for all user accounts at the current computer. The corresponding values in HKCU\Software\Microsoft\Command Processor do the same for the current account. In all cases, the character should be specified as a hexadecimal value—for example, 0x4 for Ctrl+D, 0x6 for Ctrl+F, 0x9 for Tab, 0xC for Ctrl+L, and so on. To disable a completion character, specify a value of 0x20 (the space character) or 0x0.

If completion characters are specified in both HKLM and HKCU, the HKCU settings take precedence. If you start Cmd with /F:on, Command Prompt uses Ctrl+D and Ctrl+F as completion characters, regardless of your registry settings. If you start Cmd with /F:off, completion characters are disabled, regardless of your registry settings.

Using Wildcards for File and Folder Name Completion

Command Prompt recognizes wildcards in file and path specifications. Typing *cd pro**, for example, might take you to your Program Files folder (depending, of course, on where you are when you type it). Because you can include multiple wildcards in a string, you can even create formulations such as *cd pro*\com*\mic** to get to Program Files\Common Files\Microsoft Shared.

Using Command Extensions

Command extensions are changes or additions to the following internal commands: Del, Erase, Color, Cd, Chdir, Md, Mkdir, Prompt, Pushd, Popd, Set, Setlocal, Endlocal, If, For, Call, Shift, Goto, Start, Assoc, and Ftype. For example, with command extensions enabled, you can use Cd or Chdir to switch to a folder whose name includes space characters, without enclosing the path specification in quotation marks. For details about a particular command's extensions, type the command name followed by /?. (Alternatively, type *help,* followed by the command name. For a complete reference to all MS-DOS commands, choose Start | Help. On the Contents tab, select Reference\MS-DOS Commands.)

Command extensions are available only in Cmd.exe, not in Command.com, and are enabled by default. Set the REG_DWORD value EnableExtensions in HKLM \Software\Microsoft\Command Processor to 0 to disable them for all user accounts at the current machine. Set EnableExtensions in HKCU\Software\Microsoft\Command Processor to 0 to disable them for the current user account. Start Command Prompt with /E:off or /E:on to disable or enable them for the current session, regardless of the registry settings.

Using Cmd's Command-Line Syntax

The complete command-line syntax for Cmd.exe is

```
cmd [/a|/u] [/q] [/d] [/e:on|/e:off] [/f:on|/f:off] [/v:on|/v:off] [[/s]
    [/c|/k] commandstring]
```

All arguments are optional.

/A | /U. This argument lets you specify the encoding system used for text that's piped to a file or other device. Use /A for ANSI or /U for Unicode. The default is ANSI.

/Q. The /Q argument starts Command Prompt with echo off. (With echo off, you don't need to include an @echo off line to suppress screen output in a batch program. To turn echo back on after starting Command Prompt with /Q, enter *echo on* at the command prompt.)

/D. The /D argument disables execution of any AutoRun commands specified in the registry. *(See "Using AutoRun to Execute Commands When Command Prompt Starts," page 188.)*

/E:on | /E:off. The /E argument lets you override the current registry settings regarding command extensions. (*See "Using Command Extensions," page 190.)*

/F:on | /F:off. The /F argument lets you override the current registry settings regarding file and folder name completion. *(See "Using File and Folder Name Completion," page 189.)*

/V:on | /V:off. The /V argument lets you enable or disable delayed variable expansion. With /V:on, for example, the variable !var! is expanded only when executed. The default is /V:off. To turn on delayed variable expansion as a default, add the REG_DWORD value DelayedExpansion to HKLM\Software\Microsoft\Command Processor (for all users at the current machine) or HKCU\Software\Microsoft \Command Processor (for the current user account only) and set DelayedExpansion to 1. (Delayed variable expansion is useful in conditional statements and loop constructs in batch programs. For more information, type *help set* at the command prompt.)

/S /C | /K *commandstring*. As discussed earlier in this chapter *(see "Starting Command Prompt and Running a Command," page 187)*, the alternative /C and /K arguments allow you to run a command when Command Prompt starts—with /C terminating the session at the command's completion and /K keeping it open. Including /S before /C or /K affects the processing of quotation marks in *commandstring*.

If you do not include /S, *and* there are exactly two quotation marks in *commandstring*, *and* there are no "special" characters (&, <, >, (,), @, ^, or |) in *commandstring*, *and* there are one or more white-space characters (spaces, tabs, or linefeeds) between the two quotation marks, *and commandstring* is the name of an executable file, then Command Prompt preserves the two quotation characters.

If the foregoing conditions are not met and if the first character in *commandstring* is a quotation mark, Command Prompt strips the first and last quotation marks from *commandstring*.

Using Network Commands

This section describes some of the common commands for working with a network via the command prompt. Using the command prompt for these network functions is completely optional; most operations described here can also be done through

Windows Explorer. You'll find, however, that using the command prompt is sometimes easier and faster.

You might simply be working in a Command Prompt window and not want to go to the trouble of switching to another window. But a more compelling reason to learn and use network commands is that you can execute a series of network commands in a batch program and thus automate repetitive network tasks in a way that can't be done through the graphical interface.

Connecting to Shared Resources

You can connect to a shared resource by specifying a device name and a network name as part of the Net Use command, like this:

```
net use x: \\zion\document
```

This command maps a shared folder called \\Zion\Document as drive X. If the command succeeds, you can use drive X exactly as you would any drive on your local computer—subject to any restrictions imposed by the owner. For example, the owner might allow anyone to read files but allow only selected users to write, modify, or delete them.

The Chdir and Cd commands do not accept UNC path specifications. However, you can supply a UNC path as an argument for Pushd, the command that switches folders and saves the current folder on a stack (allowing you to return to the current folder with Popd). When you connect to (and switch to) a network share in this manner, Command Prompt assigns the share the first available drive letter, starting at the end of the alphabet and moving toward the beginning.

So, for example, the command

```
pushd \\Zion\Document
```

if entered at D:\ would connect with and switch to \\Zion\Document, assigning that share the drive letter Z (if Z were not already in use), and save D:\ on a stack. You could subsequently use Popd to return to D:\.

You can use Net Use to connect to network printers the same way you can use it to connect to other shares. For example, after you issue the command

```
net use lpt1 \\yellowstone\laserjet4
```

anything you print to LPT1 will go to this shared printer.

If you map a network folder to a drive letter using Windows Explorer, you can use that drive letter at the command prompt. Similarly, if you connect to a shared folder with the Net Use command, you can use that drive letter in your Windows-based applications.

You can access a shared resource directly without first mapping it to a drive letter. Simply use the network name in place of the drive name. For example, to copy Work.bat from the \Bat folder of \\Zion\Public to your C drive, use the network name rather than a drive letter, as follows:

```
copy \\zion\public\bat\work.bat c:
```

Connecting to Password-Protected Resources

Some operating systems, such as Windows 9x (using share-level access control), control access to shared resources by requiring you to enter a password for the resource. (Windows 2000, by contrast, maintains a list of users and groups that are permitted to access each shared resource. Passwords are assigned to users, not shared resources.) If you are connecting to a password-protected resource, you can append an asterisk to the Net Use command, like this:

```
net use x: \\acadia\optrarx *
```

The asterisk tells Windows 2000 to prompt you for the password. This way, the password is not displayed as you type it. You can type the password on the command line rather than use an asterisk, but anyone looking at your screen can see the password. In batch programs, you can use the asterisk or include the password with the batch command line, as your security needs dictate.

When you are finished using a resource, you can disconnect from it with the Net Use command's /Delete switch (usually abbreviated as /D), like this:

```
net use x: /d
```

Browsing Network Resources

The Net View command browses the network for the servers and shared resources you might be interested in. First you browse domains or workgroups to see which servers are available; then you browse the servers to see which shared resources are available. (For purposes of this discussion, workgroups function exactly like domains.)

You can browse the servers in your domain by typing *net view*, which displays a list of servers similar to the following:

```
Server Name          Remark
----------------------------------------------------------------
\\ACADIA             CD server
\\BADLANDS           Chris' Pentium
\\DENALI             Tommy Boy
\\KATMAI             Fax server
\\VOYAGEURS          Blake Whittington
\\YELLOWSTONE        Paula Berg
The command completed successfully.
```

The following command checks to see which other domains are available for browsing:

```
net view /domain
```

To view the servers in a domain other than your own, specify the domain name, like this:

```
net view /domain:boston
```

After you've found the name of a server, you can browse its shared resources. For example, typing *net view \\acadia* might display information similar to this:

```
Shared resources at \\acadia

CD server
Share name    Type      Used as   Comment
-------------------------------------------------------------------------------
CD-ROM 1       Disk               Windows 98
CD-ROM 2       Disk               Bookshelf '97
CD-ROM 3       Disk     W:
CD-ROM 4       Disk               Corel DRAW!
CD-ROM 5       Disk     T:        Microsoft TechNet
CD-ROM 6       Disk               Microsoft drivers
OPTRARX        Disk               Drivers for Lexmark
ROOT           Disk               Root directory

The command completed successfully.
```

When you find a resource you're interested in, you can use the Dir or Tree command to examine its contents (as long as you have been granted appropriate permissions), like this:

```
tree /f \\acadia\root | more
```

Browsing through lists of computers and shared resources should raise some concerns about how you want your own computer to appear. Remember that everyone on the network can see your computer name and the shared resources you have. Be sure to keep sensitive data in folders that are not shared, or set the permissions appropriately. If you do want to share a resource, be sure to add comments so that browsers will know what you are offering. Comments are optional when you set up your own shares, but they can save a lot of frustration for people searching for information.

Part 4

Managing Hardware

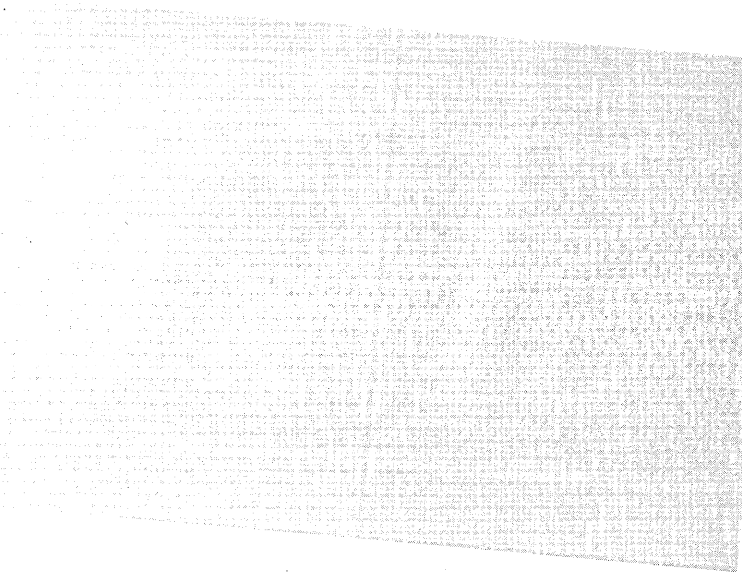
Chapter 12
Managing Disks 197

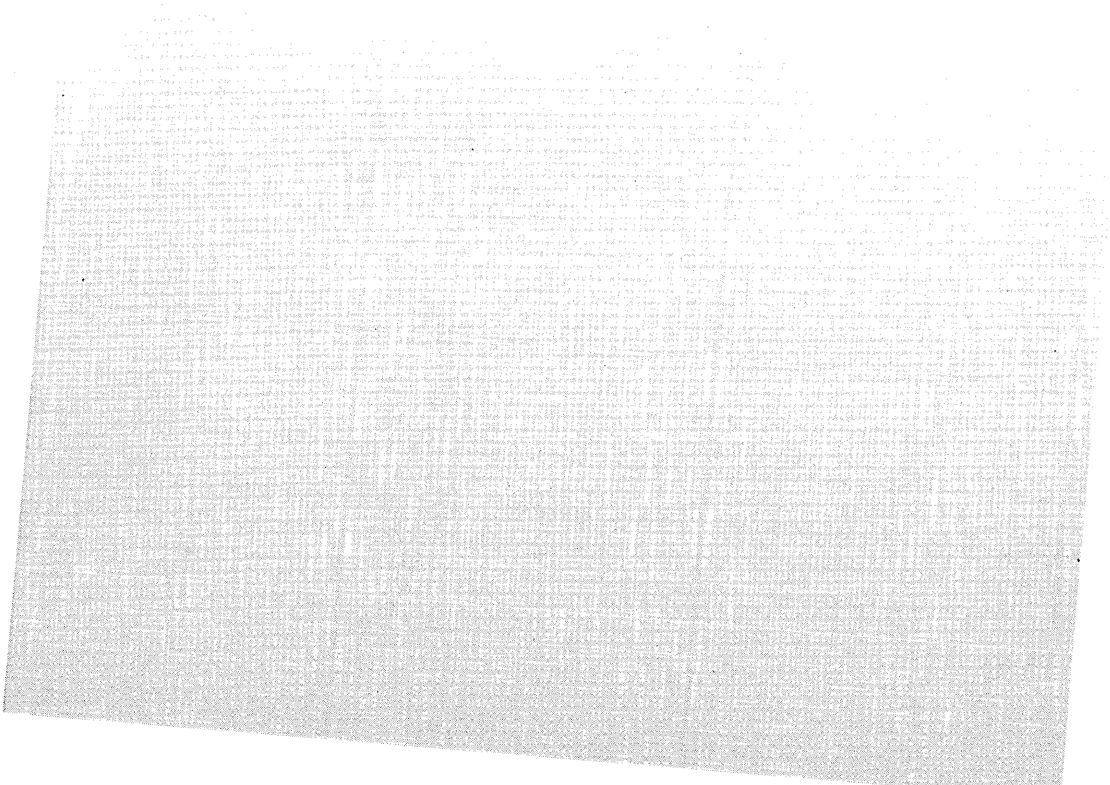
Chapter 13
Managing a Print Server 221

Chapter 14
Using Removable Storage 235

Chapter 15
Power Management 257

Chapter 16
Using Device Manager and Hardware Profiles 269





Chapter 12

Managing Disks

In This Chapter

Using Disk Management 197

Understanding Disk Terminology 201

Working with Basic Disks 205

Working with Dynamic Disks 211

Performing Other Tasks 213

Without disks, you have no way to save, recall, or archive your work. Disks, especially hard disks, are as essential to computer use as paper is to a library or bookstore. This chapter has little to do with saving data but everything to do with giving that data a congenial and well-designed home. It is about Disk Management, a tool that allows you to manage the space on your hard disks.

Using Disk Management

Disk Management is a Microsoft Management Console (MMC) snap-in that replaces the Disk Administrator program from Windows NT and the antediluvian Fdisk program from MS-DOS and Windows 9x. *For more information about MMC, see Chapter 4, "Using and Customizing Microsoft Management Console."* The purpose of Disk Management is to manage your hard disks, removable disks, and, to a lesser extent, your CD-ROM drives. You can use Disk Management to

- Create partitions, logical drives, and volumes
- Create spanned volumes and striped volumes—volumes that comprise disk regions from two or more disks
- Extend volumes to increase their size
- Format volumes

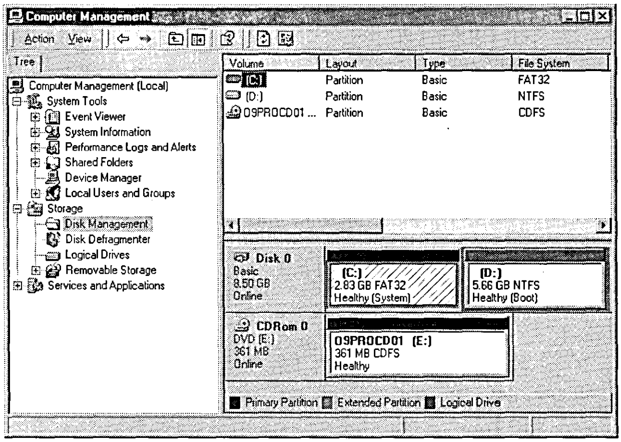
- Delete partitions, logical drives, and volumes
- Convert basic disks to dynamic disks, and vice versa
- Assign drive letters to hard disk volumes, removable disk drives, and CD-ROM drives
- Create mounted drives
- Check the size, format, status, and other properties of disks and volumes

One major improvement of Disk Management over its predecessors is that you no longer need to restart your computer after you make disk configuration changes. (And you don't need to fastidiously save your disk configuration, as you did with Windows NT; Disk Management does this automatically.) Of course, Disk Management still warns you if you ask it to do something destructive such as delete a partition or format a drive. But after you give your assent, Disk Management makes the changes immediately.

To use Disk Management, you must be logged on as a member of the Administrators group.

Starting Disk Management

The Disk Management snap-in is included in the Computer Management console, which you open by right-clicking My Computer and choosing Manage. (Alternatively, choose Start | Settings | Control Panel | Administrative Tools | Computer Management.) In Computer Management, navigate to Storage\Disk Management. Figure 12-1 shows an example.



Volume	Layout	Type	File System
(C:)	Partition	Basic	FAT32
(D:)	Partition	Basic	NTFS
09PROCD01 ...	Partition	Basic	CDFS

Disk 0
Basic
8.50 GB
Online

(C:)
2.83 GB FAT32
Healthy (System)

(D:)
5.66 GB NTFS
Healthy (Boot)

CDRom 0
DVD (E:)
361 MB
Online

09PROCD01 (E:)
361 MB CDFS
Healthy

Figure 12-1
The Disk Management snap-in is included in the Computer Management console.

Note Wondering about the other items under Storage in Computer Management? You'll find information elsewhere in this book. *For information about Disk Defragmenter, see Chapter 40, "Performing Routine Maintenance." For information about Removable Storage, see Chapter 14, "Using Removable Storage."* Logical Drives merely shows your drive mappings—information that can just as easily be gleaned from Windows Explorer or Disk Management.

If you prefer to see Disk Management without the distractions imposed by the Computer Management console, you can open it in its own window. Choose Start | Run, type *diskmgmt.msc,* and click OK. Throughout the rest of this chapter, we show this more focused form of the Disk Management console.

Using Disk Management to Manage Remote Computers

Starting Disk Management by using either of the preceding methods opens a window on your local computer's disk drives. You can also use Disk Management to view or modify the disks on any other computer on your network, as long as you log on as a member of that computer's Administrators group. You can open a Disk Management console on another computer in any of the following ways:

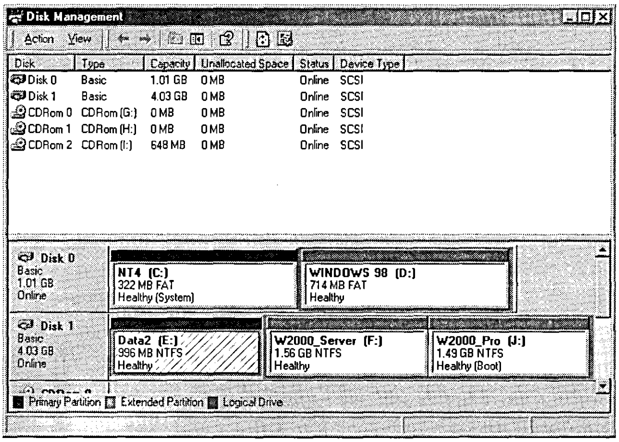
- In Computer Management, right-click Computer Management (Local)—the top item in the console tree—and choose Connect To Another Computer.
- Open Disk Management in author mode (choose Start | Run and type *diskmgmt.msc /a*) and click the Show/Hide Console Tree/Favorites toolbar button to display the console tree. Choose the Console | Add/Remove Snap-In command, click Add, select Disk Management, click Add, and select Another Computer. Specify the name of the computer you want. Using this method, you can add all your computers to a single console if you like.

Customizing the Display

You can modify the Disk Management display to suit your needs. First, decide what information you want to display. You can choose among three different display panels to include in the top portion and bottom portion of the details pane:

- **Disk List.** A detailed view of each physical disk drive in a computer, as shown at the top of Figure 12-2.
- **Volume List.** A detailed view of each volume (generally the same as lettered drives; *see "Volumes," page 203, for a more precise definition*) in a computer, as shown at the top of Figure 12-1.

- **Graphical View.** A view that shows each disk on one row, with the disk's volumes and unallocated space displayed graphically, as shown at the bottom of Figures 12-1 and 12-2.



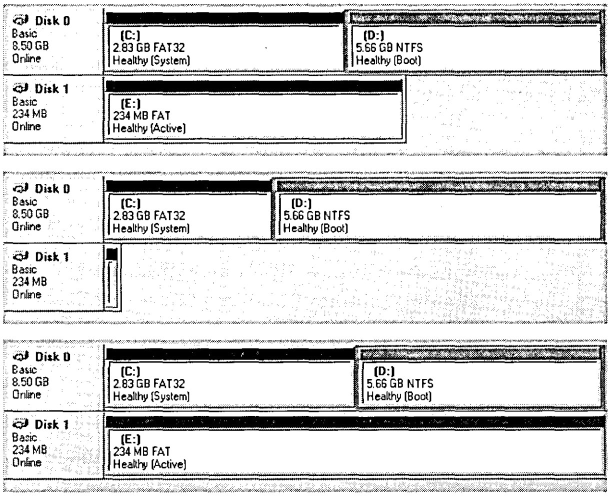
Disk	Type	Capacity	Unallocated Space	Status	Device Type
Disk 0	Basic	1.01 GB	0 MB	Online	SCSI
Disk 1	Basic	4.03 GB	0 MB	Online	SCSI
CDRom 0	CDRom (G:)	0 MB	0 MB	Online	SCSI
CDRom 1	CDRom (H:)	0 MB	0 MB	Online	SCSI
CDRom 2	CDRom (I:)	648 MB	0 MB	Online	SCSI

Figure 12-2
This console displays Disk List view at the top and Graphical View at the bottom.

To select one of these views, open the View menu and choose Top or Bottom; then choose the view name. The Bottom submenu also includes a Hidden command, which allows the top view to fill the entire details pane. Drag the border between the top and bottom if you want to reallocate the space allotted to each.

You can further customize the appearance of the Graphical View by choosing the View | Settings command. On the Appearance tab of the View Settings dialog box, for each type of disk region you specify a color and a pattern for the band across the top of its display.

On the Scaling tab of the View Settings dialog box, you specify the size of the boxes that represent disk regions. Your choice in the Disks box determines the relative overall display widths of each physical disk. Your choice in the Disk Regions box determines the relative display width of partitions, volumes, and other regions within the display space occupied by the disk. For each of these settings, you can opt to make all items equal in width, scale the items proportionally to their actual relative size (linear scaling), or use logarithmic scaling. The scaling that's most readable for you depends on the variance in disk and volume sizes on your computer. Figure 12-3 shows the effects of scaling settings on a system that has two disks: an 8.5-GB disk and an ancient 234-MB disk. As you can see, with this much size disparity, linear scaling is nearly useless.



Logarithmic scaling

Linear scaling

Same size

Figure 12-3
In each of these views, the Disks and Disks Regions scaling are set the same.

Understanding Disk Terminology

What appears in My Computer to be a hard disk drive might or might not correlate to a single physical device. A single physical device can be subdivided into partitions, volumes, or logical drives—each appearing in My Computer as a separate drive letter. Conversely, several physical devices (or portions thereof) can be combined to appear as a single drive letter. These configurations are described by the terms explained in this section. With support for dynamic disks, Windows 2000 adds some new terms to the lexicon and redefines others.

Let's start at the beginning: *disk* (or *hard disk*) refers to the physical hard disk drive installed in your computer. Your computer's first hard disk drive is identified in Disk Management as Disk 0. If you have additional hard disk drives installed, they're identified as Disk 1, Disk 2, and so on.

Basic Disks and Dynamic Disks

Windows 2000 now supports two types of disk structures, called basic disks and dynamic disks.

A *basic disk* is a physical disk that contains one or more partitions. The basic disk structure has been used by all versions of MS-DOS, Windows, and Windows NT; it is, therefore, the only disk type that is compatible with all these operating systems and with Windows 2000.

Similarly, a *dynamic disk* is a physical disk that contains one or more dynamic volumes. Dynamic disks are a new feature of Windows 2000, and they can't be accessed by earlier Microsoft operating systems. The advantage to dynamic disks is their flexibility:

- You can create an unlimited number of volumes on a disk. (With an extended partition on a basic disk, you can create an unlimited number of logical drives, but logical drives have limited capability. For example, you can't use a logical drive as a boot partition or system partition and you can't extend a logical drive.)
- Disk Management can modify the disk configuration in ways that it can't do with basic disks.
- Dynamic disks allow you to make disk configuration changes without rebooting your computer.
- Disk configuration information for dynamic disks is stored in a disk management database in a reserved area on the disk—not in the registry. This can make moving disks between computers and recovering data from corrupted disks easier.

Although these advantages—particularly the ability to make configuration changes without rebooting—are useful in servers for large enterprises, you must decide whether the benefits outweigh the need for compatibility with other operating systems. (By the way, just as Windows 9x computers on a network can access a shared NTFS volume, any type of computer can access across a network shared volumes on a dynamic disk.)

Your computer can have both types of disk, and the volumes on each disk can be formatted with any combination of NTFS and FAT file systems. Determining which kind you have is easy: in Disk Management, the Disk List view shows either Basic or Dynamic in the Type column, and the Graphical View shows the disk type just below the disk name.

Partitions and Logical Drives

A basic disk can be divided into one or more *partitions.* A section of the disk with its own starting and ending sector numbers, a partition is essentially a drive within a drive. Depending on the function it performs, a partition can be primary or extended; and it can be an active, system, or boot partition.

You can have up to four partitions per hard disk: four primary partitions, or three primary partitions and one extended partition.

A *primary partition* is one that can be used for starting Windows 2000 (and other operating systems). A primary partition cannot be further subdivided.

An *extended partition* can be further divided into one or more logical drives. This allows you to have more than four volumes on a basic disk. (From an end user's perspective, a *logical drive* is the same as a partition. At the Disk Management level, however, there is a difference: a logical drive can't span multiple disks.) You can create an extended partition on a disk that doesn't have any primary partitions, but you can't start Windows 2000 from such a disk.

Whereas primary and extended partitions refer to partition structure, active partition, system partition, and boot partition refer to content and functionality.

The *active partition* is the partition from which the computer starts up; to run Windows 2000 or other Microsoft operating systems, the active partition must be a system partition. A disk can have multiple system partitions, but only one can be marked active at any time. *For more information, see "Marking the Active Partition," page 208.*

The *system partition* contains the files needed to load Windows 2000 or another operating system. It must always be a primary partition, and it must be marked active if you want to start Windows 2000 or another operating system on the Windows 2000 boot menu. *For information about dual booting, see Chapter 3, "Working with Multiple Operating Systems."*

The *boot partition*, which sounds as though it ought to be the one you boot from, is actually the partition that contains the Windows 2000 system and support files—the files in the %SystemRoot% folder. If you run Windows 2000 from a single partition, the boot partition is, indeed, the same as the system partition. But you can install Windows 2000 to a partition other than the system partition.

Volumes

When a partition or logical drive is formatted for a particular file system (FAT or NTFS) and assigned a drive letter, it's called a *volume*. A volume appears in My Computer as a local disk.

A *basic volume* is a volume on a basic disk. Basic volumes include formatted primary partitions and formatted logical drives on extended partitions. (If you upgraded from Windows NT, you might also have volume sets or stripe sets—now called spanned volumes and striped volumes, respectively—on a basic disk. You can't create these types of volumes with Windows 2000, but you can continue to use them.)

A *dynamic volume* is a volume on a dynamic disk. On a computer running Windows 2000 Professional, Disk Management works with three types of dynamic volumes: simple volumes, spanned volumes, and striped volumes.

A *simple volume* is made up of space on a single disk. It can be a single region on a disk or several regions on the same disk that are linked together by a process called *extending* a volume.

A *spanned volume* is made up of space on two or more disks, which are linked together to appear as a single volume. A spanned volume is the dynamic-disk equivalent of a Windows NT volume set.

Similarly, a *striped volume* is made up of space on two or more disks (32 disks maximum). The difference is that data in a striped volume is allocated alternately to the equally sized regions on each disk in the striped volume. Striped volumes offer improved system performance by spreading the job of disk access across multiple read/write heads. Striped volumes are not quite as flexible as spanned volumes: the regions on each disk must be approximately the same size (therefore, the size of a striped volume is limited to the size of the unallocated space on the disk with the least unallocated space times the number of disks), and they can't be extended.

Fault-Tolerant Disk Storage with Windows 2000 Server

Microsoft Windows 2000 Server supports two additional volume types that allow the server to recover from disk failure or data loss: mirrored volume (formerly known as mirror set) and RAID-5 volume (formerly known as stripe set with parity). A *mirrored volume*, as its name implies, protects data by duplicating it on two disks so that if one of the disks fails, data can still be recovered from the "mirror image" on the other disk. A *RAID-5 volume* protects data by adding parity information and striping across three or more disks; the parity information can be used to recover the data if part of a stripe is lost when a disk fails.

Windows 2000 Professional doesn't support the use of fault-tolerant volumes on local disks. However, you can use Disk Management running on Windows 2000 Professional to create fault-tolerant volumes on a remote computer running Windows 2000 Server.

Mounted Drives

A *mounted drive* is a volume that is linked to a folder on an NTFS volume. In Windows Explorer and elsewhere, you navigate to it via the drive and folder to which it's linked instead of addressing it by a drive letter. (A mounted drive can also have a drive letter and can be mounted to more than one folder.)

With mounted drives, which are a new feature of Windows 2000, you're no longer limited to 26 drive letters.

You might see other terms in a discussion of mounted drives: *mount point, reparse point*, and *junction point* are all used to describe the file system object that links to another volume. In this book, we stick to *mounted drive*.

Adding a New Disk to Your Computer

You'll use Disk Management when you add a new disk to your computer—whether it's an additional disk for data or a disk you've moved from another computer. After you install the disk, you should open Disk Management and choose Rescan Disks from the Action menu.

New disks are added as basic disks. If you're adding a new disk for storage of data files (that is, it won't be used for an operating system), you should consider converting it to a dynamic disk before you create any partitions or volumes. By doing so, you can extend it later when you need even more storage space.

If you're installing a dynamic disk that you've moved from another computer, check the disk's status (in Disk List view or Graphical View); it should be Foreign. Right-click the disk and choose Import Foreign Disks. Windows 2000 then incorporates the disk's configuration information (which is stored at the end of each dynamic disk) into your computer's disk management database, thereby making the disk's existing volumes visible and accessible.

Working with Basic Disks

On basic disks, you can perform the following disk management tasks:

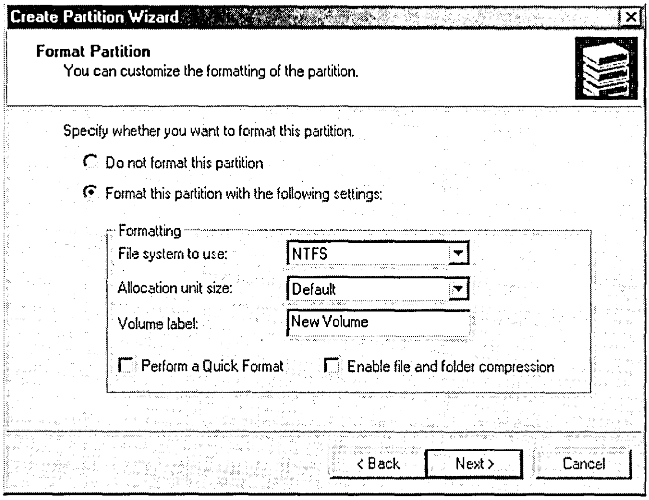
- Create primary and extended partitions
- Create logical drives in an extended partition
- Mark a partition as active
- Convert to a dynamic disk
- Other tasks that are described later in this chapter, including formatting a partition or logical drive; deleting a partition or logical drive, or volume sets and striped sets created with Windows NT; and assigning a drive letter or drive path *(for details, see "Performing Other Tasks," page 213.)*

Creating a Partition

To create a new partition, you need free—that is, unallocated—space on your hard disk. This space can belong to a portion of a new hard disk that you have not assigned to either a primary or an extended partition, or it can be space you make available by deleting an existing partition.

To create a primary partition (one that cannot be divided into multiple logical drives):

1. In Graphical View, right-click an unallocated portion of a disk and choose Create Partition.
2. In the Create Partition Wizard that appears, click Next.
3. On the Select Partition Type page, select Primary Partition and click Next.
4. On the Specify Partition Size page, specify how much of the unallocated space you want to use.
5. On the Assign Drive Letter Or Path page, you have three choices:
   - You can specify a drive letter for the partition. The list includes only drive letters that are not currently being used for local disks or for mapped network drives.
   - You can create a mounted drive, which appears as a subfolder of another drive. *For more information, see "Assigning a Drive Letter or Drive Path," page 215.*
   - You can choose not to specify a drive letter or path. If you choose this option, you won't be able to access the partition except in Disk Management. Before you can actually use the partition for storing and retrieving data, you need to assign a drive letter or create a mounted drive.
6. On the Format Partition page, make the following settings:
   - Choose a file system: NTFS, FAT, or FAT32. *For more information, see "Selecting a File System," page 539.*
   - Choose an allocation unit size, or cluster size. The allocation unit size is the smallest space that can be allocated to a file. Smaller sizes result in less wasted disk space (because on average, every file has slack space equal to half a cluster) but can result in more fragmentation. Unless the partition is dedicated to a special purpose (such as storage of a large database), using the Default selection, in which Windows 2000 selects a cluster size based on volume size, is best.
   - Specify a volume label. The volume label appears in Windows Explorer, and the novelty of the default label, New Volume, quickly wears off.
   - Select Perform A Quick Format if you merely want Disk Management to set up the volume structure but not scan the data area of the volume.
   - Select Enable File And Folder Compression if you want to squeeze more data on a volume (available only if you select the NTFS file system).



Create Partition Wizard

Format Partition
You can customize the formatting of the partition.

Specify whether you want to format this partition.

○ Do not format this partition

● Format this partition with the following settings:

Formatting

File system to use: NTFS

Allocation unit size: Default

Volume label: New Volume

□ Perform a Quick Format □ Enable file and folder compression

7. Click Next, confirm your settings, and click Finish.

Note Many of the settings you make in the Create Partition Wizard can be changed at any time later, as described elsewhere in this book. Specifically, you can

- Assign a different drive letter or create a mounted drive
- Convert a FAT- or FAT32-formatted volume to NTFS
- Change the volume label
- Enable file and folder compression

If your hard disk contains no more than three primary partitions, you can create an extended partition in the remaining space. The main benefit of an extended partition is its ability to support more than one logical drive.

To create an extended partition:

1. In Graphical View, right-click an unallocated portion of a disk and choose Create Partition.
2. In the Create Partition Wizard that appears, click Next.
3. On the Select Partition Type page, select Extended Partition and click Next. (This option is available only if the disk doesn't already have an extended partition.)
4. On the Specify Partition Size page, specify how much of the unallocated space you want to use.
5. Click Next, confirm your settings, and click Finish.

After you create an extended partition, you must define one or more logical drives within it, as explained in the following section.

Creating a Logical Drive

A logical drive is a part of an extended partition that you "wall off" and format so that you can use it as if it were a truly separate disk drive. Creating a logical drive is very similar to creating a new partition.

To create a logical drive:

1. In Graphical View, right-click the free space within an extended partition and choose Create Logical Drive.
2. In the Create Partition Wizard that appears, click Next two times. (Why the wizard doesn't skip the Select Partition Type page, nobody knows.)
3. On the remaining wizard pages, specify the size, drive letter or path, and format—just as you would for a primary partition, as described in the previous section.

Marking the Active Partition

The active partition on a basic disk is the one from which an x86-based computer boots. On these machines, one primary partition—the one containing the files needed for startup—must be marked active for the computer to start itself and an operating system. The active partition must always be on the first hard disk attached to the system (Disk 0).

If you use Windows 2000 exclusively, or if you use Windows 2000 and Windows NT, Windows 9x, or MS-DOS, you do not have to change the active partition. In fact, Disk Management won't let you. However, if you use another operating system, such as OS/2, you must mark its system partition as active and reboot in order to use the alternate operating system.

To mark the active partition and start a different operating system:

1. In the Volume List view or Graphical View, right-click the partition you want to mark active and choose Mark Partition Active.
2. Reboot the computer.

Converting a Basic Disk to a Dynamic Disk

On a basic disk, the partition table—information about the partitions on the disk—is located in a 64-byte section of the MBR (master boot record), the first sector on the disk. A dynamic disk keeps additional information about the disk's layout in a disk management database that is stored in the last 1 MB of the disk. You might have noticed (if you created one or more partitions during setup) that the Windows 2000 setup program refuses to use the entire unallocated space on the disk. Instead, it reserves space for the disk management database, which is needed if you convert the basic disk to a dynamic disk.

Disk Management makes converting a basic disk to a dynamic disk easy. You should do that if you run only Windows 2000, you have more than one disk, and one or more of the following is true:

- You want to use more than four volumes on a disk.
- You want to extend a volume onto unused space on the same disk or another disk.
- You want to create a striped volume.

Note

> Although Windows 2000 supports the continued use of volume sets and stripe sets that were created with Windows NT, you can't create them. If you want this functionality in Windows 2000 (and your basic disk isn't already configured that way), you must use spanned volumes or striped volumes, which can be created only on dynamic disks.

On the other hand, you should use basic disks if your computer also runs another operating system. Only Windows 2000 can access dynamic volumes.

Before you convert, you should be aware of these additional limitations of dynamic volumes:

- You can't use dynamic disks on a portable computer. *(For more information, see Microsoft Knowledge Base [KB] article Q232463. KB articles are available at* support.microsoft.com.*)*
- If you create a dynamic volume from unallocated space on a dynamic disk, you can't install Windows 2000 to that volume. (Of course, to get this far, you must already have Windows 2000 installed, so this limitation comes into play only if you're reinstalling Windows 2000 or moving the disk to another computer.)
- You can't extend a dynamic volume that was a basic volume before the dynamic disk upgrade.

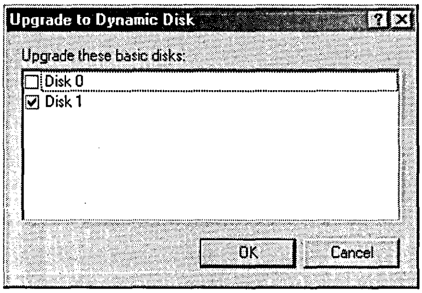
Taken together, these last two limitations mean that you can't extend the system volume or boot volume. For that reason—and for compatibility purposes—we recommend the following:

- Install Windows 2000 on your first hard disk and leave it as a basic disk. If you plan to dual boot with another operating system, partition the first disk so that each operating system is on a separate partition. *(For more explanation, see Chapter 3, "Working with Multiple Operating Systems.")*

- Use additional disks for data. But before you partition them or store anything on them, convert them to dynamic disks. That way, you can easily extend your data volumes, which might come in handy when your collection of MP3 files (or whatever) fills your first data disk.

To convert a basic disk to a dynamic disk:

1. Close any programs (other than Disk Management) that are using the disk you're converting.
2. In Disk List view or Graphical View, right-click the disk you want to convert and choose Upgrade To Dynamic Disk.
3. If you have more than one disk, select which one(s) you want to upgrade and click OK.

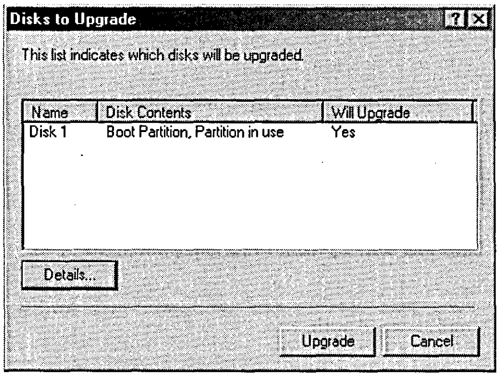


Upgrade to Dynamic Disk

Upgrade these basic disks:

☐ Disk 0
☑ Disk 1

4. In the Disks To Upgrade dialog box, click Upgrade.



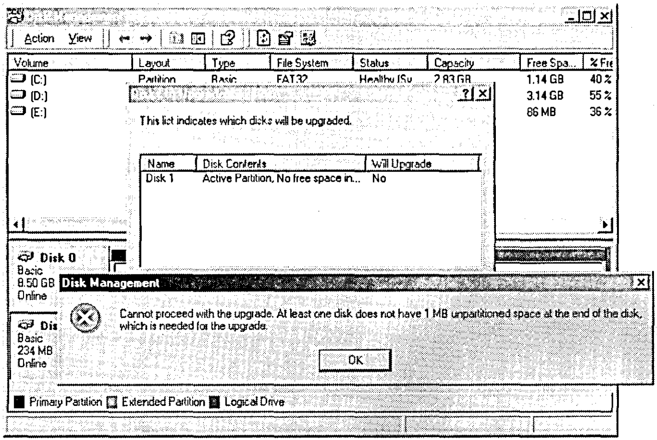
Disks to Upgrade

This list indicates which disks will be upgraded.

Name	Disk Contents	Will Upgrade
Disk 1	Boot Partition, Partition in use	Yes

Troubleshooting

You can't convert a basic disk to a dynamic disk unless at least 1 MB of unallocated space exists at the end of the disk. If you use Windows 2000 to create partitions (either during setup or with Disk Management), it automatically reserves that space. But if you're using a disk that was partitioned with an earlier operating system, you might see an error message like the one shown in the following illustration:



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Fre
(C:)	Partition	Basic	FAT32	Healthy (Sy	2.83 GB	1.14 GB	40 %
(D:)						3.14 GB	55 %
(E:)						86 MB	36 %

This list indicates which disks will be upgraded.

Name	Disk Contents	Will Upgrade
Disk 1	Active Partition, No free space in...	No

Disk Management

Cannot proceed with the upgrade. At least one disk does not have 1 MB unpartitioned space at the end of the disk, which is needed for the upgrade.

If you want to upgrade to dynamic disks, you must delete the last partition, which will destroy all the data it contains. (You can re-create the partition with Disk Management before or after you convert to dynamic disk, but you can't recover any destroyed data.) Alternatively, you might be able to resize the last partition with third-party software such as PartitionMagic or System Commander.

Working with Dynamic Disks

On dynamic disks, you can perform the following disk management tasks:

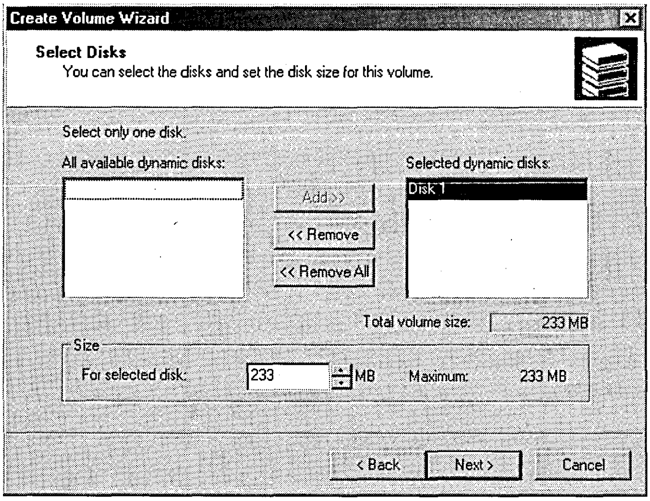
- Create a simple volume, spanned volume, or striped volume
- Extend a simple volume or spanned volume
- Convert to a basic disk
- Other tasks that are described later in this chapter, including formatting a volume, deleting a volume, and assigning a drive letter or drive path for a volume *(For details, see "Performing Other Tasks," page 213.)*

Creating a Volume

The process of creating a volume on a dynamic disk is quite similar to that of creating a partition on a basic disk. As in that procedure, a wizard guides you through the process.

To create a volume:

1. In Graphical View, right-click an unallocated portion of a disk and choose Create Volume.
2. In the Create Volume Wizard that appears, click Next.
3. On the Select Volume Type page, select a type: Simple Volume, Spanned Volume, or Striped Volume. (If you have only one dynamic disk, Simple Volume is your only choice.) *For information about these types, see "Volumes," page 203.* Consider your needs: simple and spanned volumes can be extended (onto the same disk or other disks) in the future; striped volumes offer better performance.
4. On the Select Disks page, select which disks you want to use by placing them in the Selected Dynamic Disks list. (If you're creating a simple volume, you can select only one disk.) Then specify how much of the unallocated space you want to use.



Create Volume Wizard

Select Disks
You can select the disks and set the disk size for this volume.

Select only one disk.

All available dynamic disks:

Selected dynamic disks:
Disk 1

Total volume size: 233 MB

Size
For selected disk: 233 MB
Maximum: 233 MB

5. On the remaining wizard pages, specify the drive letter or path and format—just as you would for a primary partition. *For details, see "Creating a Partition," page 205.*

Extending a Volume

If you have additional unallocated space on a dynamic disk—either the same disk or another disk—you can extend an existing volume to increase its size. You can do so, that is, subject to the following limitations:

- You can extend only simple volumes and spanned volumes on dynamic disks; you can't extend striped volumes or volumes on basic disks.
- You can extend a volume only if it's formatted with NTFS or it's unformatted; you can't extend FAT or FAT32 volumes.
- You can extend a volume only if it was originally created on a dynamic disk; you can't extend volumes that have been upgraded from basic to dynamic.
- You can't extend a system volume or boot volume.

Still with us? To extend a volume:

1. In Volume List view or Graphical View, right-click the volume you want to extend and choose Extend Volume.
2. In the Extend Volume Wizard that appears, click Next.
3. On the Select Disks page, select which disks you want to use by placing them in the Selected Dynamic Disks list. You can extend a simple volume to use unallocated space on the same disk or on another disk. (In the latter case, it becomes a spanned volume.) Then specify how much of the unallocated space you want to use.
4. Click Next and then click Finish.

After a volume is extended, you can't reduce its size—except by deleting the entire volume.

Converting a Dynamic Disk to a Basic Disk

Remember how easy it was to convert a basic disk to a dynamic disk? Disk Management left all your existing data in place. Unfortunately, the conversion back to basic is not so pleasant. To convert a dynamic disk to basic, you must first delete all volumes on the dynamic disk, destroying all your data in the process. *For details, see "Deleting a Partition, Logical Drive, or Volume," page 214.*

After you've deleted the volumes (presumably after backing up your data to another medium or copying it to a drive available through a network), the conversion process is simple. In Disk List view or Graphical View, right-click the disk you want to convert and choose Revert To Basic Disk.

Performing Other Tasks

This section describes tasks that you can perform on basic disks and dynamic disks:

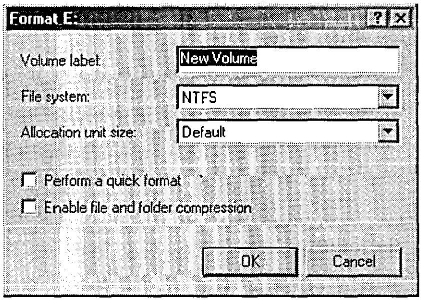
- Formatting a partition, logical drive, or volume
- Deleting a partition, logical drive, or volume
- Assigning or changing a volume label

- Assigning a drive letter or drive path
- Checking properties and status for a disk or volume

Some of these disk management tasks also apply to removable disks (such as Zip disks and CDs). For example, you can use Disk Management to format a Zip disk (although there's no particular reason to, because you can also format from other programs that you're more likely to have open: Windows Explorer or a command prompt). More important, you use Disk Management to assign drive letters (or drive paths for mounted drives, if you prefer) for all types of drives—and you can't do that elsewhere.

Formatting a Partition, Logical Drive, or Volume

Formatting a partition, logical drive, or volume deletes any existing files and prepares the volume for use. You can let the Create Partition Wizard or Create Volume Wizard format a partition, logical drive, or volume when you create it, or you can format it any time later by right-clicking the volume and choosing Format. You'll see a dialog box that offers the same choices as the wizard, as shown in Figure 12-4.


Format E:

Volume label: New Volume

File system: NTFS

Allocation unit size: Default

□ Perform a quick format

□ Enable file and folder compression

Figure 12-4
Formatting without the wizard offers the same choices.

Note Windows 2000 will not let you format the system volume or boot volume.

Of course, you don't need to visit Disk Management to format an existing volume. You can do that from Windows Explorer, where you'll see yet another dialog box that offers the same options and performs the same task. Or if you're a command-prompt fan, use the Format command.

Deleting a Partition, Logical Drive, or Volume

The most important thing to know about deleting a partition, logical drive, or volume is this: *All information in the partition, drive, or volume will be irrevocably lost.* The only time you should consider deleting a partition, drive, or volume is when you want to reorganize a disk and are certain that all important programs and data have been backed up to another medium. Deleting means starting over.

Deleting a spanned volume (known as a volume set in Windows NT) or striped volume (stripe set) deletes the entire volume. That is, all disk regions on all disks that are part of the volume become unallocated space.

Windows 2000 will not allow you to delete the system partition, the boot partition, or an extended partition that contains logical drives. (You must delete the logical drives first and then delete the partition.)

To delete a partition, logical drive, or volume:

1. Verify that all needed files have been backed up.
2. In Graphical View, right-click the item you want to delete and choose Delete Partition, Delete Logical Drive, or Delete Volume.
3. After reassuring yourself that the item you selected contains no data you'll need again, click Yes in the confirmation dialog box.

Note Don't delete a volume if all you want to do is change its file system. If you want to change from FAT to NTFS, you can use the Convert command at a command prompt. This command converts the volume without destroying its contents. *For details, see "Converting a Volume to NTFS," page 542.*

If you want to change from NTFS to FAT, you must use a third-party program such as Partition Magic (*www.powerquest.com*) or System Commander (*www.v-com.com*).

Assigning or Changing a Volume Label

If you choose not to assign a volume label when you create or format a volume, or if you later decide to change a volume label to a more descriptive one, you can do so by right-clicking a volume and choosing Properties. (You can also do this in Windows Explorer.) Use the Label box on the General tab.

The volume label on a FAT (or FAT32) volume can be up to 11 characters long and can include spaces. Whether you type uppercase or lowercase letters, the volume label is stored in uppercase letters only. A FAT volume label cannot include the following characters:

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

Only one restriction applies when you assign a volume label for an NTFS volume: the maximum length is 32 characters. You can use any symbols you want, and uppercase and lowercase letters are retained (and displayed) exactly as you type them.

Assigning a Drive Letter or Drive Path

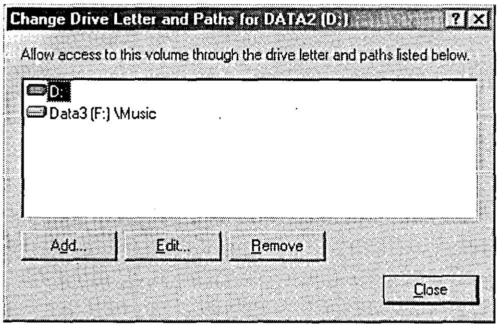
Drive letter assignments in Windows 2000 are persistent, which means that, once assigned, the assignments remain the same every time you start Windows 2000. But how does Windows 2000 initially parcel out the letters? The algorithm is rather complex, and it depends on how you initially installed Windows 2000 (upgrade or clean install; if upgrade, from which operating system; and so on), the types of disks, partitions, and volumes you have; and other factors. (For details, see KB article Q234048.)

You can change the assigned drive letters, which you might want to do if, for example, a system-assigned drive letter interferes with a mapped network drive.

A volume can have only one drive letter (or no drive letter at all), but you can also assign one or more drive paths to create one or more mounted drives. A mounted drive appears as a folder within another volume, which allows you to access a volume without reserving a drive letter for it—thereby getting past the limit of 26 drive letters. For example, you might remove the drive letter assignment for your CD-ROM drive and instead mount it to a folder on drive C called CD. You would then find a CD's contents in C:\CD rather than in D:\ (or whatever the previous drive letter assignment was).

To assign a drive letter:

1. In Volume List view or Graphical View, right-click the volume you want to change and choose Change Drive Letter And Path.



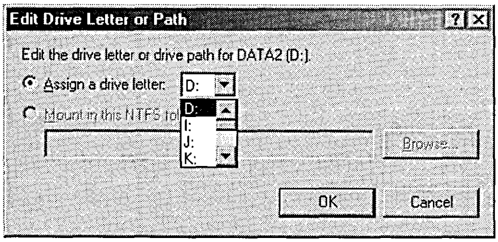
Change Drive Letter and Paths for DATA2 (D:)

Allow access to this volume through the drive letter and paths listed below.

D:

Data3 (F:) \Music

2. To change an existing drive letter, select it and click Edit. To assign a drive letter if one isn't currently assigned, click Add.



Edit Drive Letter or Path

Edit the drive letter or drive path for DATA2 (D:).

● Assign a drive letter: D:

○ Mount in this NTFS fol

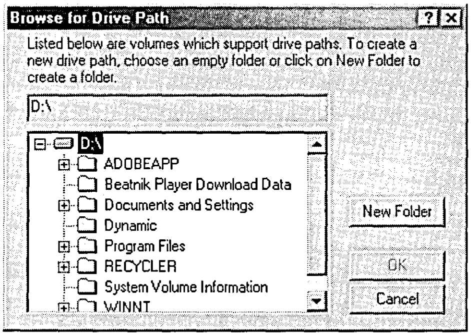
D:
I:
J:
K:

3. Select a drive letter, click OK, and click Close.

Note You can't change the drive letter of the system volume with Disk Management. If you really need to do this—which is unlikely—KB article Q223188 explains the procedure.

To create a mounted drive:

1. In Volume List view or Graphical View, right-click the volume you want to change and choose Change Drive Letter And Path.
2. Click Add. (You can't edit an existing drive path. If you want to change one, you must delete it—select it and click Remove—and then create a new one.)
3. Select Mount In This NTFS Folder and then type the path to an empty folder on an NTFS volume. Easier yet, click Browse. (Browsing is not available on remote volumes.) The Browse For Drive Path dialog box that appears shows only your NTFS volumes, and the OK button is enabled only if you select an empty folder. Select an empty folder or click New Folder to create one.



Browse for Drive Path

Listed below are volumes which support drive paths. To create a new drive path, choose an empty folder or click on New Folder to create a folder.

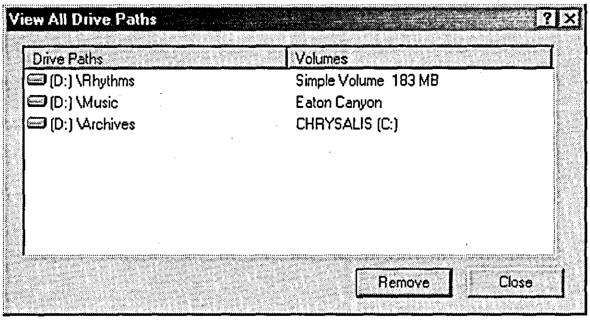
D:\

The folder you specify appears in Windows Explorer as a drive icon, not a folder icon. Opening that icon displays the root folder of the mounted drive.

Note Although the folder in which you mount a drive must be an empty folder on an NTFS volume, the volume you're mounting can be formatted with any file system.

Note Be careful to avoid creating a loop in the namespace (for example, by mounting a volume to a folder on a second volume and then mounting the second volume to a folder on the first volume). Windows lets you do this, but it's usually a bad idea because an application that opens subfolders (such as a search) will go into an endless loop.

To see a list of all the mounted drives on your system, open the View menu and choose All Drive Paths. A dialog box like the one shown in Figure 12-5 appears.



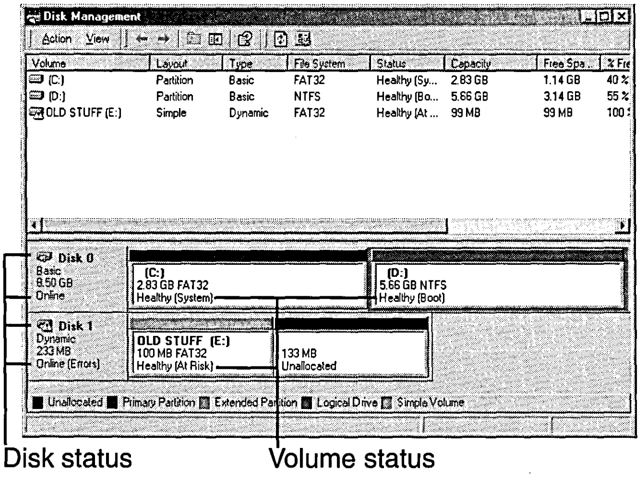
Drive Paths	Volumes
(D:) \Rhythms	Simple Volume 183 MB
(D:) \Music	Eaton Canyon
(D:) \Archives	CHRYSALIS (C:)

Figure 12-5
This dialog box lists all the mounted drives on a system and shows the volume label, if any, of the mounted drive.

Checking Properties and Status

Like most objects in Windows 2000, disks and volumes have a properties dialog box that provides details about the object. To view it, right-click the object and choose Properties. The properties dialog box for a volume is the same as the one you would see by viewing the same volume's properties dialog box in Windows Explorer.

But you needn't visit the properties dialog box to learn a lot about your disks and volumes. Most of the key information—disk type, volume type, file system, capacity, and status—is visible in both the list and graphical views. Of particular interest is the status, which is helpful if you have problems with a disk or volume. Figure 12-6 shows where you can find status information. Table 12-1 describes the possible status conditions for disks, and Table 12-2 describes volume status conditions.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Fre
(C:)	Partition	Basic	FAT32	Healthy (Sy...	2.83 GB	1.14 GB	40 %
(D:)	Partition	Basic	NTFS	Healthy (Bo...	5.66 GB	3.14 GB	55 %
OLD STUFF (E:)	Simple	Dynamic	FAT32	Healthy (At ...	99 MB	99 MB	100 :

Figure 12-6
Volume List view (shown here) and Disk List view both include a Status column, and Graphical View also indicates status.

Table 12-1. Disk Status

Status	Description	Action Required
Online	This is the normal status, and it means that the disk has no known problems.	None
Online (Errors)	This status, which can appear only on dynamic disks, indicates that I/O errors have occurred.	Right-click the disk and choose Reactivate Disk.
Offline	This status, which can appear only on dynamic disks, indicates that the	Check to see that the disk is not powered disk was once available
but is not	down or disconnected. currently accessible. The disk might be corrupt.	
Foreign	This status, which can appear only on dynamic disks, indicates that the disk has been moved to your computer from another computer and it hasn't yet been set up for use on your computer.	Right-click the disk and choose Import Foreign Disks.
Unreadable	The disk is inaccessible and might be corrupt or have I/O errors. The disk management database may be corrupt.	Right-click the disk and choose Rescan Disks, or reboot the computer. If the status is still unreadable, the disk is probably unrecoverable.
Unrecognized	The disk has a signature that prevents Disk Management from using the disk; disks from UNIX systems display this status.	Nothing you can do.
No Media	This status, which appears only for CD-ROM drives or removable media drives (for example, Zip drives), indicates that no disk is in the drive.	Insert a disk in the drive.

Table 12-2. Volume Status

Status	Description	Action Required
Healthy	This is the normal status and means that the volume has no known problems.	None.
Healthy (At Risk)	This status, which can appear only on dynamic volumes, indicates that I/O errors have occurred on the underlying disk. If an I/O error occurs anywhere on the disk, all the disk's volumes are marked Healthy (At Risk).	Right-click the disk and choose Reactivate Disk.
Initializing	This status, which can appear only on dynamic volumes, indicates that the disk is initializing.	Relax! Wait a few seconds.
Failed	This status indicates that the volume can't be initialized.	To repair a failed dynamic volume, checkto see whether the disk is Online. (If not, right-click the disk and choose Reactivate Disk.) Then right-click the volume and choose Reactivate Volume. If the failed volume is on a basic disk, be sure that the disk is properly connected.

Note Other volume status conditions—Resynching, Regenerating, Failed Redundancy, and Failed Redundancy (At Risk)—can appear only on fault-tolerant volumes, which are not supported in Windows 2000 Professional (and are therefore not described in this book). If you're managing mirrored volumes or RAID-5 volumes on a remote computer running Windows 2000 Server, check the online help for more information.

Chapter 13

Managing a Print Server

In This Chapter

Sharing a Printer 221
Setting Printer Permissions 223
Setting Advanced Printer Properties 224
Using Separator Pages 227
Setting Up a Printer That's Connected Directly to the Network 228
Setting Up a Printer for Non–Windows 2000 Clients 229
Setting Server Properties 232

With Plug and Play, an improved and more powerful Print dialog box, and better printer drivers, Microsoft Windows 2000 has greatly simplified the tasks of installing, configuring, and using a local printer. So much so, in fact, that we don't cover those topics in this book at all. You'll find information on those topics in our other book, *Running Microsoft Windows 2000 Professional* (Microsoft Press, 2000).

Instead, this chapter focuses on setting up a print server—a computer that manages the printers on a network. In the same way that you can share folders on a computer running Windows 2000 Professional to create a file server, you can share printers to create a print server. You don't need Windows 2000 Server to share and manage printers so that everyone on the network has access to them. This chapter discusses the printer configuration options that you're more likely to use with shared printers.

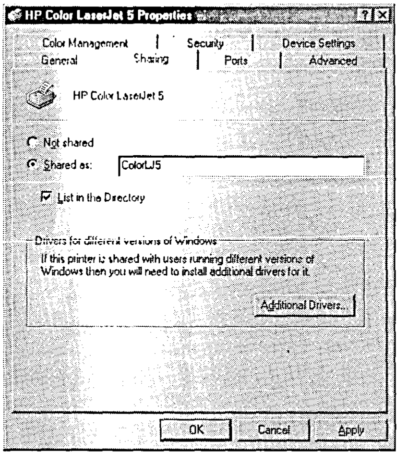
Sharing a Printer

You configure all options for a printer—whether you plan to share it or not—using the printer's properties dialog box. To display it, open the Printers folder (Start | Settings | Printers), right-click the printer you're interested in, and choose Properties.

To make a printer available to other network users, simply click the Sharing tab, select Shared As, and provide a share name. Windows 2000 permits spaces and other characters in printer names, but if you're going to share with users of other operating systems, you should observe the following restrictions:

- Use only letters and numbers; don't use spaces, punctuation, or special characters.
- The entire universal naming convention (UNC) name, including the requisite backslashes and your computer name, should be 31 or fewer characters. For example, assume that your computer name is YELLOWSTONE (11 characters). When you add slashes, the length becomes 14 characters, meaning that the share name should be 17 characters or less. This results in a UNC name something like \\YELLOWSTONE\HPLASERJET4000.
- If any MS-DOS users will connect to the printer;·the share name must be no longer than 8 characters.

If your computer is part of a Windows 2000 domain that uses Active Directory, select List In The Directory (see Figure 13-1) to publish the printer in the directory, which makes finding your printer easier for others.



○ Not shared

● Shared as: ColorLJ5

☑ List in the Directory

If this printer is shared with users running different versions of Windows then you will need to install additional drivers for it.

Figure 13-1
On the Sharing tab, specify a share name and, if you're on a Windows 2000 Server domain, decide whether you want the printer included in the Active Directory.

Troubleshooting

If other network users can't find your shared printer, check to be sure that you've enabled printer sharing. In the Network And Dial-Up Connections folder, right-click the Local Area Connection icon and choose Properties. On the General tab, select File And Printer Sharing For Microsoft Networks.

Troubleshooting

If you have problems installing a driver for a shared printer that's connected to a different print server (this sometimes happens with Windows NT–based print servers), install the printer as a local printer rather than as a network printer. "Connect" it to an unused port on your system, such as LPT3. Then, at a command prompt, type *net use lpt3 \\server\share /persistent:yes* (replace *server* with the computer name of the print server and replace *share* with the name of the shared printer) to redirect output to the network printer. It's messy, but it works.

Setting Printer Permissions

When you set up a printer, initially all users in the Everyone group have Print permission for documents they create, which provides access to the printer and the ability to manage their own documents in the print queue. And by default, members of the Administrators and Power Users groups also have Manage Printers and Manage Documents permission. Table 13-1 shows the basic permissions and their associated privileges that Windows 2000 provides for printers.

Table 13-1. Basic Printer Permissions and Privileges

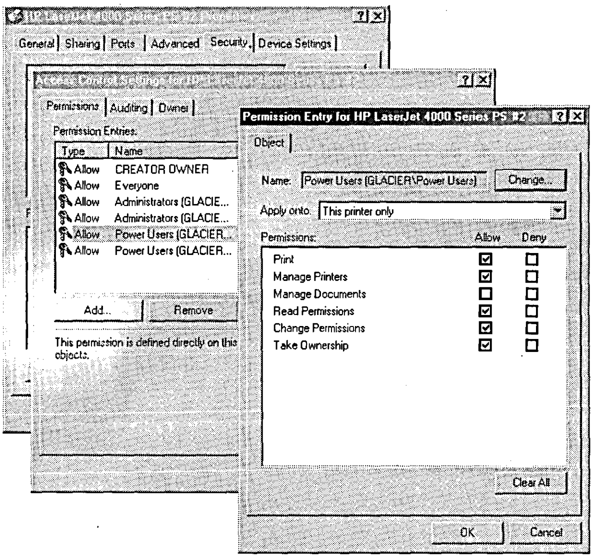
Permission	Privileges
Print	Print documents
	Control properties of owned documents
	Pause, restart, and remove owned documents
Manage Printers	Share printer
	Change printer properties
	Remove printer
	Change printer permissions
	Pause and restart the printer
Manage Documents	Pause, restart, move, and remove all queued documents

A user account that doesn't have any of these permissions can't connect to the printer, print to it locally, or view its queue.

If you have Manage Printers permission for a printer, you can change other users' permissions for that printer. To do so, click the Security tab of the printer's properties dialog box. To add another user or group to the list, click Add. After you select the users or groups you want in the Select Users, Computers, Or Groups dialog box, return to the printer's properties dialog box. Then select each new user or group and assign permissions by clicking Allow, Deny, or neither. (If you select neither, permissions are determined by the user's group membership.)

Permissions on the Security tab apply to users who log on locally as well as those who connect via network to a shared printer.

Clicking Advanced on the Security tab leads to an access control settings dialog box (the center dialog box shown in Figure 13-2). From there, you can select an entry and click View/Edit to display the permission entry dialog box shown in the foreground. As you can see, this dialog box gives you granular control over printer permissions: for a particular user or group, you can apply permissions to the printer, to documents, or to both; and you can set a few individual permissions that are encompassed in the basic permissions. Although this might be fun for tweaking, you'll seldom have any reason to visit these dialog boxes; we present them here so that you'll never have to go there.



Permission Entries:

Type	Name
Allow	CREATOR OWNER
Allow	Everyone
Allow	Administrators (GLACIE...
Allow	Administrators (GLACIE...
Allow	Power Users (GLACIER...
Allow	Power Users (GLACIER...

This permission is defined directly on this objects.

Name: Power Users (GLACIER\Power Users)

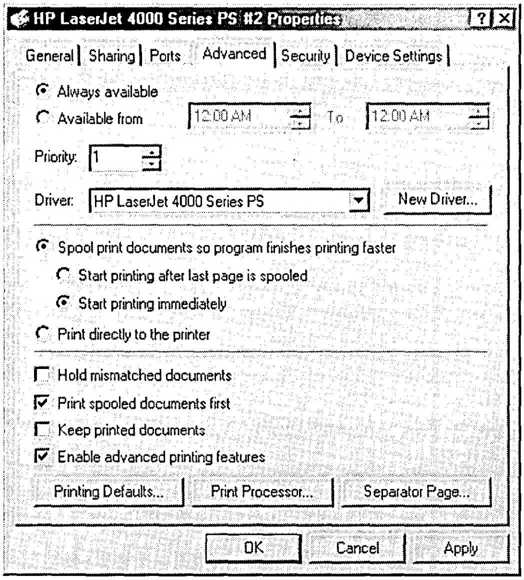
Apply onto: This printer only

Permissions:	Allow	Deny
Print	☑	□
Manage Printers	☑	□
Manage Documents	□	□
Read Permissions	☑	□
Change Permissions	☑	□
Take Ownership	☑	□

Figure 13-2
Advanced security settings give you granular control over permissions—something you'll probably never need.

Setting Advanced Printer Properties

The Advanced tab of the printer's properties dialog box, shown in Figure 13-3, includes a number of options that are both intriguing and confusing. Making changes to these options requires Manage Printers permission.



● Always available

○ Available from 12:00 AM To 12:00 AM

Priority: 1

Driver: HP LaserJet 4000 Series PS

● Spool print documents so program finishes printing faster

○ Start printing after last page is spooled

● Start printing immediately

○ Print directly to the printer

☐ Hold mismatched documents

☑ Print spooled documents first

☐ Keep printed documents

☑ Enable advanced printing features

Figure 13-3
The Advanced tab offers a collection of unrelated options.

- **Always Available** and **Available From.** To restrict the availability of the printer to certain times of day, select Available From and specify the range of times. Print jobs that are sent outside of these hours are held in the queue until the appointed time. One possible use: you might want to create a printer (remember that you can create multiple logical printers for a single print device) that you use only for low-priority, long print jobs, which could be queued to run at night instead of tying up the printer during working hours.
- **Priority.** The Priority setting has a similar purpose: if you create multiple printers for a single print device, documents sent to the printer with the higher Priority setting print ahead of those sent to the other printer. You might want to create a high-priority printer that certain users have permission to use when they need to cut in line to get a document printed quickly. Or you might want to assign Print permission to the high-priority printer to one group of users, and permission to the lower-priority printer to another group of users with different (less urgent) needs.
- **Driver.** This list includes all the printer drivers currently installed on your system; use it to select the correct driver for the print device. If the correct driver isn't in the list, click New Driver to launch the Add Printer Driver Wizard.

- **Spool settings.** The four option buttons in the center of the dialog box determine whether a document should be spooled to a hard disk before sending it to the printer. *For information about specifying the location of spool files, see "Setting Server Properties," page 232.* Spooled documents are then sent to the print device in the background. Ordinarily, you should select the first and third options, which cause fastest return of control to your application and fastest printing completion. But if you have trouble with complex print jobs being interrupted by pages from another document, select Start Printing After Last Page Is Spooled.
- **Hold Mismatched Documents.** Selecting this option tells the spooler to check a document's properties against the printer properties and to hold the document in the queue if the properties don't match. A mismatched document typically occurs when an application specifies a form that's not currently assigned to a printer tray, for example. Correctly matched documents continue to print normally, bypassing any mismatched documents in the queue.
- **Print Spooled Documents First.** Selecting this option directs the spooler to print documents that have completed spooling ahead of documents that are still spooling, even if the latter documents have a higher priority. When this option is cleared, the spooler selects the next document to print based only on its priority. Selecting this option maximizes printer efficiency because the print device doesn't have to wait for an incomplete, high-priority document to finish spooling before it can begin printing a complete, lower-priority document.
- **Keep Printed Documents.** When this option is selected, the spooler doesn't delete documents from the queue after they print. You can then reprint a document from the queue rather than from the program that created it, or you can delete the document manually.
- **Enable Advanced Printing Features.** Selecting this option turns on metafile spooling for print jobs from Windows 2000 clients using Windows-based applications. Of more interest to most users, selecting this option enables new options in the common Print dialog box for some printers and some applications, such as Booklet Printing and Pages Per Sheet. The only reason to clear this option is if you have problems printing.
- **Printing Defaults.** Clicking this button displays the printing defaults dialog box—the same one that appears if you right-click a printer and choose Printing Preferences. In this dialog box, you specify default document settings for options such as orientation, two-sided printing, paper tray selection, and so on. Your settings here become the default settings for all users of the printer. (Another reason to create multiple logical printers for a single device: you might want to create printers with different default settings for different types of documents or for users with different needs.)

- **Print Processor.** Clicking this button opens the Print Processor dialog box, a place you'll probably never need to venture. In a nutshell, it displays the available print processors (a *print processor* tells the spooler how to alter a print job depending on the document data type) and the default datatype for the selected print processor. The *Microsoft Windows 2000 Server Resource Kit* provides detailed information about print processors and datatypes.
- **Separator Page.** Click this button to specify a separator page. *For more information, see the next section.*

Using Separator Pages

A separator page prints before each document (much like a fax cover page) and identifies the name of the user who printed the job, the date and time it was sent, and other details. Using separator pages makes finding your document among a stack of others in the printer's output bin easier. In addition, two of the separator pages furnished with Windows 2000 switch between PostScript and PCL (the Printer Control Language used by most Hewlett-Packard printers), which is useful for printers that don't automatically switch languages.

Windows 2000 includes four separator page files, which you can use ready-made or you can customize. The supplied files, which are stored in the %SystemRoot%\System32 folder, are described in Table 13-2.

Table 13-2. Separator Page Files

File Name	Description
Sysprint.sep	Switches the printer to PostScript and then prints a separator page that includes account name, job number, date, and time
Pcl.sep	Switches the printer to PCL and then prints a separator page that includes account name, job number, date, and time
Pscript.sep	Switches the printer to PostScript but does not print a separator page
Sysprtj.sep	A variant of Sysprint.sep that uses Japanese fonts, if available

Separator page files are plain text files with the extension .sep. You can create your own separator pages either by modifying the files supplied with Windows 2000 or by typing codes into a new plain-text document and saving that document in your %SystemRoot%\System32 folder. Be sure to save the document as a plain-text file.

The codes you can use for your separator pages are listed in Table 13-3. Each separator file must start with a single character on a line by itself; that character becomes the *command delimiter*, which identifies commands elsewhere in the file. You can use any character as a command delimiter. In Table 13-3, the @ character is used as the command delimiter. For these commands to work, the first line of your file must contain only a single @ character.

Table 13-3. Separator Page Codes

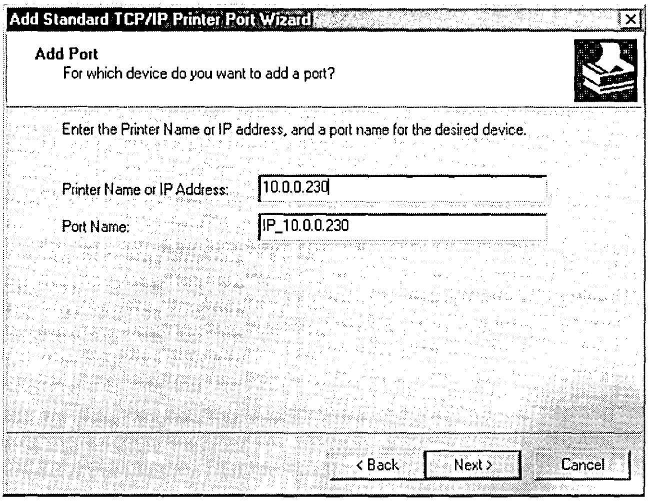
Code	Description
@N	Prints the user name of the person who submitted the print job.
@I	Prints the job number.
@D	Prints the date, in the date format specified by Regional Options in Control Panel.
@T	Prints the time, in the time format specified by Regional Options in Control Panel.
@L	Prints all characters following @L up to the next @ code or until the page width specified by @W is reached.
@F*pathname*	Prints the contents of the file specified by *pathname.*
@H*nn*	Sends a printer-specific control code, where *nn* is a hexadecimal value. For example, use @H1B to send an escape code, which has a hexadecimal value of 0x1B (27 decimal).
@W*nnn*	Sets the maximum width of the separator page to the decimal value specified by *nnn*. Any characters beyond this width are truncated. (The default width is 80; the maximum is 256.)
@B@S	Prints in single-width block characters.
@B@M	Prints in double-width block characters.
@U	Turns off block-character printing.
@*n*	Skips *n* lines. (*n* can be 0 through 9.)
@E	Ejects the current page from the printer.

Setting Up a Printer That's Connected Directly to the Network

Your print device doesn't necessarily have to be connected directly to the computer that's acting as the print server. That is, it needn't be connected to one of the computer's local ports, such as a parallel port (LPT*x*), a serial port (COM*x*), an infrared (IrDA) port, a universal serial bus (USB) port, or a 1394 port. If your print device has a built-in Ethernet adapter (or it's connected to a network interface device such as a Hewlett-Packard JetDirect), all you need to do is set up a standard TCP/IP port—a simple procedure in Windows 2000:

1. Be sure that the print device is connected to the network and powered on.
2. In the printer's properties dialog box, click the Ports tab. Click Add Port.
3. In the Printer Ports dialog box that appears, select Standard TCP/IP Port and then click New Port.
4. On the first page of the Add Standard TCP/IP Printer Port Wizard, click Next.

5. On the Add Port page, type the IP address of the printer. (You can get that by printing a configuration report from the print device or network interface device. See the device's manual for instructions.) You can accept the Port Name that the wizard proposes or create your own. Click Next.



Add Standard TCP/IP Printer Port Wizard

Add Port
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 10.0.0.230

Port Name: IP_10.0.0.230

6. The wizard's final page shows your settings and also shows information (such as the adapter type) that confirms successful communication with the print device. Click Finish.

The Standard TCP/IP Print Monitor (SPM) is a new feature of Windows 2000, and it supplants the LPRMON protocol that was used in Windows NT for printing to network interface print devices. SPM is much easier to configure, and because LPRMON uses double spooling, SPM (which spools only once) is 50 percent faster.

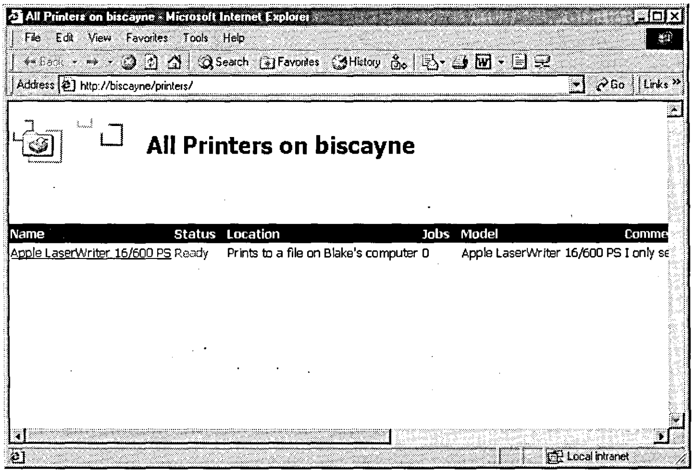
Setting Up a Printer for Non–Windows 2000 Clients

Your network probably includes computers that are not running Windows 2000. By configuring your print server properly, you can make it easy for users of the other computers to use your printers. A Windows 2000–based print server includes support for the following types of clients:

- **Windows 2000, Windows NT, and Windows 9x.** To provide access for these types of clients, click the Sharing tab in the printer's properties dialog box. Click Additional Drivers and then select each of the client types you want to support. When one of these clients connects to the printer for the first time, Windows 2000 automatically sets up the printer on the client system.
- **Windows 3.x and MS-DOS.** These clients must install a 16-bit printer driver on their systems and must redirect a local port to the network share. For example, you'd configure a printer driver on such a machine to print to LPT1, and then

issue this command to the network redirector: *net use lpt1: \\server\share*. (Replace *server* with the computer name of your print server and replace *share* with the share name of the printer.)

- **UNIX.** On the print server, install Print Services For UNIX. (Go to Control Panel | Add/Remove Programs | Add/Remove Windows Components | Other Network File And Print Services | Details | Print Services For UNIX.) You also need to set the TCP/IP Print Server service (the name of Print Services for UNIX as it appears in the Services snap-in) to start automatically. *For information about controlling services, see Chapter 20, "Managing Services."* Set up an LPR port by opening the printer's properties dialog box and clicking Ports | Add Port | LPR Port | New Port. UNIX clients then connect to the printer using the Line Printer Daemon (LPD) service.
- **Internet.** Clients that support Internet Printing Protocol (IPP) can print to a Windows 2000 print server using HTTP. (Currently, only Windows 2000 and Windows 9x clients support IPP.) To provide access for Internet (or intranet) clients, you must install Internet Information Services (IIS) *For details about IIS, see Chapter 27, "Managing a Web Server."* To connect to a shared printer using IPP; at the client computer, type *http://server/printers/* (replace *server* with the URL or the computer name of the server) in the Address bar of Microsoft Internet Explorer. Figure 13-4 shows an example of what a Web browser might see. Clicking the name of a printer displays a screen similar to the one shown in Figure 13-5, where a user (with the requisite permissions) can view the queue, manage the printer, and manage documents. Clicking Connect (under Printer Action in the left frame) automatically installs the printer on the client computer if it's not already installed.

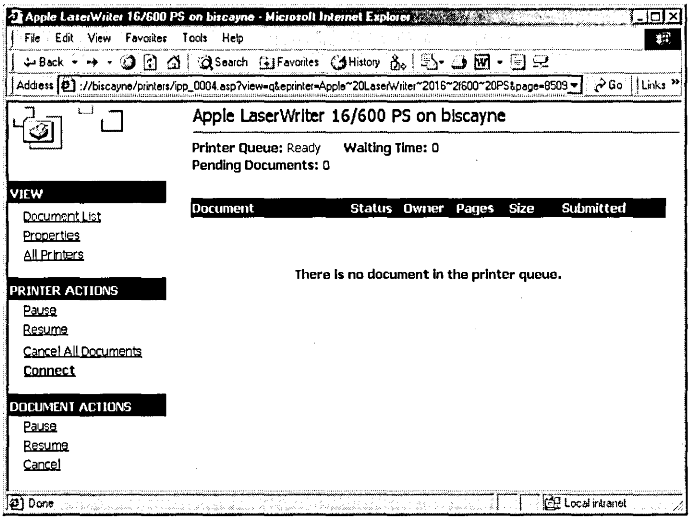

All Printers on biscayne - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Go
Links
Local intranet

Address http://biscayne/printers/

All Printers on biscayne

Name	Status	Location	Jobs	Model	Comme
Apple LaserWriter 16/600 PS	Ready	Prints to a file on Blake's computer	0	Apple LaserWriter 16/600 PS	I only se

Figure 13-4
With Internet printing, you can use a Web browser to view the Printers folder.


Apple LaserWriter 16/600 PS on biscayne - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address ://biscayne/printers/ipp_0004.asp?view=q&eprinter=Apple~20LaserWriter~2016~2f600~20PS&page=8509
Go
Links
VIEW
Document List
Properties
All Printers
PRINTER ACTIONS
Pause
Resume
Cancel All Documents
Connect
DOCUMENT ACTIONS
Pause
Resume
Cancel
Done
Local intranet

Apple LaserWriter 16/600 PS on biscayne

Printer Queue: Ready **Waiting Time:** 0
Pending Documents: 0

Document	Status	Owner	Pages	Size	Submitted

There is no document in the printer queue.

Figure 13-5
The Web interface allows a user with appropriate permissions to manage printers and documents.

Installing Windows 2000 Drivers on a Windows NT Print Server

Windows NT has a similar capability of storing and installing appropriate printer drivers for various versions of Windows. If you're print server is a computer running Windows NT, you'll want to add Windows 2000 drivers to it so that when computers running Windows 2000 connect to that server, they can automatically find and install the correct drivers. Doing this is easy:

1. Using a computer that is running Windows 2000, log on using an account that's a member of the Administrators (or Domain Admins) group on the Windows NT system.
2. Open the Printers folder on the computer running Windows NT. (In an address bar or in Start | Run, type \\NTserver, where *NTserver* is the computer name of the print server. Then open the Printers folder.)
3. In the Printers folder, choose File | Server Properties | Drivers | Add.
4. On the Environment And Operating Systems page of the Add Printer Driver Wizard, select Windows 2000.

Printing on a Network with Apple Macintosh Computers

With Microsoft Windows 2000 Server, Macintosh clients can connect to shared printers on a Windows 2000 network. Alas, this capability is not included with Windows 2000 Professional, so it's beyond the scope of this book to describe Print Server for Macintosh. Briefly, what you need to do on the computer running Windows 2000 Server is to install Print Server for Macintosh. (Go to Control Panel | Add/Remove Programs | Add/Remove Windows Components | Other Network File And Print Services | Details | Print Server For Macintosh.) Doing so also installs the requisite AppleTalk protocol.

Another solution for setting up a mixed network (Macintosh and computers running Windows) is to use a program called DAVE, which runs on the Macintosh computers. DAVE is a product of Thursby Software Systems, Inc. (*www.thursby.com*).

Setting Server Properties

In addition to setting properties for individual printers by using their properties dialog box, you can set other properties by visiting the Print Server Properties dialog box. To get there, open the File menu or right-click a blank area of the Printers folder and then choose Server Properties.

The first three tabs control the list of items you see in the properties dialog box for a printer:

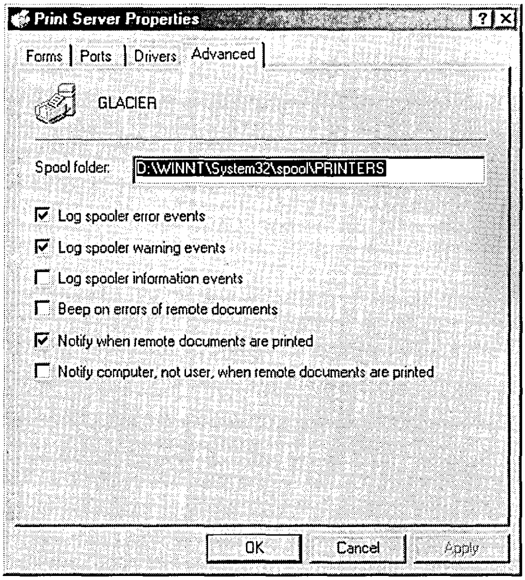
- The Forms tab controls the list of forms that you can assign to trays using the Device Settings tab in a printer's properties dialog box. You can create new form definitions and delete any that you create, but you can't delete any of the predefined forms.
- The Ports tab offers the same capabilities as the Ports tab in a printer's properties dialog box.
- The Drivers tab offers a list of all the installed printer drivers and provides a centralized location where you can add, remove, or update drivers.

The Advanced tab, shown in Figure 13-6, offers a potpourri of options:

- You can specify the location of spool files. You might want to change to a folder on a different drive if, for example, you frequently run out of space on the current drive when you attempt to print large documents.

Note Your Spool folder setting on the Advanced tab gets stored in the DefaultSpoolDirectory value in the HKLM\Software\Microsoft \Windows NT\CurrentVersion\Print\Printers registry key, and it determines the spool folder for all your local printers. If you want to use a different folder for a particular printer, you must edit the registry directly. Go to the HKLM\Software\Microsoft\Windows NT\CurrentVersion \Print\Printers\printer key (where *printer* is the name of the printer you want to modify) and set the SpoolDirectory value to the path you want to use.

- The first three check boxes on the Advanced tab determine which types of events merit entries in the Windows 2000 System log, which you can view with the Event Viewer snap-in. *For more information, see Chapter 5, "Monitoring System and Application Activities with Event Viewer."*

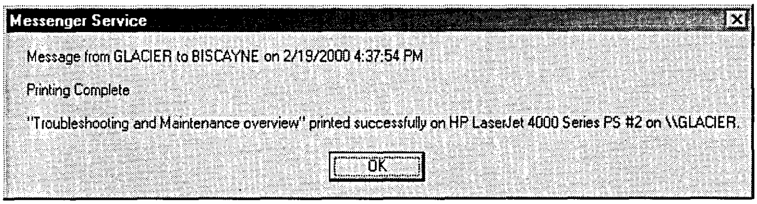


Spool folder: D:\WINNT\System32\spool\PRINTERS

☑ Log spooler error events
☑ Log spooler warning events
☐ Log spooler information events
☐ Beep on errors of remote documents
☑ Notify when remote documents are printed
☐ Notify computer, not user, when remote documents are printed

Figure 13-6
Settings you make here affect options available in all printer properties dialog boxes.

- The last two check boxes control notification of completed print jobs. Windows 2000 can cause a message to pop up to let you know when you can fetch your printout. (See Figure 13-7.) If you don't select the last check box, the message goes to the first workstation at which the user who printed the job is logged on. If that user account is logged on to more than one workstation, then the message might not go to the one that generated the print job. To ensure that it does, select the last check box also, which causes the message to be delivered to the computer that generated the print job.



Message from GLACIER to BISCAYNE on 2/19/2000 4:37:54 PM

Printing Complete

"Troubleshooting and Maintenance overview" printed successfully on HP LaserJet 4000 Series PS #2 on \\GLACIER.

Figure 13-7
The print server can notify users with a message like this.

Windows 2000 uses the Alerter service on a print server to send notification to users when network printing jobs are complete. By default, the Alerter service does not run automatically in Windows 2000 Professional. If you plan to use this feature, you'll need to start the Alerter service using the Services snap-in in Computer Management.

To receive such a message, a computer must be running the Messenger service. Users right next to the printer might want to stop this service (and not be bothered by the pop-ups), whereas users down the hall can leave it running.

Troubleshooting

If a document gets stuck in the print queue and you can't delete it, open the Services snap-in in the Computer Management console and stop the Print Spooler service. Then restart the service.

Chapter 14

Using Removable Storage

In This Chapter

Getting Started with Removable Storage 236

Setting Up and Using Media Pools 237

Using Hardware Devices 241

Securing Devices and Media 251

Using Backup with Removable Storage 252

Removable Storage is a new feature of Microsoft Windows 2000 that tracks your removable storage media, such as tapes, CDs, and optical discs. It also manages the hardware devices, such as changers and jukeboxes, that contain the removable storage media. Removable Storage keeps track of device status, media requests from programs, and media usage. By providing a common media management service, application developers no longer need to create specific programs and drivers for each device type. And with Removable Storage in control, it's easier to share media and devices among programs and among users.

Not everyone agrees that Removable Storage is a feature, however. It's best suited to robotic libraries, tape autoloaders, and other hardware that's more likely to be found in large corporate networks than in the networks operated by most small businesses and home networks. Whether you consider Removable Storage to be a boon or a bane depends on the type of removable storage hardware you have, your backup procedures, and your desire to manage your collection of removable media.

One word of encouragement to those who come down on the "bane" side: as more applications become Removable Storage–aware, its value will increase and its inconvenience will diminish. Such applications will call on the Removable Storage service directly and transparently so that you won't need to be bothered with it. In the meantime, you have the opportunity to explore the inner workings of this new service!

Getting Started with Removable Storage

Removable Storage is a snap-in in the Computer Management console. You find it by opening Computer Management and navigating to Computer Management \Storage\Removable Storage. Alternatively, you can open the snap-in in its own window by opening Ntmsmgr.msc. Figure 14-1 shows an example.

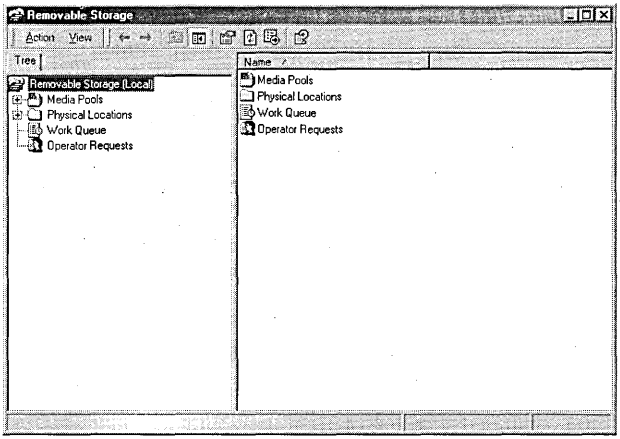
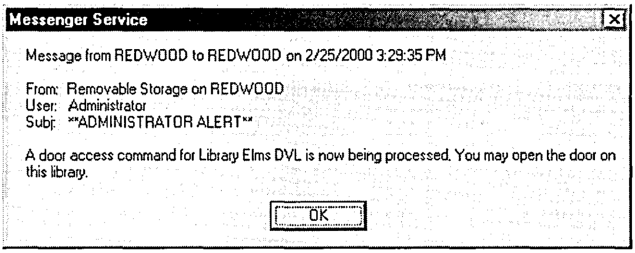


Figure 14-1
Opening Ntmsmgr.msc eliminates the clutter of other Computer Management snap-ins.

Removable Storage has four top-level folders:

- Media Pools contains, in a hierarchical structure, a record for each piece of managed media, be it tape, CD, Zip disk, optical disc, or some other type of removable storage media. *For more information, see the next section, "Setting Up and Using Media Pools."*
- Physical Locations contains a folder for each device. Each device's folder includes both a folder for the media currently installed in the device and a folder for the drives in the device. In addition, Physical Locations contains an Off-Line Media folder—a repository for records of media that you have inventoried but that are no longer in any physical device. *For more information, see "Using Hardware Devices," page 241.*
- Work Queue displays a list of all pending and completed tasks, such as requests to mount a CD or inventory the media in a device. These requests can come from an application or from Removable Storage itself. You can right-click a task to delete it from the queue or, in the case of pending mount requests, to change the order.
- Operator Requests displays a list of the tasks that Removable Storage asks you to perform. It makes these requests by displaying a message similar to the one shown here.



Message from REDWOOD to REDWOOD on 2/25/2000 3:29:35 PM

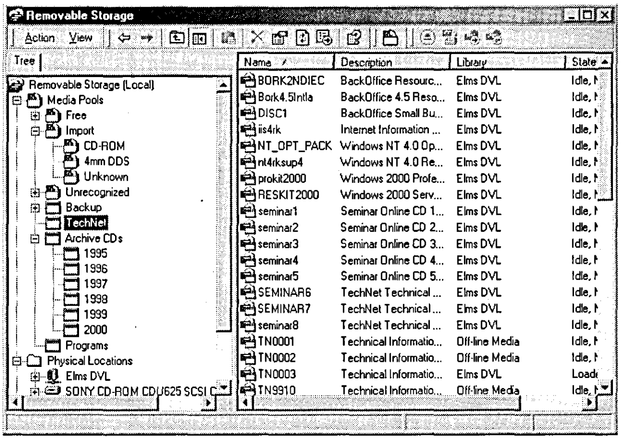
From: Removable Storage on REDWOOD
User: Administrator
Subj: **ADMINISTRATOR ALERT**

A door access command for Library Elms DVL is now being processed. You may open the door on this library.

Setting Up and Using Media Pools

Removable Storage organizes all media into logical groups called media pools. A *media pool* is a collection of related records—one for each tape, disc, or cartridge. In Removable Storage, each media pool is represented by a folder icon; media pools and media are analogous to folders and files in Windows Explorer. You'll find one difference from file folders, however: each media pool can contain only one type of media.

Initially, Removable Storage includes three *system* media pools: Free, Import, and Unrecognized. (Actually, each of these folders is a container for other media pools. The Free, Import, and Unrecognized folders contain a folder for each type of media used on your system. For example, the system shown in Figure 14-2 contains folders for CDs, 4-mm DDS tapes, and unknown media types.)



Name	Description	Library	State
BORK2NDIEC	BackOffice Resourc...	Elms DVL	Idle,
Bork4.5Intla	BackOffice 4.5 Reso...	Elms DVL	Idle,
DISC1	BackOffice Small Bu...	Elms DVL	Idle,
iis4rk	Internet Information ...	Elms DVL	Idle,
NT_OPT_PACK	Windows NT 4.0 Op...	Elms DVL	Idle,
nt4rksup4	Windows NT 4.0 Re...	Elms DVL	Idle,
prokit2000	Windows 2000 Profe...	Elms DVL	Idle,
RESKIT2000	Windows 2000 Serv...	Elms DVL	Idle,
seminar1	Seminar Online CD 1...	Elms DVL	Idle,
seminar2	Seminar Online CD 2...	Elms DVL	Idle,
seminar3	Seminar Online CD 3...	Elms DVL	Idle,
seminar4	Seminar Online CD 4...	Elms DVL	Idle,
seminar5	Seminar Online CD 5...	Elms DVL	Idle,
SEMINAR6	TechNet Technical ...	Elms DVL	Idle,
SEMINAR7	TechNet Technical ...	Elms DVL	Idle,
seminar8	TechNet Technical ...	Elms DVL	Idle,
TN0001	Technical Informatio...	Off-line Media	Idle,
TN0002	Technical Informatio...	Off-line Media	Idle,
TN0003	Technical Informatio...	Elms DVL	Load
TN9910	Technical Informatio...	Off-line Media	Idle,

Figure 14-2
Media pools help you to organize your media into logical groups.

- The Free media pools contain media that are not currently in use by any application and can therefore be used by an application that makes a request.

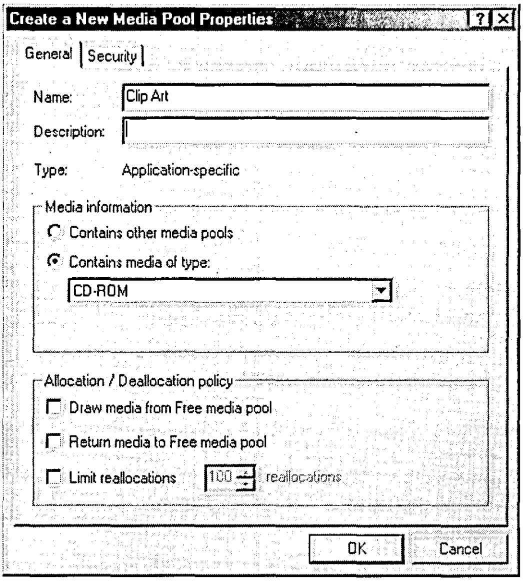
- The Import media pools contain media that have just been added to the system and that can be identified by Removable Storage. This includes media that have been formatted but have not been used before by a Removable Storage–aware application. If you inject a tape that you've used with a previous version of NT Backup, a CD, or a Zip disk, for example, it initially appears in the Import media pool for the appropriate media type. The Import media pools are simply a temporary holding place for media; you'll want to move the media to an appropriate application media pool.
- The Unrecognized media pools are another temporary holding place for recently added media. Unformatted media (or media with an unrecognized format) arrive in the Unrecognized pool for the appropriate media type. If you want to make such media available to applications, you should move them to the corresponding Free media pool.

In addition to the system media pools, Removable Storage can contain *application* media pools. Application media pools can be created by an application (Backup is the one application included with Windows 2000 that creates its own media pool), or you can create them. Figure 14-2 shows several application media pools: Backup (the one created by Backup), TechNet, Archive CDs (which is actually a container for several media pools), and Programs.

Creating a Media Pool

You can use media pools to organize your media into logical groups. For example, on our Elms DVL (a CD-ROM jukebox that holds 100 CDs, now sold as the Cygnet id100), we have the entire collection of Microsoft TechNet CDs, which now numbers over 30. (By the way, TechNet is an excellent resource for Windows 2000 experts. For more information, visit *www.microsoft.com/technet.*) To make it easier to find the TechNet CDs, we created a TechNet media pool to contain them.

To create a media pool, right-click Media Pools and choose Create Media Pool. A dialog box similar to the one shown in Figure 14-3 appears. Provide a name and, optionally, a description. In the Media Information box, you can specify whether the media pool will contain only one type of media or whether it can contain other media pools. The options in the Allocation/Deallocation Policy box are applicable only to rewritable media (such as tapes); you can set up a media pool so that an application automatically fetches and returns its media to the Free media pool as needed. On the Security tab of this dialog box, you can set permissions for access to the media pool. *For more information, see "Securing Devices and Media," page 251.*



Name: Clip Art

Description:

Type: Application-specific

Media information

○ Contains other media pools

● Contains media of type:

CD-ROM

Allocation / Deallocation policy

□ Draw media from Free media pool

□ Return media to Free media pool

□ Limit reallocations 100 reallocations

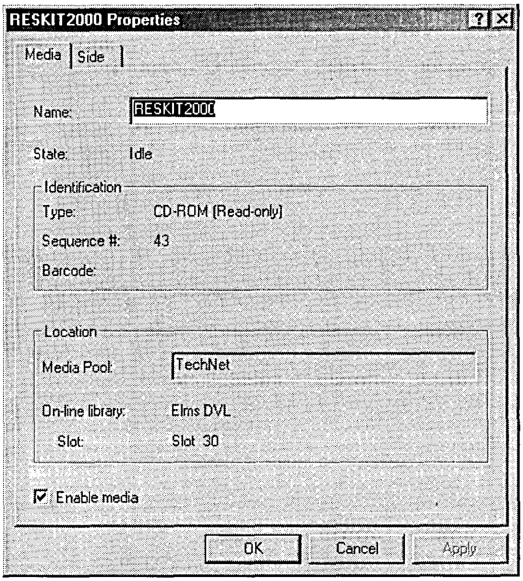
Figure 14-3
You can create your own application media pools.

Troubleshooting

If you receive a message that reads "The media pool identifier does not represent a valid media pool" when you click OK in the Create A New Media Pool Properties dialog box, it's because you selected a media pool before you chose the Create Media Pool command. (The command, of course, shouldn't be available in that context—but it is.) Simply select the folder in which you want to create a new application media pool—either the top-level Media Pools folder or an existing folder that is set to contain other media pools—before you choose Create Media Pool.

Managing Media in Media Pools

To view or modify the properties for a tape, CD, or disc, simply double-click its record in the details pane (or right-click and choose Properties). You'll see a dialog box similar to the one shown in Figures 14-4 and 14-5. The description you specify on the Side tab appears in the details pane. You can also change the name that Removable Storage assigns to media. It initially uses the volume name or the name provided by the application, but you can change it to something more meaningful and Removable Storage can still correctly identify and track the media.



Name: RESKIT2000

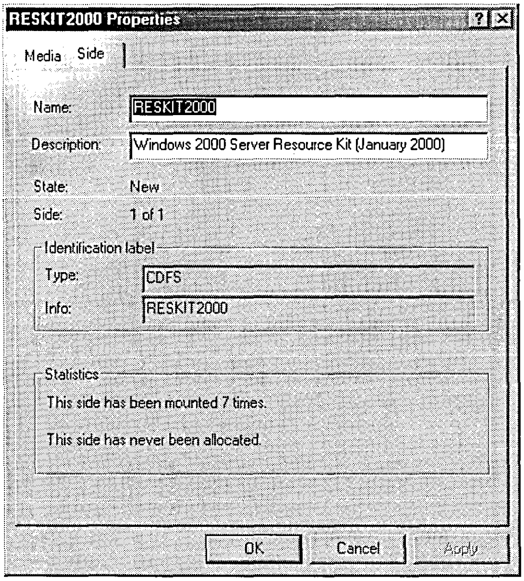
State: Idle

Identification
Type: CD-ROM (Read-only)
Sequence #: 43
Barcode:

Location
Media Pool: TechNet
On-line library: Elms DVL
Slot: Slot 30

☑ Enable media

Figure 14-4
The Media tab shows the volume name (which you can change) and the current location.



Name: RESKIT2000
Description: Windows 2000 Server Resource Kit (January 2000)

State: New
Side: 1 of 1

Identification label
Type: CDFS
Info: RESKIT2000

Statistics
This side has been mounted 7 times.
This side has never been allocated.

Figure 14-5
The Side tab provides a Description box as well as statistics about media usage.

Applications can move media from the Import or Unrecognized pools into the Free pool or into their own application pool. Applications that use rewritable media also move media between the Free pool and their own application pool as needed or as the media become available. If you create a set of application pools to organize your media collection (as we did in the system shown earlier in Figure 14-2), you can move media from one pool to another by dragging or by using Cut and Paste commands—just as you can with files in Windows Explorer.

Note The menus and toolbar also include a Copy command, but it actually works like Cut. You can't have records for the same media in more than one media pool.

Using Hardware Devices

Removable Storage manages a variety of removable storage devices, ranging from stand-alone drives to robotic libraries. Stand-alone drives hold a single tape or disc, which you manually insert in the drive. Robotic libraries hold multiple tapes or discs, and they have a mechanism for moving media from the storage slots to the drives. Some robotic libraries include other components that are controlled by Removable Storage, such as doors, inject/eject ports, cleaner cartridges, and bar-code readers.

Using Removable Storage with Stand-Alone Drives

If your computer has a CD-ROM drive, a Zip drive, or other drive that holds a single removable disk or cartridge (other than a tape drive), you'll find that you can use it as you always have. It shows up as a drive letter in My Computer and in Disk Management, and its files are accessible through Windows Explorer and other applications as soon as you insert media.

You might not realize it, but even with stand-alone drives, Removable Storage keeps track of the media. You can demonstrate this by opening Removable Storage, right-clicking your drive (under Removable Storage\Physical Locations), and choosing Inventory. This causes Removable Storage to identify the media, ensuring that it accurately shows information about the current media. If you navigate down to Media or Drives, you'll see an identifier (by default, the volume name) for the media. And you'll also find the media in the Import media pool, the place where new, unidentified media first arrive.

Fascinating as that may be, you'll generally have no reason to bother with Removable Storage to manage a stand-alone drive. If you want to keep statistics about particular media (such as how often you mount one) or save some descriptive information about each one (such as the CD key), you can do that with Removable Storage. The trick is that you must move the piece of media from the Import media pool into another media pool. (Media in the Import and Unrecognized pools are automatically deleted when you remove the media from the device.) Then, when you eject the media, Removable Storage moves it to the Off-Line Media folder (and also leaves a record in the media pool to which you moved it). When you reinsert the media, Removable Storage recognizes the previously used media and uses its record instead of creating a new one and placing it in the Import media pool.

For example, we have a computer that we use as a test platform for various projects, and software gets installed and removed repeatedly. We created a new media pool called Program CDs, and when we insert the CD for a new program, we move it from the Import pool to the Program CDs pool. We then open the properties dialog box for the CD and type the CD key in the Description box. The next time we have to reinstall the program—by then, the jewel case bearing the CD key on a yellow sticker is long lost—we simply insert the CD, and the CD key appears in the Description column in the Media folder. You might find much better and easier ways to manage such information (not losing the jewel case, for example), but this turns out to be a convenient tool for us. You might also discover other uses for Removable Storage, even with a stand-alone drive.

Using a CD Changer

Owners of ATAPI CD-ROM changers, such as the popular series of CD-ROM changers from NEC, are among those who complain loudest about Removable Storage. These changers typically fit in a single drive bay and allow you to insert as many as seven CDs. Under Windows 9x and Windows NT, such devices appear in Windows Explorer as a separate CD-ROM drive for each slot, each with its own drive letter. To use a CD—in Windows Explorer or another application—you simply address it by its drive letter. When you specify a drive letter, the CD-ROM changer loads the correct CD.

But in fact, although these devices contain a number of slots for CDs, they contain only a single CD-ROM drive—and Windows 2000 treats it exactly so. In Windows Explorer and in Disk Management, for example, you'll see only a single CD-ROM drive. Worse, the drive appears to be empty (that is, it doesn't contain a CD) even if you have filled all the slots. A CD becomes available in Windows Explorer and other applications only when you use Removable Storage to mount it. Removable Storage then allows access to a mounted CD by using the drive's letter or a mount point for the drive. *For information about mount points, see "Assigning a Drive Letter or Drive Path," page 215.*

Note Some CD changers (not the ones included on the Hardware Compatibility List) are not detected as changers. These changers act like a single CD-ROM drive; in Removable Storage only one CD appears, and you can't mount any other CDs that are installed in the changer.

There's no getting around it: for users of CD changers, the discipline imposed by Removable Storage is a step backward. The extra step of mounting a CD (as well as the inability of Removable Storage to notice when you insert a CD in the changer or remove one from it) is an annoyance. But we've found two workaround solutions that make the use of CD changers practical:

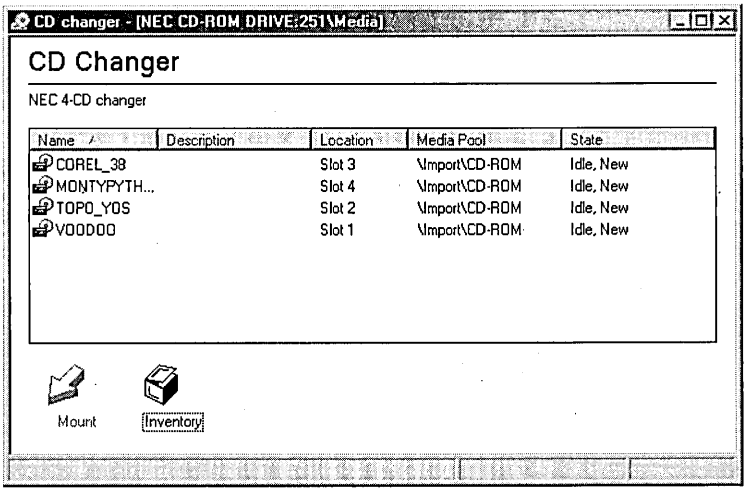
- A custom MMC console
- A batch program

Creating a Custom MMC Console

With MMC, you can easily create a console that focuses just on the tasks you need to perform. *For detailed information about MMC, see Chapter 4, "Using and Customizing Microsoft Management Console."*

For one of our NEC changers, we set up the console shown in Figure 14-6. As you can see, it has only two tasks—Mount and Inventory—which you use as follows:

- To use a CD, simply select it and click Mount.
- When you insert CDs or remove them from the changer, click Inventory to update the list of CDs. (Removable Storage automatically inventories the contents when you start your computer.)



CD changer - [NEC CD-ROM DRIVE:251\Media]

CD Changer

NEC 4-CD changer

Name	Description	Location	Media Pool	State
COREL_38		Slot 3	\Import\CD-ROM	Idle, New
MONTYPYTH...		Slot 4	\Import\CD-ROM	Idle, New
TOPO_YOS		Slot 2	\Import\CD-ROM	Idle, New
VOODOO		Slot 1	\Import\CD-ROM	Idle, New

Figure 14-6
This MMC taskpad view allows simple management of a CD changer.

You can find this console, CD changer.msc, on the companion CD. If you have exactly the same type of changer (identified as NEC CD-ROM DRIVE:251), you can use it unmodified. If you have a different type, the console still works, but you'll have to double-click your drive name and then double-click Media to get to the list of CDs. That extra effort defeats the purpose of this one-click solution—but you can easily create a custom console that works with your changer by following these steps:

1. Start MMC. (Choose Start | Run and type *mmc.*)
2. Add the Removable Storage Management snap-in by choosing Console | Add /Remove Snap-In | Add | Removable Storage Management | Add.
3. In the console tree, navigate to Console Root\Removable Storage\Physical Locations\drivename\Media.
4. Right-click Media and choose New Taskpad View.
5. The default settings in the New Taskpad View Wizard are generally appropriate. On the Taskpad Display page, you might want to consider changing List Size to Medium.
6. In the New Task Wizard, create two new tasks. Both are menu commands:
   - Using List In Details Pane as the command source, select Mount in the Available Commands list.
   - Using Tree Item Task as the command source, select the drive name in the Console Tree list and select Inventory in the Available Commands list.
7. Clean up the clutter. Choose View | Customize and clear all options except Status Bar.
8. Choose Console | Options. Give the console a name, and change the icon if you like. Set the console mode to User Mode—Limited Access, Single Window.
9. Choose Console | Save.

Like other MMC consoles you create, this one appears in the Administrative Tools folder of your Start menu, which provides an easy way to open it. But if you use it frequently, you'll want to add a shortcut to your desktop or to your Quick Launch toolbar.

This simple console performs all the tasks that are necessary on most CD changers. You might want to customize it in any of the following ways:

- You could add task buttons for Dismount and Eject if those tasks work with your changer. (Rather than adding task buttons to test these commands, you can find out whether they work by right-clicking a CD and choosing a command.) With most CD changers, the Eject command doesn't work. (For the reasons why, see Microsoft Knowledge Base [KB] article Q231814.) And there's no reason to use Dismount with most changers, since you don't need to dismount one CD before you can mount another. You can eject a CD by using the Eject command in Windows Explorer or by using the changer's front-panel controls. Either way, Removable Storage is unaware of the change, and you'll need to click Inventory if you want the CD list to accurately reflect the changer contents.

- You could clean up the display by removing the Description and Media Pool columns from the details pane and making the window smaller.
- If you want to use Removable Storage to manage your CD collection, you could add tasks or views that let you move CDs from the \Import\CD-ROM media pool (the place where new CDs show up) to the appropriate pool. The main advantage of doing so is that you could then add a description to each CD, and the description would appear each time you inserted the CD. This might be useful, for example, if the information provided by the CD volume name is inadequate. (With only a handful of CDs in the changer, however, this usually isn't a problem. And if you're using audio CDs, CD Player Deluxe—or whatever playback software you use—likely stores much more useful information about each CD in your collection.)

Troubleshooting

If Removable Storage appears not to work—for example, it won't update the Media folder when you use the Inventory command, or the Work Queue folder shows a number of Failed operations—try stopping and restarting the service. Using the Services snap-in in Computer Management, right-click Removable Storage and choose Restart. If you prefer to use the command prompt, type *net stop ntmssvc* and then, after the service has stopped, type *net start ntmssvc*.

Using a Batch Program

If you're a command-line junkie, you'll be pleased to know that Windows 2000 includes something for you: the ability to control Removable Storage from a command prompt. With Rsm.exe, you can do anything you can do with the Removable Storage snap-in, which makes it an ideal tool for creating batch programs to control your removable storage device.

Note For detailed information about the command-line syntax for Rsm.exe, open Help in Removable Storage and, on the Contents tab, navigate to Removable Storage\Advanced Topics\Using The Command Line For Removable Storage. You can get some help at the command prompt, but you must first know the name of the command for which you need help. To get help, type *rsm command /help*, replacing *command* with one of the following commands: allocate, createpool, deallocate, deletepool, dismount, eject, ejectatapi, mount, refresh, or view.

The following batch program, called Mount.bat, lets you mount a CD from a particular slot by typing *mount* followed by the slot number at the command prompt. And for changers that support the eject method used by Removable Storage, you can eject the currently mounted CD by typing *mount e*. You can find this batch program, which is adapted from the one included in KB article Q227425, on the companion CD. Save it to %SystemRoot%\System32 or another folder on your search path.

```
@echo off

rem - Extract the friendly name of your changer using: rsm view /tchanger
rem - then replace the string following /cf with the string returned.

rem Example:

rem rsm view /tchanger

rem CHANGER

rem NEC CD-ROM DRIVE:253

rem The command completed successfully.

if "%1"=="" goto usage
if "%1"=="/?" goto usage
if "%1"=="1" goto slot1
if "%1"=="2" goto slot2
if "%1"=="3" goto slot3
if "%1"=="4" goto slot4
if "%1"=="e" goto eject
if "%1"=="E" goto eject

goto usage

:SLOT1
rsm mount /sf"Slot 1" /cf"NEC CD-ROM DRIVE:253" /oread
if %errorlevel% equ 536870916 goto mounted
@echo %errorlevel%
goto end

:SLOT2
rsm mount /sf"Slot 2" /cf"NEC CD-ROM DRIVE:253" /oread
if %errorlevel% equ 536870916 goto mounted
@echo %errorlevel%
goto end

:SLOT3
rsm mount /sf"Slot 3" /cf"NEC CD-ROM DRIVE:253" /oread
if %errorlevel% equ 536870916 goto mounted
@echo %errorlevel%
goto end
```

```
:SLOT4
rsm.exe mount /sf"Slot 4" /cf"NEC CD-ROM DRIVE:253" /oread
if %errorlevel% equ 536870916 goto mounted
@echo %errorlevel%
goto end


:MOUNTED
@echo .
@echo Reason: Media already mounted, or no media in slot
goto end

:USAGE
@echo .
@echo To mount media enter slot number between 1 and 4
@echo e.g. Mount 1
@echo .
@echo To eject current slot enter Mount E
goto end

:EJECT
net stop ntmssvc
start /wait rsm ejectatapi /n0
@echo %errorlevel%
net start ntmssvc


:END
rem @echo .
rem @echo DONE!!!
```

You'll need to modify this batch program to work properly with your changer. First, as the remarks at the beginning of the file state, you can enter *rsm view /tchanger* to determine the name of your changer. Use the text that is returned to replace all instances of NEC CD-ROM DRIVE:253 in the batch program. To be sure that the batch program includes handlers for the requisite number of slots—and that they're named correctly in the batch program—enter *rsm view /tstorageslot*. The responses here should replace the text following each occurrence of /sf in the batch program. Note that the so-called friendly names are case sensitive; you must enter them in the batch program exactly as the Rsm View command returns them.

If your computer has more than one changer with the same friendly name, you'll need to use each changer's globally unique identifier (GUID) rather than the friendly name. To find the GUIDs, enter *rsm view /tchanger /guiddisplay*. Then, in the batch program, replace all occurrences of

```
/cf"NEC CD-ROM DRIVE:253"
```

with

```
/cgguid
```

where *guid* is the actual GUID. To make a single batch program handle all your changers, you might want to modify it to include a section for each slot in each changer and set up the initial branching to use a two-digit number to identify the changer and slot. For example, typing *mount 23* would mount the CD in changer 2, slot 3.

Using a Jukebox

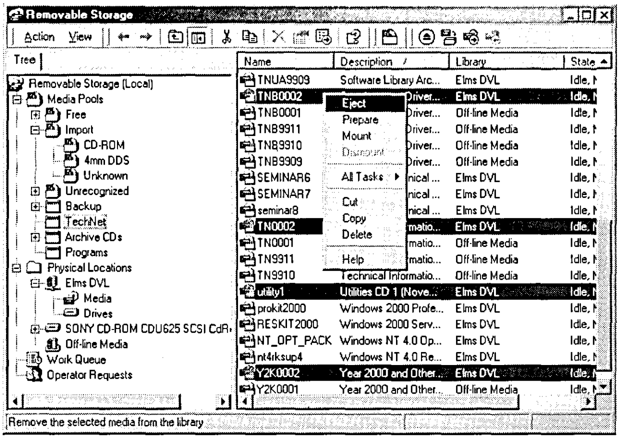
This chapter explains that Removable Storage is unnecessary with stand-alone removable disk drives. And Removable Storage is an annoyance with CD changers. So where does Removable Storage become useful? Jukeboxes! A CD-ROM jukebox is an overgrown changer. Typically, jukeboxes hold 100 or more CDs, they might have several CD-ROM drives, and they have a robotic transport mechanism that moves CDs from the storage area to a CD-ROM drive. Although they're not inexpensive, they provide convenient access to a large collection of CDs. And you can easily share their drives so that everyone on the network has access to the CDs.

Applications that are compatible with Removable Storage can send the commands to mount any CD the application needs. At this writing, however, such applications are few and far between. That means that you (and any network users who want to use CDs in the jukebox) need to run Removable Storage to mount and dismount CDs as needed.

Our own network includes a CD jukebox, and every network user has a desktop shortcut to a custom MMC console that includes the Removable Storage snap-in for the network computer. Mounting a CD merely puts it in a drive, ready to use. For a network user to be able to use a mounted CD, the drive must be shared, and the user must have permission to use the share. When one of our users needs a CD, he or she opens the MMC console, dismounts a CD if all the drives are full (preferably not one that someone else is using!), and then mounts the needed CD. That CD is then available through the shared network drive; all users have shortcuts to these drives in their My Network Places folder.

With the assistance of wizards, adding CDs to the library is fairly simple. The procedure varies somewhat, depending on the hardware; here, we use our Elms DVL to demonstrate the process. We mentioned earlier that our CD jukebox contains all the TechNet CDs, among others. Many of those CDs are updated monthly, so each month someone must remove all the old CDs and then add the new ones. Here's how we do it:

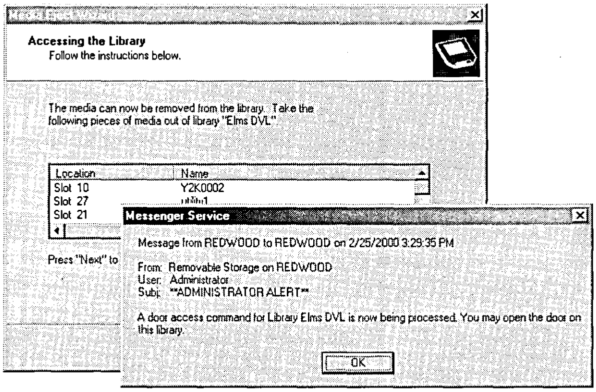
1. In the TechNet media pool, we select all the CDs that need to be replaced (hold down Ctrl and click to select multiple CDs), right-click, and choose Eject.



Name	Description	Library	State
TNUA9909	Software Library Arc...	Elms DVL	Idle, N
TNB0002	Driver...	Elms DVL	Idle, N
TNB0001	Driver...	Off-line Media	Idle, N
TNB9911	Driver...	Off-line Media	Idle, N
TNB9910	Driver...	Off-line Media	Idle, N
TNB9909	Driver...	Off-line Media	Idle, N
SEMINAR6	nical ...	Elms DVL	Idle, N
SEMINAR7	nical ...	Elms DVL	Idle, N
seminar8	nical ...	Elms DVL	Idle, N
TN0002	matio...	Elms DVL	Idle, N
TN0001	matio...	Off-line Media	Idle, N
TN9911	matio...	Off-line Media	Idle, N
TN9910	Technical Informatio...	Off-line Media	Idle, N
utility1	Utilities CD 1 (Nove...	Elms DVL	Idle, N
prokit2000	Windows 2000 Profe...	Elms DVL	Idle, N
RESKIT2000	Windows 2000 Serv...	Elms DVL	Idle, N
NT_OPT_PACK	Windows NT 4.0 Op...	Elms DVL	Idle, N
nt4rksup4	Windows NT 4.0 Re...	Elms DVL	Idle, N
Y2K0002	Year 2000 and Other...	Elms DVL	Idle, N
Y2K0001	Year 2000 and Other...	Off-line Media	Idle, N

Remove the selected media from the library

2. The Media Eject Wizard shows a list of the selected CDs and their locations, and Removable Storage then generates an operator request to open the door. (Some jukeboxes have an inject/eject port; the Elms DVL has a door that must be opened to get to the CDs, which are stored in 20-CD magazines.) Noting the locations of the CDs, we remove them from the library and complete the wizard.



Accessing the Library
Follow the instructions below.

The media can now be removed from the library. Take the following pieces of media out of library "Elms DVL".

Location	Name
Slot 10	Y2K0002
Slot 27	utility1
Slot 21	

Press "Next" to

Messenger Service

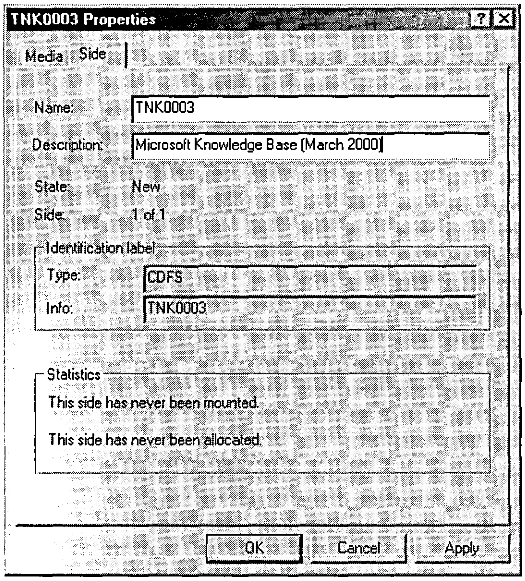
Message from REDWOOD to REDWOOD on 2/25/2000 3:29:35 PM

From: Removable Storage on REDWOOD
User: Administrator
Subj: **ADMINISTRATOR ALERT**

A door access command for Library Elms DVL is now being processed. You may open the door on this library.

3. Removable Storage, having determined that these CDs are no longer in the jukebox, moves them from the Physical Locations\Elms DVL\Media folder to the Physical Locations\Off-Line Media folder. The removed CDs remain in the TechNet media pool (unless we go to that pool and explicitly delete them), and they're automatically recognized if we should reinsert them in the Elms DVL or any other CD library attached to this computer.

4. We then right-click Elms DVL and choose Inject to begin the process of adding the new CDs. Doing so launches the Media Inject Wizard.
5. After loading the CDs in the jukebox, Removable Storage inventories the jukebox and identifies the new media. Because it hasn't seen these new CDs before, it places them in the Import media pool.
6. We add a description to each CD.



Name: TNK0003

Description: Microsoft Knowledge Base (March 2000)

State: New

Side: 1 of 1

Identification label

Type: CDFS

Info: TNK0003

Statistics

This side has never been mounted.

This side has never been allocated.

7. We move all the new CDs from the Import\CD-ROM media pool to the TechNet media pool, where users can easily find the ones they need.

Disabling AutoPlay

Many CDs have a file named Autorun.inf, which causes a program to run when the CD is inserted in a drive (or, in the case of changers and jukeboxes, mounted). This feature, called AutoPlay, can be quite handy—but it can also be an annoyance, especially on a shared drive. When you mount a CD on a shared drive that's attached to another computer, for example, the Autorun program starts on the other computer—not on your computer. If you provide network access to a changer or a jukebox—or if you simply don't want programs to run automatically—you can disable AutoPlay.

(continued)

Disabling AutoPlay *(continued)*

To disable AutoPlay on all CD drives, open Group Policy (Gpedit.msc) and navigate to Computer Configuration\Administrative Templates\System. Open the Disable Autoplay policy, select Enabled, and select CD-ROM Drives. This adds CD-ROM drives to the list of drive types for which AutoPlay is disabled by default, which, without this policy, includes floppy disk drives, network drives, and drives of an unknown type. If you also want to disable AutoPlay on other removable drives, local hard disks, and RAM disks, select All Drives.

You can also disable AutoPlay on only certain drives. We have one system that has a jukebox with shared CD-ROM drives plus a stand-alone drive. We disabled AutoPlay on the jukebox drives (so that when other network users mount a CD, it doesn't run on this system) but left it enabled on the stand-alone drive so that we could continue to enjoy the convenience of AutoPlay when inserting CDs locally. To do this, first set the Disable Autoplay policy (in Group Policy) to Not Configured or Disabled; if it's set to Enabled, AutoPlay is disabled on all CD-ROM drives, regardless of how you set the following registry value. Then use a registry editor to navigate to HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer (you might need to create the Explorer key) and create a DWORD value called NoDriveAutoRun. The value is a bitmap in which each bit represents a drive letter, starting with A as the least significant bit. Setting a bit to 1 disables AutoPlay for the associated drive letter. For example, on our system, we wanted to disable AutoPlay on drives H and I, so we set NoDriveAutoRun to 0x00000180, which we calculated as follows:

```
LKJI HGFE DCBA
0001 1000 0000 = 180 hexadecimal
```

Securing Devices and Media

When you share the drives in a library, you can apply the same types of sharing permissions as you can for any other type of drive. But you can also place restrictions on the use of Removable Storage. With Removable Storage, you can set permissions for the Removable Storage service itself, for each library, and for each media pool. To view or modify security settings, right-click the object you want to secure—Removable Storage, a library, or a media pool—choose Properties, and click the Security tab. Table 14-1 lists the privileges afforded by each permission type.

Table 14-1. Removable Storage Permissions and Privileges

Object	Permission	Privileges
Removable Storage	Use	• Connect to the service
	Control	• Cancel an operator request • Satisfy an operator request
Library	Use	• Dismount media* • Mount media*
	Modify	• Delete a library
	Control	• Open the library door • Dismount a drive • Eject media • Insert media • Inventory a library • Clean a drive • Insert/eject a cleaner
Media pool	Use	• Dismount media* • Mount media*
	Modify	• Create media pools • Move media from pool to pool
	Control	• Delete media pools

* To dismount or mount media, a user must have Use permission for the media pool and the library that contain the media.

Using Backup with Removable Storage

Backup, the backup program included with Windows 2000, relies on Removable Storage to manage backup tapes. (Removable Storage has no bearing on backups that you make to a file with this program; it's concerned only with backups to tape.) If you have a tape autoloader, this is good news. At Backup's request, Removable Storage inserts the appropriate tape when you need to back up or restore files.

But those without tape autoloaders might find this reliance to be more of an annoyance than a benefit. Some users long for the days before Windows 2000 and Removable Storage, when it was up to you to select the appropriate tape and put it in the drive at the appropriate time. On a small network with a few dozen tapes and a stand-alone drive, it's generally not too difficult to keep everything straight. Once you develop a routine with the new Backup and Removable Storage, however, you might not sing its praises, but you will find that it works perfectly well for stand-alone drives.

Troubleshooting

The first problem some users encounter is that their only choice in Backup is to back up to a file, even though they have a tape device installed. That's because for Removable Storage to recognize a tape device, the device must have a driver written specifically for Windows 2000. Legacy drivers written for earlier versions of Windows NT won't work. If your tape device is properly installed (that is, it shows up in Device Manager without any errors) and it doesn't show up in the Backup Destination list in Backup, contact the device's manufacturer for an updated driver that includes the Windows 2000 driver extensions.

Preparing Tapes

Before you can use a tape in Backup, you must use Removable Storage to "prepare" the tape. Preparing a tape erases its current contents and writes a media identifier so that Removable Storage can properly track it. To prepare a tape:

1. Insert a tape in the tape device.
2. In Removable Storage, navigate to the Media folder under the tape device (in Physical Locations).

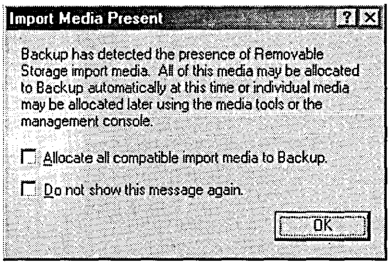
Note A new tape that you insert in the drive goes to the Import media pool if it's a format that Removable Storage recognizes. Tapes with unrecognized formats (including new, unformatted tapes) go to the Unrecognized media pool. You needn't worry about this distinction, however, if you simply locate the tape in the Media folder under Physical Locations.

3. Right-click the tape and choose Prepare. After the operation finishes, note that the Media Pool column now shows that the tape is in the Free media pool.
4. Right-click the tape and choose Eject.

Repeat these steps for each tape you want to prepare.

Backing Up Data

For Backup to use a tape, it must be located in the Import, Free, or Backup media pool. If Backup sees backup media in the Import pool, it asks, in a dialog box similar to the one shown in Figure 14-7, whether you want to allocate the media to Backup. Selecting this option causes Removable Storage to move the media from the Import media pool to the Backup media pool, where it's available only to the Backup program. If you have a stand-alone tape drive, you should select this option, as well as the option to always allocate import media to Backup, if the dialog box you see includes such an option.



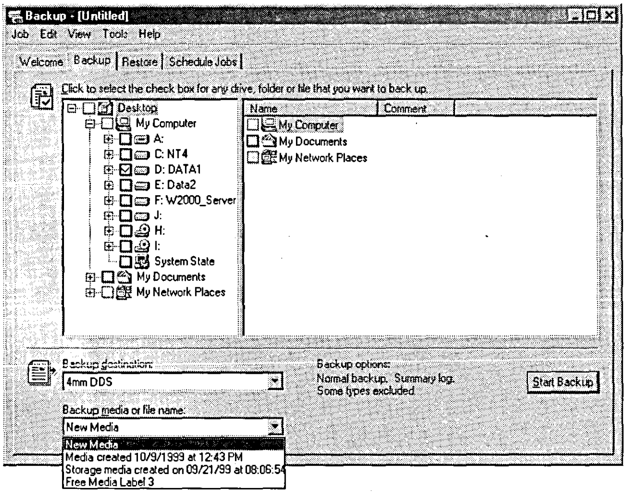
Backup has detected the presence of Removable Storage import media. All of this media may be allocated to Backup automatically at this time or individual media may be allocated later using the media tools or the management console.

□ Allocate all compatible import media to Backup.

□ Do not show this message again.

Figure 14-7
If Backup finds media that it can use in the Import media pool, a dialog box similar to this one asks whether it should move the media to the Backup media pool.

The available tapes then appear in the Backup Media Or File Name list in Backup, as shown in Figure 14-8. You simply select the tape you want to use—and you must be sure to insert that tape in the tape device. If you don't insert the right tape, Backup balks.



Click to select the check box for any drive, folder or file that you want to back up.

Backup destination: 4mm DDS

Backup options: Normal backup. Summary log. Some types excluded.

Backup media or file name: New Media

- New Media
- Media created 10/9/1999 at 12:43 PM
- Storage media created on 09/21/99 at 08:06:54
- Free Media Label 3

Figure 14-8
Tapes in the Free and Backup media pools appear in the list of available media.

Scheduling Backups

This last requirement—Backup's insistence that you insert the tape with the correct label—trips up folks who are used to managing their own tape library. It requires a new discipline in labeling and keeping track of tapes, as well as extra care in setting up scheduled backup jobs. (You can't, for example, set up a job called Daily and put in a different tape each day. You must create a different job for each day, with each one identifying that day's tape.)

Microsoft has detailed the procedure for scheduling backup jobs in KB article Q239892. The same article also tells you how to use command-line switches with Ntbackup.exe to force it to accept whatever tape is in the drive.

A Workaround: Use Backup from Windows NT

After you get used to the new way of doing things, you'll find that Removable Storage is a useful addition to Backup and that the complexity it initially adds actually does provide some benefit by helping you manage your collection of backup tapes. But if Removable Storage has you flummoxed and you're tired of fighting it when you merely want to create a simple backup, avoid Removable Storage altogether. If you upgraded from Windows NT, you can continue to use its Backup program. Windows NT Backup can't back up to a file (though you can use Windows 2000 Backup if you want to do that; it invokes Removable Storage only when backing up to tape), and it has other limitations—for example, you must map a network drive to a drive letter to see it in Backup. On the other hand, Windows NT Backup works with QIC (quarter-inch cartridge) drives, which makes it useful for some tape backup systems that aren't supported by Windows 2000 Backup. (You must have a Windows NT device driver for the drive.) The Windows NT Backup interface is, shall we say, quaint; we'll leave it to you to decide whether that's an advantage or disadvantage.

If Windows NT is still installed on your system (that is, you've set up your system for dual boot), you can run Windows NT Backup (Ntbackup.exe) directly from its current location, which by default is C:\Winnt\System32. (Note that Windows 2000 Backup has the same file name and default location; be sure that you're executing the version in your Windows NT folder.) Alternatively, you can copy two files—Ntbackup.exe and Ntctl3d.dll—from your Windows NT installation to a new folder, from which you can run Ntbackup.exe. (You might also want its help file, Backup.hlp, which you'll find in the same folder.) If you upgraded Windows 2000 over your Windows NT folder, you'll need to create a new folder for Windows NT Backup and expand its files from your original Windows NT CD. To do that, insert the CD and type the following commands at a command prompt:

```
md c:\ntbackup
expand -r f:\i386\ntbackup.ex_ c:\ntbackup
expand -r f:\i386\ntctl3d.dl_ c:\ntbackup
expand -r f:\i386\backup.hl_  c:\ntbackup
```

Replace *f* with the letter of your CD-ROM drive, and replace *c:\ntbackup* with the name of the folder you want to create. Note that the path to the folder containing Ntbackup.exe and Ntctl3d.dll must not include any spaces. (Did we mention "quaint"?)

Chapter 15

Power Management

In This Chapter

ACPI and APM—What's the Difference? 257
Enabling APM Power Management 260
Configuring Power Management Features 261
Troubleshooting Power Management 266

Microsoft Windows 2000 Professional provides three levels of power-management support. On computers that are fully compliant with the Advanced Configuration and Power Interface (ACPI) specification, the operating system maintains efficient and reliable control of the power supplied to your monitor, disk drives, peripherals, and motherboard components, reducing power to those components appropriately when your computer is inactive. On many systems that are not ACPI compliant but that use an Advanced Power Management (APM) 1.2 BIOS, Windows can provide a serviceable, if somewhat less versatile, form of power management. And on some earlier systems that do not have an APM 1.2 BIOS, the operating system can still conserve power by having the operating system shut down the monitor and disk drives during periods of inactivity. If you have a pre-APM BIOS, you might also be able to put your system manually into a low-power state called hibernation when you don't plan to use it again for a while.

In this chapter, we explore the differences between these three forms of power management. We also look at Power Options, the Windows 2000 user interface for activating, deactivating, and configuring power-management features.

ACPI and APM—What's the Difference?

The advantage of ACPI over APM is that ACPI puts power management completely in the control of the operating system. Because ACPI is an operating-system specification, Windows 2000 can provide a consistent approach to power management across all ACPI-compliant systems, thereby ensuring reliability while reducing training costs and user perplexity. With applications that are designed for ACPI, an ACPI-compliant system can also track the status of running or scheduled programs and coordinate power transitions with applications as well as hardware.

APM, on the other hand, is a BIOS specification. (The Basic Input/Output System, or *BIOS,* is a low-level interface that stands between the operating system and the various hardware components of your system.) To manage power on a system that incorporates an APM BIOS but is not fully compliant with ACPI, Windows 2000 must work cooperatively with the BIOS. Because differences exist between the various APM BIOSs that are in use, APM-enabled systems differ considerably in their power-management behavior. Therefore it's impossible to say with certainty what power-management features will be available on your own APM system, exactly how those features will be implemented, and whether all your power-management features will work with 100 percent reliability.

In addition to reliability and consistency, other advantages of ACPI include the following:

- **Control of USB and FireWire devices.** ACPI systems can track the status of devices connected to your computer via Universal Serial Bus or IEEE 1394 (FireWire). Because APM cannot monitor such devices, an APM system might attempt to go into standby or hibernation when a peripheral is active.
- **Support for wake-on-LAN and wake-on-ring.** An ACPI system can be configured to emerge from standby or hibernation when data arrives over the local area network or modem (but not if you're trying to wake a PC Card device that relies on CardBus technology). Windows 2000 cannot take advantage of wake-on-LAN or wake-on-ring on systems that use APM.
- **User definition of the power and reset buttons.** On an ACPI system, you can configure the power and reset buttons to do what you want them to do. You can set the power button so that it puts the system into standby or hibernation, for example, rather than turning the computer off—thereby making it less likely that you'll inadvertently cut the power to your system. (To change the definition of your power or reset button, choose Start | Settings | Control Panel | Power Options and go to the Advanced tab of the Power Options Properties dialog box.)
- **Better battery management.** Under ACPI, Windows 2000 can provide separate meters for each battery on the system. Under APM, Windows 2000 represents multiple batteries as though they were a single composite battery.
- **Dynamic configuration of PC cards.** On ACPI systems, you can insert and remove PC cards, and the operating system responds appropriately without requiring you to reboot.
- **Server and multiprocessor support.** APM power management is not available on any server version of Windows 2000 or on multiprocessor systems.

How Windows 2000 Determines Whether Your System Is ACPI Compliant

During setup, Windows 2000 decides whether your computer is ACPI compliant. If it is (according to the Setup program's judgment), Setup installs an ACPI hardware abstraction layer (HAL). Otherwise, Setup installs a non-ACPI HAL. The decision algorithm is as follows:

First, Setup checks the ACPI BIOS tables that are generated during the setup process. These tables list your computer's devices and their power-management capabilities. If the information is missing, or if information is in the wrong form, you're out of luck; a non-ACPI HAL is installed.

If the tables pass inspection, Setup looks to see whether your BIOS is on a list of BIOSs known to be incompatible with ACPI. If it is, you get the non-ACPI HAL.

If your BIOS isn't on the known-to-be-incompatible list, Setup checks the BIOS date. If it's later than January 1, 1999, you get the ACPI HAL.

If the BIOS date is prior to January 1, 1999, Setup checks a known-to-be-good BIOS list. If yours is there, you get the ACPI HAL. If it's not, Setup installs the non-ACPI HAL.

Determining Your System's Level of Power-Management Support

You can use Device Manager to determine whether your computer is using ACPI for power management:

1. Choose Start | Settings | Control Panel | System.
2. On the Hardware tab, click Device Manager.
3. Open the Computer entry.

If your system is ACPI compliant (and the Windows 2000 Setup program has installed an ACPI hardware abstraction layer), the Computer entry will be Advanced Configuration And Power Interface (ACPI) PC. (In the case of a multiprocessor system, MP appears rather than PC.)

You can also check for ACPI compliance in Control Panel | Power Options. If the Power Options Properties dialog box includes an APM tab, your system is not ACPI compliant. (The absence of an APM tab, however, does not necessarily mean that your system *is* ACPI compliant.)

Upgrading to ACPI

If you use a flash-BIOS update to upgrade a system from APM to ACPI support, you must reinstall Windows 2000 after performing the upgrade. That's because ACPI support is dependent on an ACPI HAL. To get the ACPI HAL, you have to reinstall. You can perform an upgrade installation. (In other words, you don't need to clean install.) This is a relatively painless operation that retains your existing settings, programs, and files.

Enabling APM Power Management

If your system is not ACPI compliant and an APM tab appears in the Power Options Properties dialog box, you can use APM for power management. On some systems, the Windows 2000 Setup program enables APM power management automatically. These are systems with BIOSs known to cooperate effectively with Windows 2000. (The list of known-good BIOSs appears in the file Biosinfo.inf. Depending on how your system was set up, you might find a copy of that file in %SystemRoot%\Inf. If you're curious, you can read the file by opening it in a text editor such as Notepad.) On other systems, Windows 2000 provides support for APM power management, but you have to enable it yourself. You do that by going to the APM tab in Power Options and selecting the Enable Advanced Power Management Support check box. You do not have to restart your system after enabling APM power management. If you subsequently disable APM, however, you do need to restart.

(Some systems have APM BIOSs that are known *not* to work reliably with Windows 2000. The list of these known-to-be-troublesome BIOSs also appears in Biosinfo.inf. On such systems, Windows 2000 does not provide APM support.)

APM is designed to monitor hardware interrupts and I/O port data traffic at the BIOS level to determine whether your system is active or inactive. The BIOS measures periods of inactivity against thresholds that you set via your system's BIOS Setup program. If the BIOS timer arrives at a preset threshold, the BIOS sends a message to Windows 2000 requesting some form of power transition (standby mode, for example). Windows 2000 verifies that your computer is ready for the requested power reduction and then tells the BIOS to go ahead with the requested transition. On a portable computer, the BIOS might also monitor battery status and send Windows a power-reduction request when battery strength falls below a specified threshold.

Unfortunately, Windows 2000 cannot discriminate between the various possible reasons for an APM power-transition request. It cannot tell, for example, whether the BIOS is asking for power reduction because the system is idle, because battery power is low, or because the user has pressed a "sleep" button. Because Windows 2000 tries to honor the BIOS request under all circumstances, the system might attempt to go into standby or hibernation at a time when the computer is not actually idle.

To avoid such problems, Microsoft recommends that if you're using an APM system, you either set the BIOS inactivity thresholds to their highest possible values or disable these thresholds altogether. (On some systems, APM will not work if you disable the BIOS power-reduction thresholds.) With BIOS thresholds disabled or set to high values, you can rely on activity timers provided by Windows 2000 for power management. (For information about adjusting BIOS power-management settings, consult the documentation that came with your computer.)

Microsoft also recommends that you not use a supplemental video card on a portable computer that relies on APM power management. The APM BIOS might not be able to detect a video card that is added to the system or that's in a docking station, and if the supplemental adapter is not detected, suspend might not work.

Configuring Power-Management Features

To configure any of the Windows 2000 power-management features, choose Start | Settings | Control Panel | Power Options. The appearance of your Power Options Properties dialog box depends on your system—whether it's ACPI compliant, whether it has a battery, whether it has power backup in the form of an uninterruptible power supply (UPS), and so on. The figures in this chapter were created on a portable APM-enabled system. Your own Power Options Properties dialog box might differ in some details.

Using Hibernation

Hibernation is a way of shutting down your computer without shutting down the operating system. When you hibernate, Windows 2000 copies everything in memory to disk and then powers down all components of your computer. When you emerge from hibernation (by pressing your computer's power switch), the memory image that was copied to disk is restored, and you're ready to go back to work.

Hibernation saves time because it relieves Windows 2000 of all the housekeeping chores it would normally perform during shutdown and restart. Instead of having to close files on shutdown, redetect hardware, reconstitute the hardware-specific sections of your registry, reload drivers, and restart programs, the operating system simply saves and restores the state of your computer.

Because hibernation puts your work into nonvolatile storage, it's a safer way to reduce power during periods of inactivity than standby. If you experience a power failure while your computer is hibernating, you don't lose anything because your computer's memory has been copied to disk. On the other hand, hibernation requires an extent of free disk space equivalent to the amount of your computer's random access memory. If you have a 128-MB system, for example, you need 128 MB of free disk space to hibernate. Moreover, it takes longer to emerge from hibernation than to come off standby, because the operating system has to restore data from disk.

With either hibernation or standby, you might be prompted for your account password when you return to work. Whether you are or not depends on the Prompt For Password When Computer Goes Off Standby check box, on the Advanced tab of the Power Options Properties dialog box. Yes, that check box refers only to standby, but it affects emergence from hibernation as well!

Hibernation is an option on many systems, even if they're neither APM nor ACPI compliant. But on many systems, you have to select an Enable Hibernation Support check box on the Hibernate tab of the Power Options Properties dialog box before you can hibernate. After you have enabled hibernation support, if your system uses APM or ACPI for power management, you can use power schemes to put your system automatically into hibernation after prescribed periods of inactivity. *(For details, see "Using Power Schemes," below.)* You'll also be able to hibernate manually by choosing Start | Shut Down and selecting Hibernate from the list of shutdown options. (If your system does not use APM or ACPI, this is the only way you can hibernate.)

Using Standby

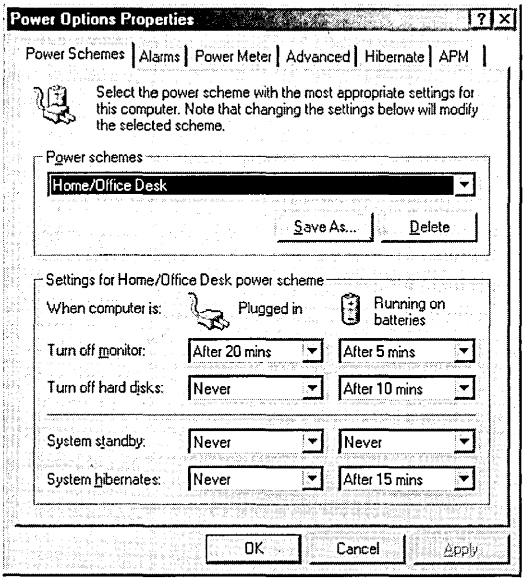
Standby, like hibernation, is a mode in which power to all components is significantly reduced. Its advantages over hibernation are that it doesn't require free disk space and it allows nearly instant system reactivation. On systems that support standby, standby is automatically available, via the Start menu's Shutdown command, power schemes, or both. You do not have to select a check box to enable it, as you do for hibernation. (You do have to enable APM, however, if your system uses APM for power management.)

Using Power Schemes

A power scheme is a named combination of power-reduction settings. Windows 2000 provides a number of these (see, for example, the Portable/Laptop scheme, shown in Figure 15-1), and you can alter the supplied schemes or add your own.

To modify an existing power scheme, simply select it in the Power Schemes list, adjust the settings below, and click OK. To create a new scheme, edit an existing one. Then click Save As and supply a new name.

Note that power schemes are available even on systems that do not support APM or ACPI.



Select the power scheme with the most appropriate settings for this computer. Note that changing the settings below will modify the selected scheme.

Power schemes: Home/Office Desk

Settings for Home/Office Desk power scheme

When computer is:	Plugged in	Running on batteries
Turn off monitor:	After 20 mins	After 5 mins
Turn off hard disks:	Never	After 10 mins
System standby:	Never	Never
System hibernates:	Never	After 15 mins

Figure 15-1
Windows 2000 supplies power schemes appropriate for your computer; you can edit these and create new schemes.

Setting Battery Alarm Parameters

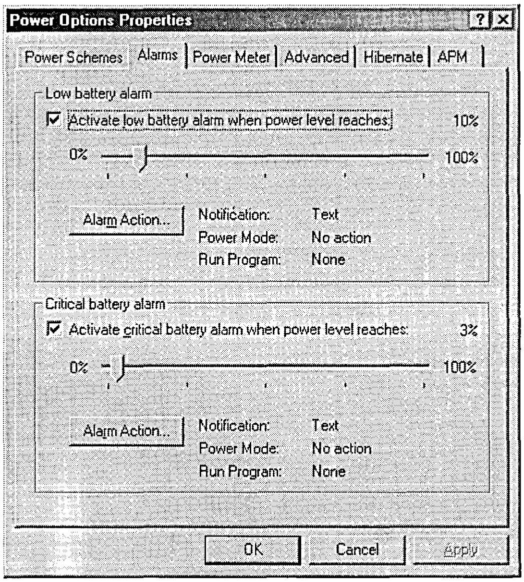
On ACPI and APM systems with batteries, Windows 2000 can display and sound alarms and take additional actions when battery power falls below a specified threshold. To set the threshold and specify the actions you want taken, go to the Alarms tab of the Power Options Properties dialog box (see Figure 15-2).

As the figure shows, you can set both a low-battery threshold and a critical battery threshold. In both cases, clicking the Alarm Action button takes you to another dialog box where you can choose the actions you want the operating system to take. Your choices there include setting the computer into standby or hibernation (if those modes are available on your system), displaying a text alert or sounding an audible one (or both), and running a program.

Displaying a Power Status Indicator

As in many corners of the Windows 2000 user interface, the Advanced tab of the Power Options Properties dialog box presents nothing the least bit advanced. It's simply a catch-all corner for miscellaneous user-interface elements.

One of those elements in the case of the Power Options Properties dialog box is an option to display a power status icon in your taskbar's notification area. Should you accept, a battery icon appears while you're running on batteries, and a power-cord icon appears when you're not. When your battery power falls below about 50 percent, the battery icon changes to a "half-full" appearance.



Low battery alarm

☑ Activate low battery alarm when power level reaches: 10%

0% 100%

Alarm Action...

Notification: Text
Power Mode: No action
Run Program: None

Critical battery alarm

☑ Activate critical battery alarm when power level reaches: 3%

0% 100%

Alarm Action...

Notification: Text
Power Mode: No action
Run Program: None

Figure 15-2
You can set two different low-battery thresholds and specify the action that Windows 2000 should take when power falls below these thresholds.

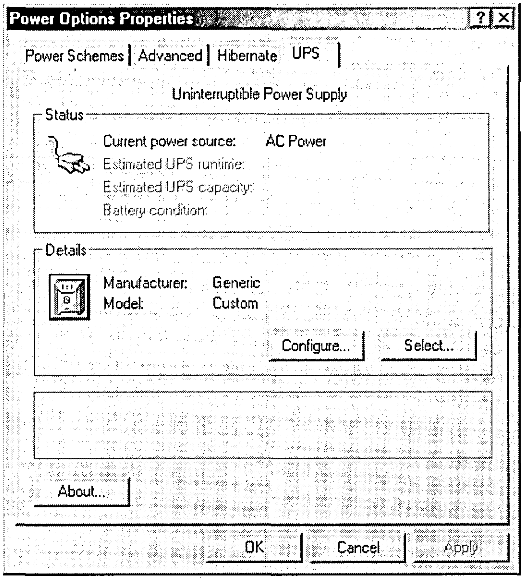
Double-clicking the icon provides more detailed information about your battery's condition. Right-clicking the icon generates a shortcut menu, from which you can return to the Power Options Properties dialog box.

Configuring an Uninterruptible Power Supply

If your computer uses a Windows 2000–supported uninterruptible power supply (UPS), a UPS tab appears in your Power Options Properties dialog box. You should visit this corner of the power-management UI to make sure that your UPS is properly identified and configured. (See Figure 15-3.)

If the UPS tab doesn't already identify the make and model of your UPS, click Select. In the ensuing dialog box, you can specify a manufacturer and model as well as the port to which the UPS is connected.

To configure the actions taken by your UPS and by Windows 2000 should your normal power become unavailable, click the Configure button. In the UPS Configuration dialog box, shown in Figure 15-4, you can specify such things as a program that should run either when the UPS battery is either close to exhaustion or when your system has been running on UPS battery power for a specified period of time.



Uninterruptible Power Supply

Status

Current power source: AC Power

Estimated UPS runtime:

Estimated UPS capacity:

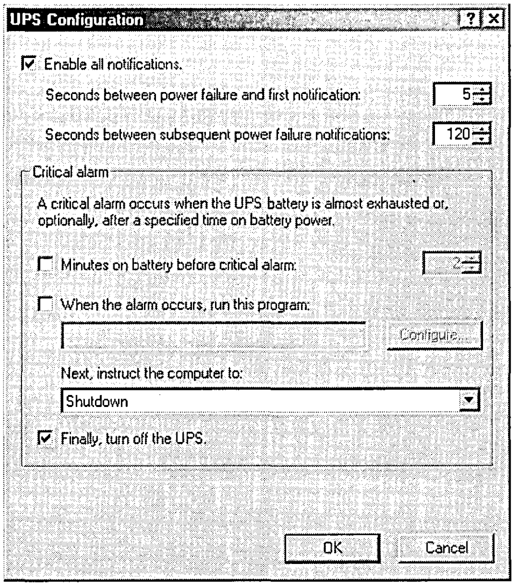
Battery condition:

Details

Manufacturer: Generic

Model: Custom

Figure 15-3
On the UPS tab, you can tell Windows 2000 which model of UPS you're using and how you want it to behave.



☑ Enable all notifications.

Seconds between power failure and first notification: 5

Seconds between subsequent power failure notifications: 120

Critical alarm

A critical alarm occurs when the UPS battery is almost exhausted or, optionally, after a specified time on battery power.

☐ Minutes on battery before critical alarm: 2

☐ When the alarm occurs, run this program:

Next, instruct the computer to:

Shutdown

☑ Finally, turn off the UPS.

Figure 15-4
In the UPS Configuration dialog box, you can tell Windows 2000 what you want it to do when the power is out and the UPS battery is approaching exhaustion.

Troubleshooting Power Management

If you think Windows 2000 should provide APM support for your computer, but it does not do so, the first thing to investigate is your computer's BIOS setup program. If APM is disabled in the BIOS when Windows 2000 is installed, the Windows 2000 Setup program does not install APM support. If APM is disabled in your system's BIOS, try reenabling it and reinstalling Windows 2000.

If you still don't have APM support after taking these measures, your BIOS might be one that Windows 2000 regards as troublesome and declines to support. You can confirm this by inspecting the file Biosinfo.inf. Or, if that's inconvenient, you can run the program Apmstat.exe, which is one of the support tools included on your Windows 2000 CD-ROM. To install the support tools, navigate to the \Support\Tools folder on the CD and then run Setup.

It's best to run Apmstat with the *verbose* switch, like this:

```
apmstat -v
```

If the news from Apmstat is disagreeable, your next step is to contact your hardware vendor and see whether a BIOS upgrade is available. Microsoft strongly recommends that you do not try to circumvent its decision not to support your current BIOS.

Difficulty Emerging from Standby

If your computer uses APM for power management and sometimes fails to come out of standby, check the time-out settings in your BIOS Setup program. If these thresholds are lower than the ones set via the Power Options Properties dialog box, you might sometimes be unable to emerge from standby.

If that doesn't solve the problem, check to see whether any of your system's devices use Windows NT 4 drivers. Microsoft says that some Windows NT 4 drivers might cause problems with power management on systems running Windows 2000. If disabling your Windows NT 4 drivers solves the power-management problem, you can determine which driver is the troublemaker by reenabling them one at a time.

For information about device drivers, see Chapter 16, "Using Device Manager and Hardware Profiles."

Known Bugs

The following two bugs are known to exist in the initial release of Windows 2000 Professional:

- Your power scheme changes from Home/Office to Portable/Laptop. When you install Windows 2000 on a system that has APM disabled, Windows uses Home/Office as its default power scheme. If you subsequently enable APM and modify the Home/Office scheme, and then reinstall or upgrade Windows 2000, the default scheme changes to Portable/Laptop. You didn't do it; Windows did. Simply change it back.
- Your power-scheme settings change. The initial release of Windows 2000 is also known to change power-scheme parameters on some systems if you disable APM support (on the APM tab of the Power Options Properties dialog box) and subsequently reenable it.

Chapter 16

Using Device Manager and Hardware Profiles

In This Chapter

Running Device Manager 270

Viewing and Printing Your System's Configuration 270

Changing a Device's Configuration 274

Updating or Changing Device Drivers 275

Understanding Device Manager's Error Codes 278

Using Hardware Profiles 279

The support for Plug and Play provided by Microsoft Windows 2000 has greatly simplified the process of installing and removing hardware devices. In many cases now, you can install a new piece of equipment simply by hooking it up. Thanks to Plug and Play, the operating system recognizes the new device, installs the required drivers, and allocates whatever resources the new device needs. Plug and Play represents a huge advance over the way hardware was managed under earlier versions of the Windows NT platform.

Nevertheless, for a variety of reasons (among them the continued widespread use of legacy devices and the remaining imperfections of Plug and Play), you will undoubtedly still need to take a hands-on approach at times to the configuration of your computer's hardware. For those times, Windows 2000 provides Device Manager, an MMC console that lets you inspect, troubleshoot, configure, update, install, and remove hardware components of your system. We survey Device Manager in this chapter.

Hardware profiles are a mechanism by which you can set up multiple hardware configurations on a single system. We look at the procedures for setting up and using hardware profiles at the end of this chapter.

Running Device Manager

You can get Device Manager running by using any of the following methods:

- Right-click My Computer, choose Manage from the shortcut menu, and select Device Manager in the console tree of Computer Management.
- Choose Start | Settings | Control Panel | System. On the Hardware tab of the System Properties dialog box, click Device Manager.
- Type *devmgmt.msc* at any command prompt.

The first of these methods displays Device Manager in the context of a larger MMC console. The second has the minor drawback of leaving a Control Panel dialog box open while you work with Device Manager. The command-line approach is the simplest and most direct. If you use Device Manager frequently, you might want to encapsulate Devmgmt.msc in a shortcut.

Installing, uninstalling, and configuring devices require that you run Device Manager under an administrative account. Therefore, if you create a shortcut to Device Manager, you might want to select the Run As Different User check box (on the Shortcut tab of the shortcut's properties dialog box). That way, you can do your normal work in a nonadministrative account and run Device Manager using your administrator's logon. *For more information, see "Running a Program Under a Different User Account," page 142.*

Viewing and Printing Your System's Configuration

The first thing to know about viewing your system's configuration in Device Manager is that Device Manager, by default, does not list all devices. Non–Plug and Play devices, local printers, and "phantom" devices (devices that are not currently connected to the system but that have not been uninstalled) are hidden by default. To display non–Plug and Play devices and local printers, choose Show Hidden Devices from the View menu. Unfortunately, you need to do that each time you run Device Manager.

To display phantom devices, follow these steps:

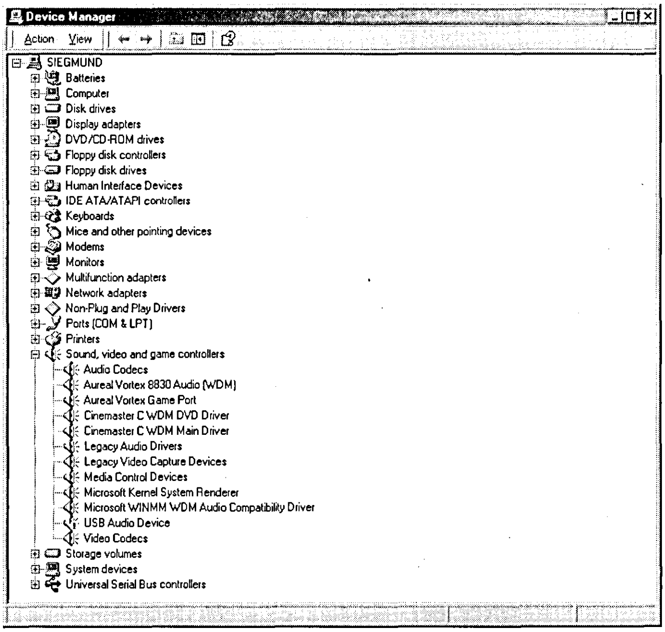
1. Run Cmd.exe.
2. At the command prompt, type *set devmgr_show_nonpresent_devices=1*
3. Still at the command prompt, type *start devmgmt.msc*

To make your phantom devices visible at all Device Manager sessions, go to Control Panel | System | Advanced | Environment Variables, and add the following to your list of System variables:

```
devmgr_show_nonpresent_devices=1
```

(You must have administrative privileges to make this change.)

As Figure 16-1 shows, Device Manager initially displays each device class on your system aş an outline entry, using the customary plus and minus signs as buttons for expanding and collapsing the outline entries. At the top of the outline, the current computer is identified by its network name. Each entry beneath the computer name represents a device class, and the subentries of each class name are your actual devices. All device-class entries are initially collapsed unless they include a problem device, in which case the problem device is flagged with a yellow exclamation point. In Figure 16-1, for example, the USB Audio Device is not correctly installed, so it gets the yellow bang.



```
SIEGMUND
    Batteries
    Computer
    Disk drives
    Display adapters
    DVD/CD-ROM drives
    Floppy disk controllers
    Floppy disk drives
    Human Interface Devices
    IDE ATA/ATAPI controllers
    Keyboards
    Mice and other pointing devices
    Modems
    Monitors
    Multifunction adapters
    Network adapters
    Non-Plug and Play Drivers
    Ports (COM & LPT)
    Printers
    Sound, video and game controllers
        Audio Codecs
        Aureal Vortex 8830 Audio (WDM)
        Aureal Vortex Game Port
        Cinemaster C WDM DVD Driver
        Cinemaster C WDM Main Driver
        Legacy Audio Drivers
        Legacy Video Capture Devices
        Media Control Devices
        Microsoft Kernel System Renderer
        Microsoft WINMM WDM Audio Compatibility Driver
        USB Audio Device
        Video Codecs
    Storage volumes
    System devices
    Universal Serial Bus controllers
```

Figure 16-1
Device Manager presents each device class as an outline entry. Devices that are not working properly are flagged with a yellow exclamation point.

Viewing Options

Device Manager offers four viewing choices in addition to the Show Hidden Devices toggle. The default, shown in Figure 16-1, is Device By Type. Using View menu commands, you can opt for Device By Connection, Resources By Type, or Resources By Connection. If you're trying to sort out a resource-contention problem—such as devices that are unable to share an IRQ line—you might want to switch to Resources By Connection or Resources By Type.

Printing Options

To print information about your system's devices and drivers, choose Print from Device Manager's View menu. The Print dialog box presents three report options:

- System Summary
- Selected Class Or Device
- All Devices And System Summary

Because the last of these generates an extremely lengthy report, the dialog box also includes a handy Print To File check box. You can use this to store a print file on disk and then copy the file to your printer at a time when printer demand is low. Alternatively, you can create a plain-text disk-file copy of the All Devices And System Summary report, as follows:

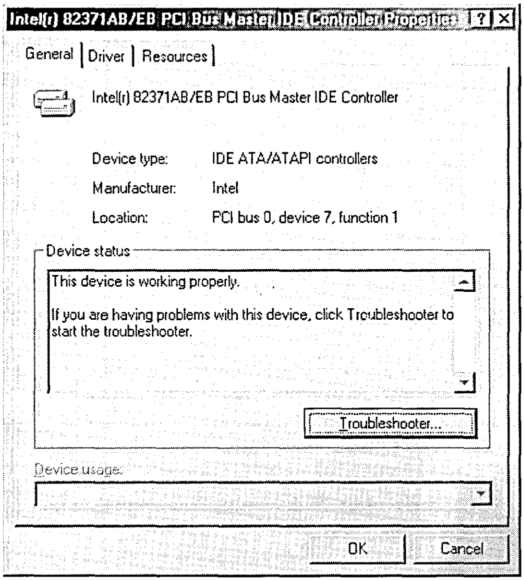
1. Choose Start | Settings | Printers | Add Printer.
2. Install the printer identified as Generic / Text Only.
3. Print the Device Manager report to the Generic / Text Only printer, using the Print To File check box.

Checking the Status of a Device

To check the status of a device, first navigate to it using Device Manager's outline controls. Then double-click the device entry to display its properties dialog box (or right-click it and choose Properties from the shortcut menu). Figure 16-2 shows a sample of a device's properties dialog box. This one includes a General tab (providing descriptive information), a Driver tab (listing the date, version, and source of the device's driver), and a Resources tab (showing which DMA channels, IRQ lines, I/O addresses, and memory ranges are used by the device). The properties dialog boxes for some devices include other information as well as options that can be selected by users.

Getting Device Driver Details

The Driver tab of a device's properties dialog box typically includes a Driver Details button. Click this button to get the file names and locations (but not the file dates) for each of the driver files used by the selected device. Figure 16-3 shows a sample of what you might see by clicking Driver Details.



Intel(r) 82371AB/EB PCI Bus Master IDE Controller Properties

Intel(r) 82371AB/EB PCI Bus Master IDE Controller

Device type: IDE ATA/ATAPI controllers

Manufacturer: Intel

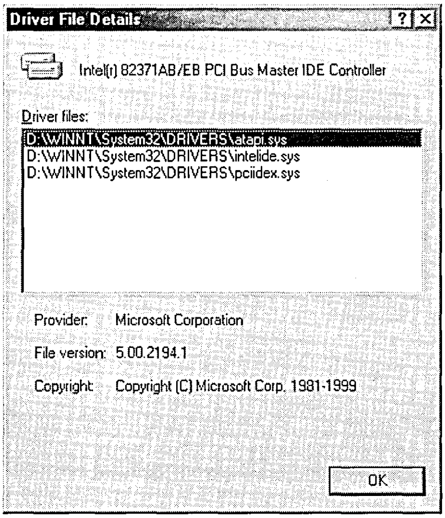
Location: PCI bus 0, device 7, function 1

Device status

This device is working properly.

If you are having problems with this device, click Troubleshooter to start the troubleshooter.

Figure 16-2
A device's properties dialog box displays descriptive information, driver details, and information about resources used by the device in question.



Driver File Details

Intel(r) 82371AB/EB PCI Bus Master IDE Controller

Driver files:

D:\WINNT\System32\DRIVERS\atapi.sys
D:\WINNT\System32\DRIVERS\intelide.sys
D:\WINNT\System32\DRIVERS\pciidex.sys

Provider: Microsoft Corporation

File version: 5.00.2194.1

Copyright: Copyright (C) Microsoft Corp. 1981-1999

Figure 16-3
Click the Driver Details button on the Driver tab of a device's properties dialog box to see the names and locations of driver files used by the selected device.

Finding Resource Conflicts

If you suspect that a device is trying to use a resource—a DMA channel, an I/O address, an IRQ line, or a memory address—that another device is also attempting to use, click the Resources tab on the device's properties dialog box. If a resource conflict involving this device exists, information about the resource in contention and the devices that are claiming it will appear in the Conflicting Device List section of the Resources tab.

Changing a Device's Configuration

Provided that you are logged on as a user with administrative privileges, you can use a device's properties dialog box to disable, reenable, uninstall, and reconfigure a device. The configuration options for certain devices are also accessible from other parts of the Windows 2000 user interface (typically Control Panel), but you can always get to them through Device Manager.

Disabling and Reenabling a Device

To disable a device, choose Do Not Use This Device (Disable) from the Device Usage list on the General tab of the device's properties dialog box. (Alternatively, right-click the device in Device Manager's console tree and choose Disable from the shortcut menu.) Device Manager will present a confirmation prompt. To reenable a disabled device, click the Enable Device button (which appears only when a device has been disabled) and follow whatever instructions appear.

Disabling a device does not remove it from Device Manager or the registry. It merely makes the device unavailable and frees the resources it was using. Disabling a device is typically a troubleshooting measure used to solve resource allocation problems. If you're not planning to use a device again, you should uninstall it.

Uninstalling a Device

You can uninstall a Plug and Play device by simply removing it physically from your system. (If it's a system-board device, shut your computer down first!) To uninstall a legacy device, right-click its entry in Device Manager's console tree, choose Uninstall from the shortcut menu, and respond to the confirmation prompt. Then physically remove the device from your system.

Changing Resource Settings

To change resource settings for a device, go to the Resources tab of the device's properties dialog box. Clear the Use Automatic Settings check box. Then, in the

Resource Settings window, select the resource whose setting you want to change. Click the Change Setting button and type the new value for the selected resource.

If the Use Automatic Settings check box is not available, either no configurable resources exist or the resources for the selected device are managed by Plug and Play and cannot be changed.

Changing Other Settings

The properties dialog boxes for many devices include other user-configurable options. In some cases, these options simply duplicate options that are available via Control Panel. For example, the Modem, Diagnostics, and Advanced tabs on your modem's properties dialog box in Device Manager are duplicated in Control Panel. (Choose Start | Settings | Control Panel | Phone And Modem Options, click the Modems tab, select a modem, and click Properties.) In other cases, however, the properties dialog boxes in Device Manager provide options not available elsewhere in the Windows 2000 user interface (that is, anywhere outside the registry)—perhaps options you didn't even know you had. You can turn off write-caching for a hard disk, for example, by visiting the Disk Properties tab in the disk's properties dialog box. You can enable digital audio for your CD-ROM drive by going to the Properties tab of its properties dialog box, or change your DVD drive's region setting by going to its Advanced Settings tab—and so on. It's worthwhile to check the properties dialog box for each device listed in Device Manager to see what choices are available.

Updating or Changing Device Drivers

It's obviously a good idea to keep your system equipped with the latest versions of its devices' drivers. Microsoft provides a Web site, called Windows Update, to assist you in this quest. One of several things the Windows Update site can do for you is scan your computer and compare your drivers with its own driver database. If it finds a newer driver for one of your devices, Windows Update can download and install it for you.

To get to the Windows Update site, choose Start | Windows Update (usually at the top of your Start menu). Or simply point your browser to *windowsupdate.microsoft.com*. On the home page of the site, click Product Updates. After the site has finished its examination of your system, you can click the Device Drivers link (in the menu on the left) to see what, if any, updated drivers the site knows about. Select check boxes for the drivers you want to download and then click the Download button.

For more details about Windows Update, see "Using Windows Update to Maintain Driver and System Files," page 676.

Third-Party Sources of Driver Updates

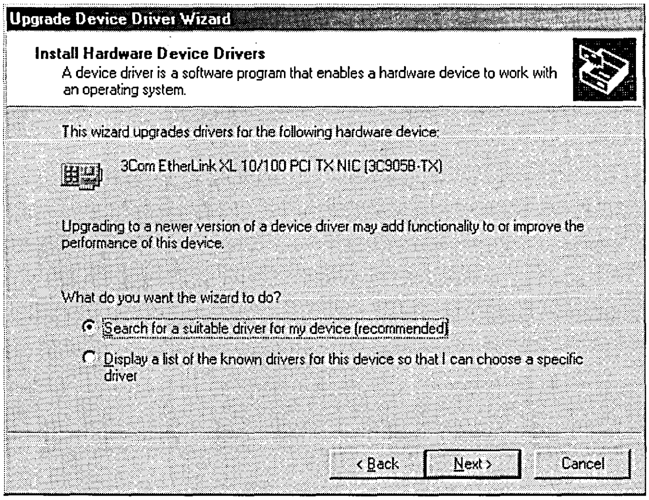
If Windows Update doesn't have an updated driver for your device, you might find one at the device vendor's own Web site. If you don't find what you need there, or if you don't know the location of your vendor's Web site, try these two third-party sites:

- *updates.zdnet.com/updates/drivers.htm*
- *www.driverguide.com*

Reinstalling a Driver

If you have reason to believe that a driver file has become corrupted, you can reinstall it as follows:

1. Double-click the device entry in Device Manager.
2. On the Driver tab of the device's properties dialog box, click Update Driver.
3. Click Next to get to the second page of the Upgrade Device Driver Wizard, shown in Figure 16-4.
4. Select Search For A Suitable Driver For My Device (Recommended) and click Next.
5. Leave the search location check boxes in their default state and click Next again.



Install Hardware Device Drivers

A device driver is a software program that enables a hardware device to work with an operating system.

This wizard upgrades drivers for the following hardware device:

3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)

Upgrading to a newer version of a device driver may add functionality to or improve the performance of this device.

What do you want the wizard to do?

● Search for a suitable driver for my device (recommended)

○ Display a list of the known drivers for this device so that I can choose a specific driver

Figure 16-4
The Upgrade Device Driver Wizard can reinstall drivers or find new ones.

Regardless of where you tell the wizard to search, it will begin by searching %SystemRoot%\Inf. (That is, it searches that default folder even if you clear all the search location check boxes.) When the wizard reports that it has found your driver, click Next one more time to reinstall the driver.

Note that all drivers supplied with Windows 2000 are stored in a single file, %SystemRoot%\Driver Cache\Driver.cab. This file is digitally signed by Microsoft and cannot be altered by third parties. If a third-party update to a system-supplied driver exists in %SystemRoot%\Driver Cache, the Upgrade Device Driver Wizard will find and install that one in preference to the one that was shipped with Windows 2000.

Installing a New Driver from a Known Location

If you download a driver from the Windows Update site or a third-party vendor's Web site, in most cases either the driver will be installed automatically or you will receive instructions about how to install it. In cases where you need to install a driver from a floppy disk, CD-ROM, network share, or some other known location, you can simply point the Upgrade Device Driver Wizard to that location:

1. Double-click the device's entry in Device Manager.
2. On the Driver tab of the device's properties dialog box, click Update Driver.
3. On the second page of the Upgrade Device Driver Wizard, select Search For A Suitable Driver For My Device (Recommended) and click Next.
4. Select Specify A Location; then clear the other search location check boxes. Click Next.
5. Specify the path of the .inf file associated with your device driver and then click Next.

The .inf file is not the driver itself, but it provides information about how the driver is to be installed. The Upgrade Device Driver Wizard needs the .inf file to proceed with the driver update.

Installing a Driver from the List of Known Drivers

The second option shown in Figure 16-4, Display A List Of The Known Drivers For This Device So That I Can Choose A Specific Driver, is useful when you want to pick a driver from the same device class, but not the default driver for your device. For example, if you want to install a driver for a CD-ROM device other than the one that's installed on your system, you can use this option to peruse all the available CD-ROM drivers. To get to the complete list of drivers available for the selected device class:

1. Double-click the device entry in Device Manager.
2. On the Drivers tab of the device's properties dialog box, click Update Driver.
3. Click Next to get to the Upgrade Device Driver Wizard's second screen. (See Figure 16-4.)
4. Select Display A List Of The Known Drivers For This Device So That I Can Choose A Specific Driver. Click Next.
5. Select Show All Hardware Of This Device Class; click Next again.

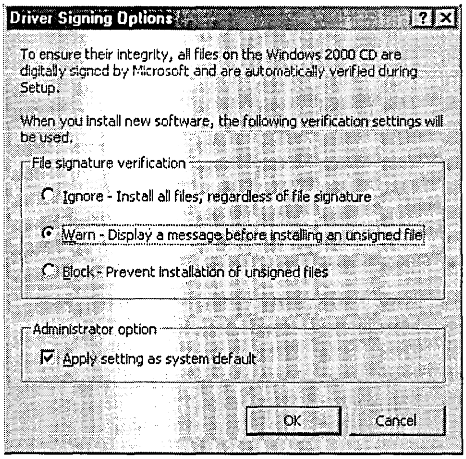
Installing Multiprocessor Support

If you upgrade your computer from a single-processor to a multiprocessor system, you might need to use the foregoing procedure to install a multiprocessor driver. Start by going to the properties dialog box for the Computer entry in Device Manager. Follow steps 2 through 5 from the preceding section. Then select the appropriate multiprocessor driver for your system and click Next.

Setting Driver Signing Options

As mentioned earlier, all drivers shipped with Windows 2000 are digitally signed by Microsoft. The digital signature is your assurance that the driver has not been altered since it passed Microsoft's quality-control tests. Other vendors might or might not add digital signatures to their own drivers.

By default, Windows 2000 warns you before installing a new driver without a valid digital signature, allowing you to decide whether you want to gamble on the unsigned item. You can change that default so that unsigned drivers are never installed or so that they are installed without question. To make either change, choose Start | Settings | Control Panel | System, click the Hardware tab, and click Driver Signing Options. Figure 16-5 shows the Driver Signing Options dialog box. If you are logged on with administrative privileges, you can use the check box at the bottom of this dialog box to make your choice apply to all users at this computer.



Driver Signing Options

To ensure their integrity, all files on the Windows 2000 CD are digitally signed by Microsoft and are automatically verified during Setup.

When you install new software, the following verification settings will be used.

File signature verification

○ Ignore - Install all files, regardless of file signature

● Warn - Display a message before installing an unsigned file

○ Block - Prevent installation of unsigned files

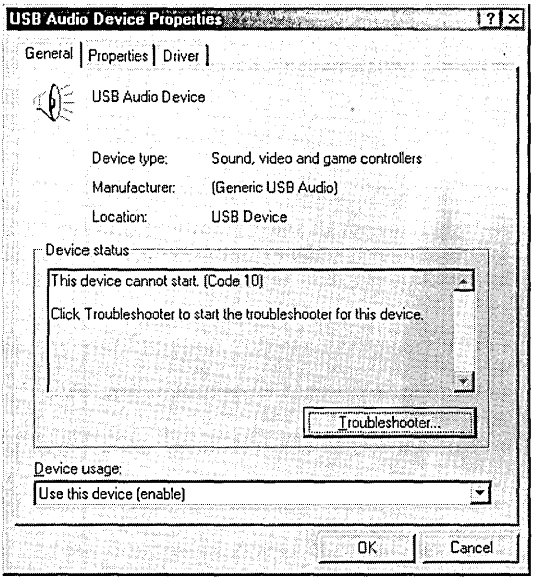
Administrator option

☑ Apply setting as system default

Figure 16-5
By default, Windows 2000 warns before installing an unsigned driver. You can opt for a higher or lower level of security.

Understanding Device Manager's Error Codes

If a device is not functioning properly, you can get some cryptic information about the nature of the problem by displaying the General tab of the device's properties dialog box. The Device Status section of the dialog box will report an error code, accompanied by a line or two of text. Often, you'll be advised to click the Troubleshooter button (shown in Figure 16-6), and, in most cases, the Troubleshooter button will fail to shoot your trouble. You can, however, read a more detailed explanation of Device Manager's 31 error codes in Microsoft Knowledge Base article Q125174, on the companion CD.



USB Audio Device

Device type: Sound, video and game controllers

Manufacturer: (Generic USB Audio)

Location: USB Device

Device status

This device cannot start. (Code 10)

Click Troubleshooter to start the troubleshooter for this device.

Device usage:

Use this device (enable)

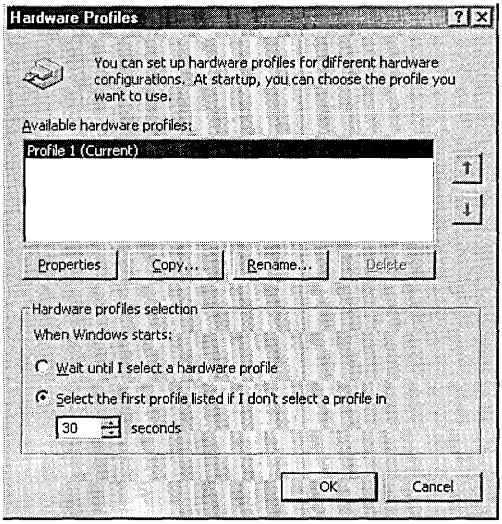
Figure 16-6
Device Manager's error codes are not particularly enlightening, and the Troubleshooter button is often of little help. You can find more details in Knowledge Base article Q125174.

Using Hardware Profiles

A *hardware profile* is a named combination of hardware settings. Hardware profiles allow you to use different sets of devices under different circumstances—for example, one set when your portable computer is docked and another when it is not docked.

The Windows 2000 Setup program creates one hardware profile. You can create as many additional ones as you want. If you have more than one profile, Windows 2000 prompts you to choose a profile when you boot the operating system.

To create a hardware profile, choose Start | Settings | Control Panel | System. Click the Hardware tab and then click Hardware Profiles. The dialog box shown in Figure 16-7 appears.



You can set up hardware profiles for different hardware configurations. At startup, you can choose the profile you want to use.

Available hardware profiles:

Profile 1 (Current)

Hardware profiles selection

When Windows starts:

○ Wait until I select a hardware profile

● Select the first profile listed if I don't select a profile in 30 seconds

Figure 16-7
Hardware profiles let you use different sets of devices under different circumstances.

Note that the dialog box has no New button. To create a new profile, you must copy an existing one. To do so, select an existing profile and click Copy. Supply a name for the new profile and then click OK.

Initially, your new profile has the same settings as the profile you copied. To adjust it (for example, to remove a device from the new profile), restart your computer using the new profile. Then open Device Manager and make the necessary changes. For example, to disable a device, double-click its entry in the console tree, go to the General tab of the properties dialog box, and select Do Not Use This Device In The Current Hardware Profile from the Device Usage list.

Part 5

Administering a System

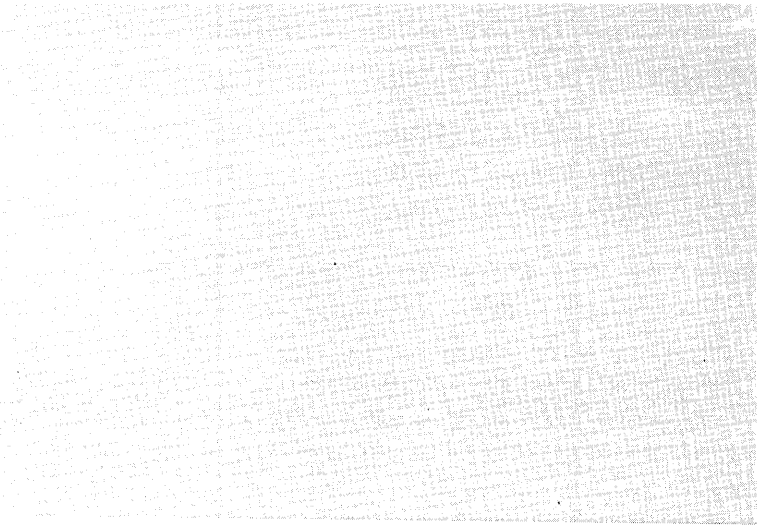
Chapter 17
Managing Users and Groups 283

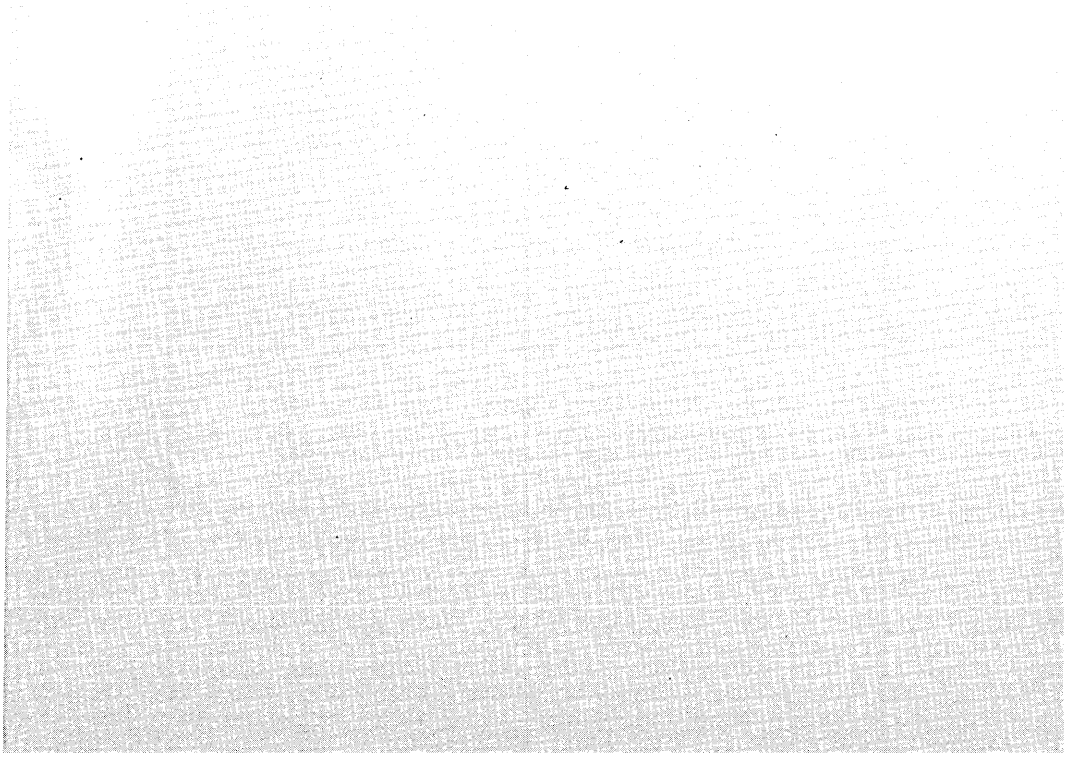
Chapter 18
Using Group Policy 297

Chapter 19
Customizing Users Work Environments 311

Chapter 20
Managing Services 331

Chapter 21
Administering Remote Systems 347





Chapter 17

Managing Users and Groups

In This Chapter

Local Accounts vs. Domain Accounts 283

Setting Up Local Users and Groups 286

Setting Security for Users and Groups 293

A basic component of security in Microsoft Windows 2000 is the user account, for all manner of rights, permissions, and privileges can be assigned or denied to a particular user account. To make administration easier, you can create groups of user accounts. You can then assign privileges to a group instead of assigning privileges to each individual user.

Local Accounts vs. Domain Accounts

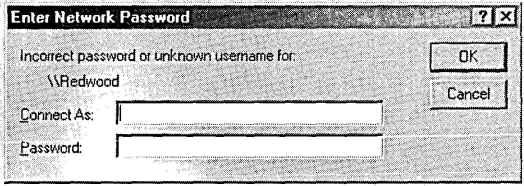
Windows 2000 stores information about user accounts and security groups in a security database. Where the security database resides depends on whether your computer is part of a workgroup or a domain.

A workgroup setup uses only local user accounts and local groups. The security database on each computer stores the local user accounts and local groups that are specific to that computer. These accounts are not accessible or recognized elsewhere on the network. With such a setup, you avoid the initial expense of purchasing and configuring Microsoft Windows 2000 Server—but because you must manage user accounts on each individual computer, it becomes unwieldy with more than five or ten computers.

Managing User Accounts in a Workgroup

In a workgroup, each computer maintains its own security database of local user accounts and groups. Networked computers do not have access to the security databases of other computers on the network. Initially, this means that, although the computers are all wired together and can see one another in My Network Places, they can't share resources with one another. You can use the following techniques to allow users on a network to access other computers:

- On each computer to which network users need access, create an account with a name and password known by all. When network users attempt to access the computer, they'll see a dialog box like the one shown here, in which they type the user name and password of an account on the target computer.



Enter Network Password

Incorrect password or unknown username for:
\\Redwood

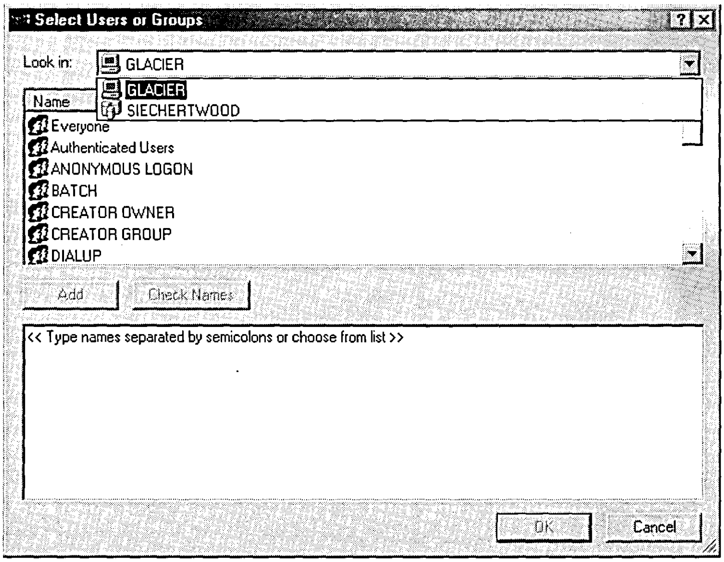
- On each computer, set up local user accounts with exactly the same user name and password. If each computer has a user account named Thomas, for example, when Thomas logs on to one computer, he can access resources to which his like-named user account has been granted access on another computer.
- On each computer, enable the Guest account. (Choose Start | Run and type *lusrmgr.msc*. In the Users folder, double-click Guest and clear the Account Is Disabled check box.) Then give the Guest account or the Guests group permission to access the folders, files, and printers that you want to share. The Guest account is the security credential that Windows 2000 uses for network access by unrecognized accounts. It's applied automatically; a user needn't explicitly log on as Guest.

To some degree, each of these solutions violates common security practices, such as frequently changing passwords. That might not be a problem in your environment; if it is, the best solution is to set up a domain using Windows 2000 Server. Be particularly careful with the Guest account, especially if your network is connected to the Internet. (You can minimize the danger by isolating your network from the Internet in various ways. *For more information, see "Securing Your Internet Connection," page 428.*)

In a domain setup, the network includes one or more computers running Windows 2000 Server or Microsoft Windows NT Server that are set up as domain controllers. A centralized security database is stored on the domain controller, which means that you can access the security database from any computer on the network. Centralized domain security offers a number of advantages, not the least of which is that it's a simple matter to allow a user to log on to any computer on the network.

Because domain accounts are a feature of Windows 2000 Server, we don't explain how to manage them in this book. However, even if your network is set up as a domain, you use the methods described in this chapter to control access to a particular computer by domain users. In some situations, you need to add domain accounts to certain local groups or assign certain user rights to domain accounts. (For example, you need to add your domain user account to a local group that has the Log On Locally user right so that you can log on using your domain account. Until you do that, you can log on only with a local user account, which doesn't have access to any network resources.)

To find domain accounts using the dialog box that appears in various places when you want to add a user or group, select either a domain name (for domain accounts) or the computer name (for local accounts) from the Look In list at the top of the dialog box. See Figure 17-1.



Look in: GLACIER

GLACIER
SIECHERTWOOD

Name
Everyone
Authenticated Users
ANONYMOUS LOGON
BATCH
CREATOR OWNER
CREATOR GROUP
DIALUP

<< Type names separated by semicolons or choose from list >>

Figure 17-1
If your computer is part of a domain, you can select domain user accounts and groups in addition to local user accounts and groups.

If you prefer to type the name of a user account or group (either in a dialog box or as part of a command), simply precede it with the domain name and a backslash (\). For example, SIECHERTWOOD\LizP refers to the LizP user account in the SIECHERTWOOD domain. You can specify local accounts in the same manner (for example, GLACIER\Thomas for Thomas's local user account on the computer named GLACIER), but you'll seldom have any reason to do so.

Setting Up Local Users and Groups

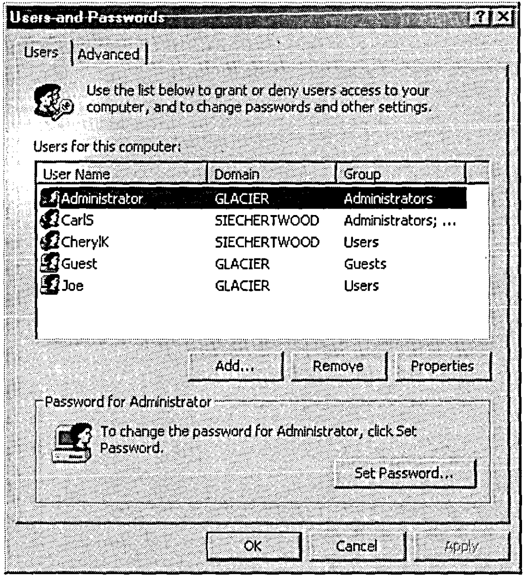
Windows 2000 includes three different interfaces for managing users and groups:

- Users And Passwords (in Control Panel)
- Local Users And Groups (an MMC snap-in)
- Command-line utilities

Which one you choose depends in part on whether you prefer a graphical interface or a command prompt. But you'll also find that each tool offers capabilities that the others don't.-

Users And Passwords in Control Panel

Reaching Users And Passwords is easy: simply go to Start | Settings | Control Panel | Users And Passwords. You'll see a dialog box similar to the one shown in Figure 17-2.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

Users for this computer:

User Name	Domain	Group
Administrator	GLACIER	Administrators
CarlS	SIECHERTWOOD	Administrators; ...
CherylK	SIECHERTWOOD	Users
Guest	GLACIER	Guests
Joe	GLACIER	Users

Password for Administrator

To change the password for Administrator, click Set Password.

Figure 17-2
Users And Passwords is useful for password changes and basic user administration.

You'll quickly find that Users And Passwords has only a few capabilities; its singular advantage over Local Users And Groups is its simplicity. If you're logged on as a member of the Administrators group, you can do the following with Users And Passwords:

- Add or remove a local user account.

- Place a local user account in a group. With Users And Passwords, you can place a user account in only one group.
- If your computer is part of a domain, you can add a domain user account to a single local group.
- Set or change the password for a local user account other than the one with which you're currently logged on. (You can't set the password for a domain user account using Users And Passwords. To set your own password—for either a local user account or a domain user account—press Ctrl+Alt+Delete and click Change Password.)

You can perform any of the preceding tasks on the Users tab. The overstated Advanced tab offers the following additional features:

- Certificate management. *(For details, see Chapter 35, "Managing Security Certificates.")*
- An Advanced button, which merely opens Local Users And Groups.
- Secure boot settings. *(For details, see "Setting Logon Options," page 37.)*

Local Users And Groups MMC Snap-In

Local Users And Groups, a Microsoft Management Console (MMC) snap-in, offers more advanced capabilities than Users And Passwords, using the now-familiar MMC interface. *(For information about MMC, see Chapter 4, "Using and Customizing Microsoft Management Console.")* You can start Local Users And Groups, shown in Figure 17-3, in any of the following ways:

- In Users And Passwords, click the Advanced tab and then click the Advanced button.
- In Computer Management, navigate to System Tools\Local Users And Groups.
- At a command prompt, type *lusrmgr.msc*.

Table 17-1 describes the tasks you can perform with Local Users And Groups.

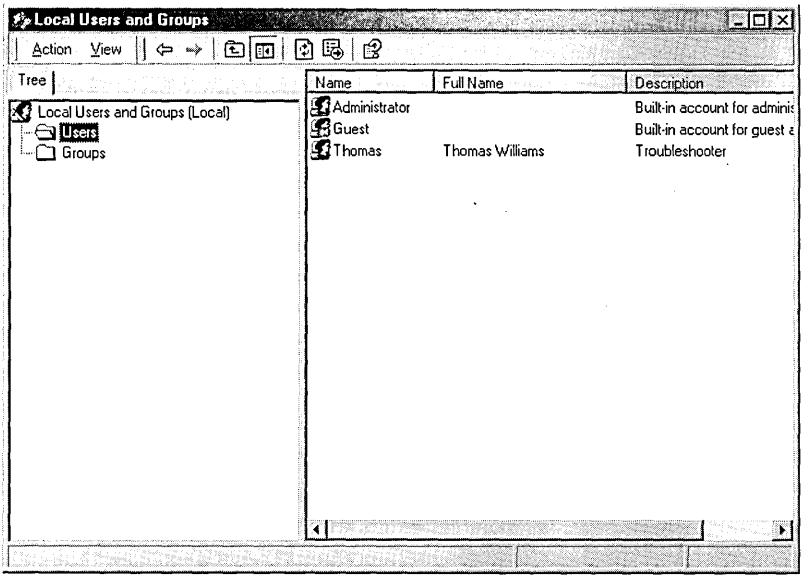
Table 17-1. Capabilities of Local Users And Groups Console

Task	Procedure
Local User Accounts	
Create	Right-click Users and choose New User.
Delete	In Users, right-click the account and choose Delete.
Set or change password	In Users, right-click the account and choose Set Password.

(continued)

Table 17-1. Capabilities of Local Users And Groups Console *(continued)*

Task	Procedure
Local User Accounts *(continued)*	
Change logon name	In Users, right-click the account and choose Rename.
Change full name or description	In Users, double-click the account to display the General tab of the properties dialog box.
Set password restrictions	In Users, double-click the account to display the General tab of the properties dialog box. *For details, see "Setting Password and Lockout Policies," page 293.*
Enable or disable	In Users, double-click the account to display the General tab of the properties dialog box, and then clear or select the Account Is Disabled check box.(When an account is disabled, the user can't log on or access resources on the computer.)
Unlock after too many	In Users, double-click the account to display the unsuccessful logon attempts General tab of the properties dialog box, and then clear the Account Is Locked Out check box.
Set group membership	In Users, double-click the account and then click the Member Of tab.
Specify profile and logon script	In Users, double-click the account and then click the Profile tab. *For details, see Chapter 19,"Customizing User Work Environments."*
Local Groups	
Create	Right-click Groups and choose New Group.
Delete	In Groups, right-click the group and choose Delete.
Rename	In Groups, right-click the group and choose Rename.
Set group membership	In Groups, double-click the group to display the properties dialog box. You can add local user accounts, local system groups, domain user accounts, and domain groups to a local group. In the Select Users Or Groups dialog box that appears when you click Add, use the Look In box to specify the computer name (for local users and groups) or domain name (for domain users and groups).



Name	Full Name	Description
Administrator		Built-in account for adminis
Guest		Built-in account for guest a
Thomas	Thomas Williams	Troubleshooter

Figure 17-3
Through its spartan interface, Local Users And Groups offers more capabilities than Users And Passwords.

One limitation of Local Users And Groups is that you can't use it to modify domain user accounts or domain groups in any way except to add them to one or more local groups. If you need to modify a domain user account or group, use one of the following methods:

- If the domain controller is running Windows 2000 Server, at the domain controller go to Start | Programs | Administrative Tools | Active Directory Users And Computers.
- If the domain controller is running Windows NT Server, at the domain controller go to Start | Programs | Administrative Tools (Common) | User Manager For Domains.

Note If you install the proper administrative tools, you can run either of these programs (Active Directory Users And Computers or User Manager For Domains) from your computer running Windows 2000 Professional. To install Active Directory Users And Computers for a Windows 2000 domain, insert the Windows 2000 Server CD and run \I386\Adminpak.msi. (Doing so installs a number of domain administration tools, including Active Directory Users And Computers.) To install User Manager For Domains for a Windows NT domain, copy Usrmgr.exe (and, optionally, its help files, Usrmgr.hlp and Usrmgr.cnt) from the domain controller's %SystemRoot%\System32 folder to a folder (either network or local) to which you have access. To successfully run either program, you must be logged on as a member of the Domain Admins group.

Command-Line Utilities

If you prefer a terse command prompt window to a gooey utility, you'll want to use Net.exe for managing local users and groups. To change any local user account or group information, you need to be logged on as a member of the local Administrators group. (Alternatively, you can use Run As to launch the Command Prompt window, or you can precede each command with *runas /user:administrator*.)

In the following sections, we describe only the most common Net commands (and their most common parameters) for managing local users and groups. This isn't an exhaustive reference, however. You can get that information from online help or by typing *net help command*, replacing *command* with the word that follows Net in the examples. For instance, to get more information about the Net Localgroup command, type *net help localgroup*. This provides more help than typing *net localgroup /?*, which shows only the command syntax.

Net User

The Net User command lets you view, add, modify, or delete user accounts.

Viewing User Account Information

Typing *net user* with no parameters causes the program to display the name of your computer and a list of local user accounts. If you follow Net User with the name of a local user account (for example, *net user thomas*), Net User displays all information about the user account, as shown in the sample that follows.

```
D:\>net user

User accounts for \\GLACIER

-------------------------------------------------------------------------
Administrator           Guest                   Thomas
The command completed successfully.


D:\>net user thomas
User name                   Thomas
Full Name                   Thomas Williams
Comment                     Troubleshooter
User's comment
Country code                000 (System Default)
Account active              Yes
Account expires             Never

Password last set           3/7/2000 3:00 PM
Password expires            3/8/2000 3:00 PM
Password changeable         3/7/2000 3:00 PM
Password required           Yes
User may change password    Yes
```

```
Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Users
```

Adding or Modifying a User Account

Following Net User *username*, you can append any or all of the parameters shown in Table 17-2. For example, you can add a new account for a user named Cheryl, create a complex password, and prevent Cheryl from changing the password with the following command:

```
D:\>net user Cheryl /add /random /passwordchg:no
Password for Cheryl is: nkHRE$oU

The command completed successfully.
```

Table 17-2. Useful Parameters for the Net User Command

Parameter	Description
password or * or /Random	Sets the password. If you type an asterisk (*), Net User prompts for the password you want to assign; it does not display the password as you type it. The /Random switch generates a hard-to-crack, eight-character password.
/Add	Creates a new user account. The user name must be 20 characters or fewer and can't contain any of these characters: " / \ [ ] : ; | = , + * ? < >
/Fullname:"*name*"	Specifies the user's full name.
/Comment:"*text*"	Provides a descriptive comment (maximum length of 48 characters).
/Passwordchg:yes or /Passwordchg:no	Specifies whether the user is allowed to change the password.
/Active:no or /Active:yes	Disables or enables the account. (When an account is disabled, the user can't log on or access resources on the computer.)

(continued)

Table 17-2. Useful Parameters for the Net User Command *(continued)*

Parameter	Description
/Expires:*date* or /Expires:never	Sets the expiration date for an account. For *date*, use the short date format set in Regional Options. The account expires at the beginning of the day on the specified date; from that time on, the user can't log on or access resources on the computer until an administrator sets a new expiration date.
/Passwordreq:yes or /Passwordreq:no	Specifies whether the user account is required to have a nonblank password.
/Times:*times* or /Times:all	Sets the times when an account is allowed to log on. For *times*, enter the days of the week you want to allow logon. Use a hyphen to specify a range of days or use a comma to list separate days. Following each day entry, specify the allowable logon times. For example, use *M-F,8am-6pm;Sa,9am-1pm* to restrict logon times to normal working hours. Use All to allow logon at any time; a blank value prevents the user from ever logging on.

Note The last three switches in Table 17-2 (/Expires, /Passwordreq, and /Times) allow you to make settings that you can't make (or even view) using Local Users And Groups. These switches provide some powerful options that are otherwise available only with Windows 2000 Server.

Deleting a User Account

To remove a user account from the local security database, simply use the /Delete switch with the Net User command, like this:

```
D:\>net user cheryl /delete
The command completed successfully.
```

Net Localgroup

The Net Localgroup command lets you view, add, modify, or delete groups.

Viewing Group Information

Type *net localgroup* with no parameters to display the name of your computer and a list of local groups. If you follow Net Localgroup with the name of a group (for example, *net localgroup "power users"*), Net Localgroup lists the members of the group.

Adding or Deleting a Group

Following Net Localgroup *groupname*, append /Add to create a new group or append /Delete to remove an existing group. When you add a group or view its information, you can optionally add a descriptive comment (maximum length of 48 characters) by appending the /Comment:*"text"* switch.

Adding or Deleting Group Members

You can add local user accounts, domain user accounts, and global groups to a local group (though you can't add other local groups). To do so, enter the names of the users or groups to add after the group name (separate multiple names with a space) and include the /Add switch. For example, to add Thomas and Cheryl to the Power Users group:

```
D:\>net localgroup "power users" thomas cheryl /add
The command completed successfully.
```

To delete one or more group members, use the same syntax, replacing the /Add switch with /Delete.

Working with Domain Accounts

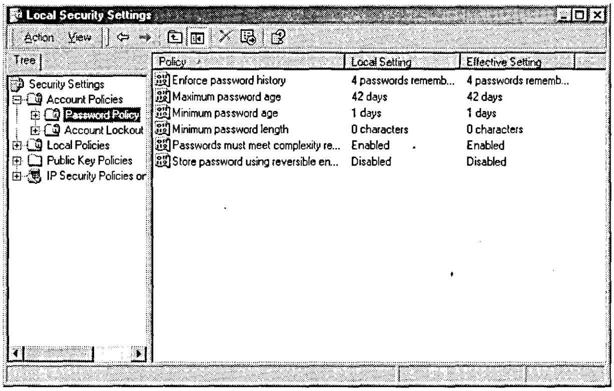
By appending the /Domain switch to any of the Net User or Net Localgroup commands described in this chapter, you can view, add, modify, or delete domain user accounts and global groups—as long as you log on as a member of the Domain Admins group. You don't need to specify the domain name; the Net User and Net Localgroup commands always work with the primary domain controller of your computer's primary domain.

Setting Security for Users and Groups

Local Security Settings is an MMC console that lets you review and set password and lockout policies for all users on a computer and assign rights to users and groups. You can open Local Security Settings, shown in Figure 17-4, by navigating to Start | Settings | Control Panel | Administrative Tools | Local Security Policy or by typing *secpol.msc* at a command prompt.

Setting Password and Lockout Policies

Using Local Security Settings, you can set a variety of parameters that control password and lockout behavior for all accounts. For each policy, Local Security Settings shows the local setting (the setting you make here) and the effective setting (the actual policy in force). The effective setting is different from the local setting if a domain-level policy, which takes precedence over local policy settings, has been set on the domain controller.



Policy	Local Setting	Effective Setting
Enforce password history	4 passwords rememb...	4 passwords rememb...
Maximum password age	42 days	42 days
Minimum password age	1 days	1 days
Minimum password length	0 characters	0 characters
Passwords must meet complexity re...	Enabled	Enabled
Store password using reversible en...	Disabled	Disabled

Figure 17-4
With Local Security Settings, you can set password requirements for all local user accounts.

Password policies place restrictions on the types of passwords users can provide and how often users can (or must) change them. Account lockout policies govern the behavior of Windows 2000 in the event that a user types an incorrect password. Table 17-3 describes each of these policies.

As an alternative to the Local Security Settings console, you can set a number of these policies using the Net Accounts command. In Table 17-3, the appropriate switch to set a policy is shown below the policy name as it appears in Local Security Settings. For example, to set the maximum password age to 21 days, you type *net accounts /maxpwage:21* at a command prompt.

Table 17-3. Account Policies

Policy, Net Accounts Switch	Description
Password Policy	
Enforce password history /Uniquepw:*number*	Specifying a number greater than 0 (the maximum is 24) causes Windows 2000 to remember that number of previous passwords and forces users to pick a different password than any of the remembered one.
Maximum password age /Maxpwage:*days*	Specifying a number greater than 0 (the maximum is 999) dictates how long a password remains valid before it expires. (To override this setting for certain user accounts, open the account's properties dialog box in Local Users And Groups and select the Password Never Expires check box.) Selecting 0 means passwords never expire. (With the Net Accounts command, use the /Maxpwage:unlimited switch if you want passwords to never expire; 0 is not an acceptable value.)

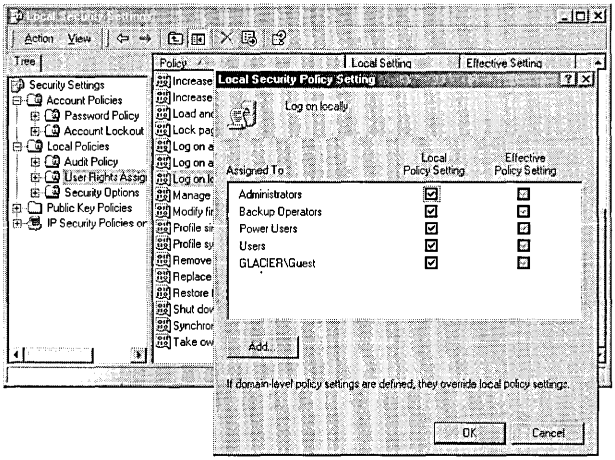
(continued)

Table 17-3. Account Policies *(continued)*

Policy, Net Accounts Switch	Description
Password Policy *(continued)*	
Minimum password age Minpwage:*days*	Specifying a number greater than 0 (the /maximum is 999) lets you set the amount of time a password must be used before a user is allowed to change it. Selecting 0 means that users can change passwords as often as they like.
Minimum password length /Minpwlen:*length*	Specifying a number greater than 0 (the maximum is 14) forces passwords to be longer than a certain number of characters. Specifying 0 permits users to have no password at all. *Note: Changes to the minimum password length setting do not apply to current passwords.*
Passwords must meet complexity requirements	Enabling this policy requires that new passwords be at least six characters long; that the password contain a mix of uppercase letters, lowercase letters, numbers, and punctuation (at least one character from three of these four classes); and that the password does not contain the user name or any part of the full name. *Note: Enabling password complexity does not affect current passwords.*
Account Lockout Policy	
Account lockout counter	Specifying a number greater than 0 (the maximum is 999) prevents a user from logging on after he or she enters a specified number of incorrect passwords within a specified time interval.
Account lockout duration	Specifying a number greater than 0 (the maximum is 99,999 minutes) specifies how long the user is to be locked out. If you specify 0, the user is locked out forever—or until an administrator unlocks the user, whichever comes first.
Reset account lockout counter after	Use this to set the time interval during which a specified number of incorrect password entries locks out the user. After this period elapses (from the time of the first incorrect password), the counter resets to 0 and starts counting again.

Setting User Rights

A *user right* is authorization to perform an operation that affects an entire computer. (A *permission*, by contrast, is authorization to perform an operation on a specific object—such as a file or a printer—on a computer.) For each user right, you can specify which user accounts and groups have the user right. To review or set user rights, go to Local Security Settings and navigate to Security Settings\Local Policies\User Rights Assignment. Then double-click a user right to view or change the list of users and groups, as shown in Figure 17-5. The *Microsoft Windows 2000 Professional Resource Kit* (Microsoft Press, 2000) contains a description of each user right.



Log on locally

Assigned To	Local Policy Setting	Effective Policy Setting
Administrators	☑	☑
Backup Operators	☑	☑
Power Users	☑	☑
Users	☑	☑
GLACIER\Guest	☑	☑

If domain-level policy settings are defined, they override local policy settings.

Figure 17-5
To review or change the local setting for a user right, double-click the user right in Local Security Settings.

Eight of the user rights—Access This Computer From The Network, Log On As A Batch Job, Log On As A Service, Log On Locally, and their corresponding "Deny" user rights—are known more precisely as *logon rights*. They control how users are allowed to access the computer—whether from the keyboard ("locally") or through a network connection, or whether as a service or as a batch job. You can use these logon rights (in particular, Log On Locally and Deny Local Logon) to control who can log on to your computer. By default, Log On Locally is granted to the local Guest account and members of the Administrators, Backup Operators, Power Users, and Users groups. If you want to prevent certain users from logging on at the keyboard (but still allow them to connect via the network, for example), create a group, add those user accounts to it, and then assign the Deny Local Logon user right to the new group. Like deny permissions, deny logon rights take precedence over allow logon rights, so if a user is a member of a group that is allowed to log on (such as Power Users) and a group that is not (such as the one described in the previous sentence), the user will not be allowed to log on. (Such users are rebuffed with an error message after they type their user name and password in the Log On To Windows dialog box.)

Chapter 18

Using Group Policy

In This Chapter

Starting Group Policy 298
Understanding the Local Group Policy Object 301
Making Settings 305
Making Different Settings for Different Users 307

Group Policy is a highly touted feature of Microsoft Windows 2000 Server and Active Directory. In that environment, Group Policy is indeed an enormously powerful feature that lets administrators configure computers throughout sites, domains, or organizational units. In addition to setting standard desktop configurations and restricting what users are allowed to change, administrators can use Group Policy to centrally manage software installation, configuration, updates, and removal; specify scripts to run at startup, shutdown, logon, and logoff; and redirect users' special folders (such as My Documents) to the network. They can customize all these settings for different computers, users, or groups.

But Group Policy can also be a useful tool for managing computers on a small network or even for managing a single computer with multiple users. Using only the local Group Policy object on a computer running Microsoft Windows 2000 Professional, you can

- Manage registry-based policy—everything from configuring the desktop to hiding certain drives to preventing the creation of scheduled tasks. These settings —and hundreds more—are stored in the HKLM and HKCU branches of the registry, which you could edit directly. But Group Policy provides two distinct advantages: it's much easier to use than a registry editor, and it periodically updates the registry automatically (thereby keeping your policies in force even if the registry is somehow modified by other means).

- Assign scripts for computer startup, computer shutdown, user logon, and user logoff.
- Specify security options.

Starting Group Policy

You make Group Policy settings using the Group Policy snap-in for Microsoft Management Console (MMC), which is shown in Figure 18-1. Windows 2000 includes an MMC console that shows only this snap-in, but you won't find it on the Start menu. To launch the console, go to Start | Run and type *gpedit.msc*. You must be logged on as a member of the Administrators group to use Group Policy.

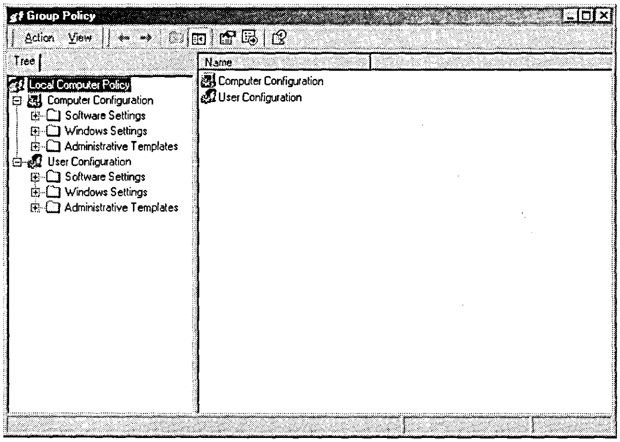


Figure 18-1
Typing *gpedit.msc* at a command prompt launches the Group Policy console.

If your computer is a member of a Windows 2000 Server domain with Active Directory–based policies, and if you have appropriate domain administrative privileges, you can configure Group Policy to display snap-in extensions that let you view and modify domain policies as well as extensions for the local Group Policy object. *(For more information, see "How Local Group Policy Settings Interact with Active Directory–Based Group Policy Settings," page 303.)* However, because our focus in this book is Windows 2000 Professional, in this chapter we explore only the local Group Policy object.

Starting Group Policy for a Remote Computer

With some MMC snap-ins (for example, Computer Management), you can use a menu command to switch from the local computer to another computer on your network. Such is not the case with Group Policy, which, once started, directs its attention toward a single computer. You can, however, start Group Policy with its gaze turned toward another computer. To do that, you must have administrative privileges on both your own computer and the other computer. Even without Windows 2000 Server and Active Directory, you can administer all the computers on your network from a single console. (A key difference is that you must set local Group Policy on each computer rather than setting Active Directory–based Group Policy that automatically applies to all computers.) You can use either of two methods to start Group Policy for a remote computer: a command-line parameter or a custom MMC console.

The simplest method is to append the /Gpcomputer parameter, as we did in this example:

```
gpedit.msc /gpcomputer:"redwood"
```

The computer name that follows /Gpcomputer can be either a NetBIOS-style name (as shown here) or a DNS-style name (for example, redwood.swdocs.com), which is the primary naming form used by Windows 2000 Server domains. In either case, you must enclose the computer name in quotation marks.

An alternative is to create a custom console that opens the local Group Policy object on another computer. The advantage of this approach is that you can create a single console that can open Group Policy for each computer you want to manage. To create a custom console:

1. Go to Start | Run and type *mmc*.
2. Open the Console menu and choose Add/Remove Snap-In.
3. On the Standalone tab, click Add.
4. Select Group Policy and click Add.
5. In the Select Group Policy Object dialog box, click Browse.
6. On the Computers tab, select Another Computer, and then type the name of the computer or click Browse to select it from a list.
7. Click OK and then click Finish.
8. Repeat steps 4 through 7 to add other computers to the console.
9. Click Close and then click OK.

For more information, see "Creating Your Own MMC Consoles," page 73.

Customizing the Group Policy Window

The Group Policy console has some easily overlooked options that you won't find in other MMC snap-ins. You can add or remove administrative templates, and you can restrict the view to show only the policies that have been configured.

Adding or Removing Policy Templates

The Administrative Templates folders (under Computer Configuration and User Configuration) are extensible. The Administrative Templates policies are defined in an .adm file. Windows 2000 includes several .adm files, of which three are displayed by default, as shown in Table 18-1.

Table 18-1. Administrative Template Files Included with Windows 2000

File Name	Description
Conf.adm (displayed by default)	Conferencing settings for NetMeeting that appear in Administrative Templates\Windows Components\NetMeeting (under Computer Configuration and User Configuration)
Inetcorp.adm	Microsoft Internet Explorer settings for use with Internet Explorer Administration Kit (IEAK), not Group Policy
Inetres.adm (displayed by default)	Microsoft Internet Explorer settings that appear in Administrative Templates\Windows Components\Internet Explorer (under Computer Configuration and User Configuration)
Inetset.adm	Microsoft Internet Explorer settings for use with Internet Explorer Administration Kit (IEAK), not Group Policy
System.adm (displayed by default)	A wide variety of settings for Windows 2000, encompassing most of the policies that appear in Group Policy
Wmp.adm	Windows Media Player settings that appear in Administrative Templates\Windows Media Player (under Computer Configuration and User Configuration)

You might want to remove the templates that contain policies you never use, or you might want to add a custom template provided with another program. For example, the Office Resource Kit includes policy templates for managing Microsoft Office 2000; for details, visit *www.microsoft.com/office/ork.* (Creating a custom template requires in-depth knowledge of both the registry and Group Policy, but the file format is actually rather simple. If you're interested in creating a custom template, study the .adm files in %SystemRoot%\Inf. To get more information, click the Help button in Group Policy, click the Index tab, and select ".adm files, creating.")

To add or remove a policy template, right-click Administrative Templates (either folder) and choose Add/Remove Templates. After you make your changes and click Close in the Add/Remove Templates dialog box, the Administrative Templates folder that you right-clicked (Computer Configuration or User Configuration) reflects your new selections. The other folder, however, continues to display policies as if you hadn't changed a thing, which might lead you to believe that you must make your selections independently for each folder. You don't; this is a bug. The simplest way to refresh both folders after you add or remove a template is to close and restart Group Policy.

Adding a policy template merely copies the .adm file to %SystemRoot%\System32\GroupPolicy\Adm; removing a template deletes the copy in that folder. Adding or removing policy templates does not change the underlying policy settings, if any; it only controls whether those policies are displayed in Group Policy.

Displaying Only Configured Policies

After you configure your local Group Policy as you want it (as described later in this chapter), you can clean up the display by hiding the myriad policies that you aren't interested in setting. It's easy to do: just right-click Administrative Templates and choose View | Show Configured Policies Only. This command is a toggle; to redisplay the full complement of policies, simply choose the command again.

Unlike the Add/Remove Templates command, Show Configured Policies Only applies only to the Administrative Templates folder that you select. If you want to filter the policies in both Computer Configuration and User Configuration, you must repeat the process in each folder.

Understanding the Local Group Policy Object

A *Group Policy object* (often abbreviated as GPO) is simply a collection of Group Policy settings. In a Windows 2000 Server–based domain, Group Policy objects are stored at the domain level and affect users and computers based on their membership in sites, domains, and organizational units. Each computer running Windows 2000 (any version) also has a single *local Group Policy object*. Because it doesn't rely on Windows 2000 Server, that's the one we focus on here.

The local Group Policy object is stored as a series of files and folders in the %SystemRoot%\System32\GroupPolicy folder. By default, the local Administrators group and the operating system itself have Full Control permissions for this folder and all the objects it contains; authenticated users have Read and Execute permissions. The GroupPolicy folder typically contains the following files and folders:

- **Gpt.ini.** This file stores information about which extensions (identified by their globally unique identifier, or GUID) contain modified settings and whether the Computer Configuration or User Configuration branch is disabled.
- **Adm.** This folder contains the administrative templates (stored as .adm files) that are in use. *(See "Adding or Removing Policy Templates," earlier in this chapter.)*
- **User.** This folder holds the Registry.pol file, which contains registry settings that apply to users. The User folder includes these subfolders:
  - Microsoft\IEAK contains settings for the items that appear in the \User Configuration\Windows Settings\Internet Explorer Maintenance folder in Group Policy.

    - Scripts includes two folders, Logon and Logoff, which contain the scripts that run when a user logs on or logs off.
- **Machine.** This folder holds the Registry.pol file, which contains registry settings that apply to the computer. Within the Machine folder is a Scripts subfolder that holds two folders, Startup and Shutdown; these contain the scripts that run when the computer starts up or shuts down.

Note Some of these files and folders are created only when you run Group Policy and make some settings.

How Group Policy Works

The majority of the Group Policy settings are in the Administrative Templates extension of the Group Policy snap-in. (As noted elsewhere in this chapter, the content of the Administrative Templates folders is derived from the .adm files in the Group Policy object.) When you configure a policy in the Administrative Templates folder (that is, you select either Enabled or Disabled and, optionally, set a value), Group Policy stores that information as a custom registry setting in one of the two Registry.pol files. As you'd expect, Group Policy uses the copy of Registry.pol in %SystemRoot%\System32\GroupPolicy\Machine for settings you make in the Computer Configuration\Administrative Templates folder in Group Policy and uses the copy in User for settings you make in User Configuration\Administrative Templates.

Computer-related Group Policy settings—those stored in Machine\Registry.pol—are copied to the appropriate registry keys in the HKLM hive when the operating system initializes and during the periodic refresh. User-related settings (in User\Registry.pol) are copied to the appropriate keys in HKCU when a user logs on and during the periodic refresh.

Note Group Policy settings—either local or Active Directory–based—take precedence over user settings (that is, settings that you make through Control Panel and other methods available to ordinary users). This is because Group Policy settings are not written to the "normal" key for a particular setting; instead, they're written to a value in a "policies" key. For example, if you use the Taskbar And Start Menu Properties dialog box to disable personalized menus, the data in the Intellimenus value in the HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced key changes. But if you use Group Policy, the Intellimenus value in the HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer key changes instead. In cases of conflicts, the value under the Policies key overrules the other.

The *periodic refresh* occurs at intervals that you define as a Group Policy setting. By default, the Registry.pol files are copied to the registry every 90 minutes plus a random offset of 0 to 30 minutes. (The random offset is intended for Active Directory–based policies; on a large network, you wouldn't want all the refresh activity occurring simultaneously. For local Group Policy, the offset serves no useful purpose but is added anyway.) By enabling and modifying the settings in Computer Configuration\Administrative Templates\System\Group Policy\Group Policy Refresh Interval For Computers and in User Configuration\Administrative Templates\System\Group Policy\Group Policy Refresh Interval For Users, you can change the interval and the random offset. You can set the interval to any value from 0 minutes (in which case settings are refreshed every 7 seconds) through 64,800 minutes (45 days).

How Local Group Policy Settings Interact with Active Directory–Based Group Policy Settings

If your computer is part of a Windows 2000 Server–based network, it might be affected by Group Policy settings other than those you set in the local Group Policy object. Group Policy settings are applied in this order:

1. Settings from the local Group Policy object
2. Settings from site Group Policy objects, in administratively specified order
3. Settings from domain Group Policy objects, in administratively specified order
4. Settings from organizational unit Group Policy objects, from largest to smallest organizational unit (parent to child organizational unit), and in administratively specified order at the level of each organizational unit

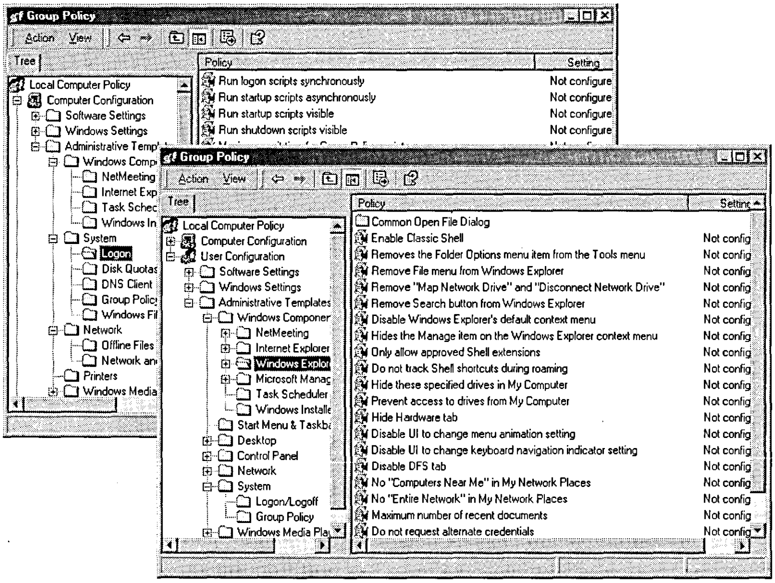
Policies applied later overwrite previously applied policies, which means that in a case of conflicting settings, the highest-level Active Directory–based policy settings take precedence. The policy settings are cumulative, so all settings contribute to the effective policy.

To view and manage Active Directory–based policies, use two MMC snap-ins: Active Directory Users And Computers and Active Directory Sites And Services.

Types of Settings

The Computer Configuration branch of Group Policy includes a variety of computer-related settings, and the User Configuration branch includes a variety of user-related settings. Figure 18-2 shows some of the major headings in the Administrative Templates folder of each branch. The line between computer settings and user settings is often blurred. Because with local Group Policy all settings apply to all users, your best bet for discovering the policies you need is to examine them all. With more than

100 computer settings and more than 350 user settings, this sounds like a daunting task—but you'll find that you can quickly scan the policies in each folder and ignore most of them.



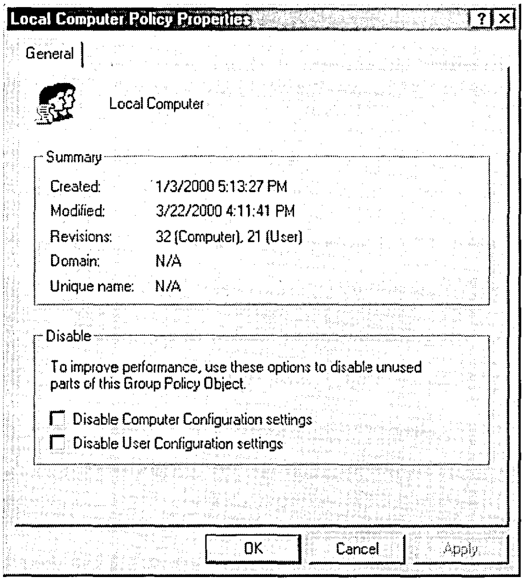
Policy	Setting
Run logon scripts synchronously	Not configure
Run startup scripts asynchronously	Not configure
Run startup scripts visible	Not configure
Run shutdown scripts visible	Not configure

Policy	Settinc
Common Open File Dialog	
Enable Classic Shell	Not config
Removes the Folder Options menu item from the Tools menu	Not config
Remove File menu from Windows Explorer	Not config
Remove "Map Network Drive" and "Disconnect Network Drive"	Not config
Remove Search button from Windows Explorer	Not config
Disable Windows Explorer's default context menu	Not config
Hides the Manage item on the Windows Explorer context menu	Not config
Only allow approved Shell extensions	Not config
Do not track Shell shortcuts during roaming	Not config
Hide these specified drives in My Computer	Not config
Prevent access to drives from My Computer	Not config
Hide Hardware tab	Not config
Disable UI to change menu animation setting	Not config
Disable UI to change keyboard navigation indicator setting	Not config
Disable DFS tab	Not config
No "Computers Near Me" in My Network Places	Not config
No "Entire Network" in My Network Places	Not config
Maximum number of recent documents	Not config
Do not request alternate credentials	Not config

Figure 18-2
The Computer Configuration and User Configuration branches owe their separation more to registry structure than to pure logic.

Some settings appear in both User Configuration and Computer Configuration. In a case of conflicting settings, the Computer Configuration setting always takes precedence.

You can speed up the application of Group Policy settings by disabling those you don't use. To see at a glance which types of policies are in use, right-click Local Computer Policy and choose Properties. In the dialog box that appears (see Figure 18-3), the Revisions line in the Summary box shows the number of Computer Configuration and User Configuration settings in use. If either value is 0 (or if you want to disable Group Policy settings for some other reason), select the appropriate check box in the Disable box.



Local Computer

Summary

Created: 1/3/2000 5:13:27 PM
Modified: 3/22/2000 4:11:41 PM
Revisions: 32 (Computer), 21 (User)
Domain: N/A
Unique name: N/A

Disable

To improve performance, use these options to disable unused parts of this Group Policy Object.

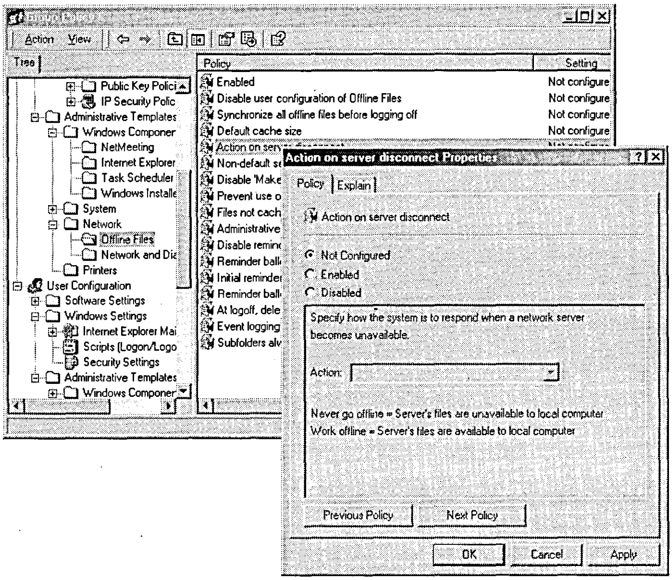
□ Disable Computer Configuration settings
□ Disable User Configuration settings

Figure 18-3
You can selectively disable computer-related or user-related Group Policy settings.

Making Settings

Each policy in the Administrative Templates folders of Group Policy has one of three settings: Not Configured, Enabled, or Disabled. By default, all policies in the local Group Policy object are initially set to Not Configured. (The policies in the Windows Settings folders do not have a Not Configured option and therefore have other default settings.)

To change a setting, simply double-click the name of the policy you want to change. The properties dialog box then appears. The dialog box for each policy under Administrative Templates looks much like the one shown in Figure 18-4. The Policy tab includes the three options—Not Configured, Enabled, and Disabled—and a large area where you can make policy-specific settings. Controls in the center area remain dimmed unless you select the Enabled option. (Many simple policies leave this area blank because the policy needs no further setting.) The Explain tab provides detailed information about the policy; the only place you're likely to find more information about each policy is in the *Microsoft Windows 2000 Professional Resource Kit* (Microsoft Press, 2000), which includes a detailed reference on its companion CD. Both tabs include Previous Policy and Next Policy buttons, which make it convenient to go through an entire folder without opening and closing the properties dialog box for each policy individually.



Policy	Setting
Enabled	Not configure
Disable user configuration of Offline Files	Not configure
Synchronize all offline files before logging off	Not configure
Default cache size	Not configure
Action on serv	
Non-default s	
Disable 'Make	
Prevent use o	
Files not cach	
Administrative	
Disable remin	
Reminder ball	
Initial reminde	
Reminder ball	
At logoff, dele	
Event logging	
Subfolders alv	

Action on server disconnect Properties

Action on server disconnect

● Not Configured
○ Enabled
○ Disabled

Specify how the system is to respond when a network server becomes unavailable.

Action:

Never go offline = Server's files are unavailable to local computer
Work offline = Server's files are available to local computer

Figure 18-4
Properties dialog boxes for all Administrative Templates policies are similar to the one shown here.

Note Pay close attention to the name of each policy, because the settings can be counterintuitive. A number of policies begin with the word *disable* (for example, Disable Autoplay in Computer Configuration\Administrative Templates\System). For those policies, if you want to *allow* the specified option, you must select the *Disable* setting. (In other words, you must disable the disabling policy.) Conversely, if you want to prohibit the option, you must select Enable.

Table 18-2. Policy Information in this Book

For Information About	See
Computer Configuration\Windows Settings	
\Scripts (Startup/Shutdown)	"Using Scripts that Run at Logon, Logoff, Startup, and Shutdown," page 320
\Security Settings\Account Policies	"Setting Password and Lockout Policies," page 293
\Security Settings\Local Policies\Audit Policy	"Enabling Auditing," page 576
\Security Settings\Local Policies \User Rights·Assignment	"Setting User Rights," page 296

(continued)

Table 18-2. Policy Information in this Book *(continued)*

For Information About	See
Computer Configuration\Windows Settings *(continued)*	
\Security Settings\Local Policies\Security Options	"Setting Logon Security Options," page 40
\Security Settings\Public Key Policies	*Chapter 33 "Using Encryption"*
\Security Settings\IP Security Policies on Local Machine	"Using IPSec," page 490
User Configuration\Windows Settings	
\Internet Explorer Maintenance	"Configuring Internet Explorer with Group Policy," page 450
\Scripts (Logon/Logoff)	"Using Scripts that Run at Logon, Logoff, Startup, and Shutdown," page 320

Making Different Settings for Different Users

Centrally managed Group Policy settings—that is, those that are stored in Active Directory on a Windows 2000 Server—can be applied to individual users, computers, or groups of either. You can have multiple sets of Active Directory–based Group Policy objects, allowing you to create an entirely different collection of settings for different users or computers.

Such is not the case with local Group Policy. Local Group Policy settings apply to all users who log on to the computer. (If the computer is part of a domain, however, the local settings might be overridden by Active Directory–based settings. *For details, see "How Local Group Policy Settings Interact with Active Directory–Based Group Policy Settings," page* 303.) You can't have multiple sets of local Group Policy objects.

Although you can't have customized settings for each of several different groups, you can effectively have two groups of users: those who are affected by local Group Policy settings and those who are not. This duality affects only the User Configuration settings; Computer Configuration settings are applied before anyone logs on.

You can do this because local Group Policy depends on users having Read access to the local Group Policy object, which is stored in the %SystemRoot%\System32\GroupPolicy folder. Policies are not applied to users who do not have Read access; therefore, by denying Read access to administrators or others whom you don't want to restrict, you free those users from control by group policies. To use this method:

1. Make the Group Policy setting changes that you want.

2. In Windows Explorer, right-click the %SystemRoot%\System32\GroupPolicy folder and choose Properties. (GroupPolicy is a hidden folder; if you can't find it in System32, choose Tools | Folder Options | View | Show Hidden Files And Folders.)
3. On the Security tab of the GroupPolicy Properties dialog box, select the Administrators group and select the Deny check box for the Read permission. (If you want to exclude any other users or groups from Group Policy control, add them to the list of names and then deny their Read permission.)

Note You must deny the Read permission rather than simply clearing the Allow check box. Otherwise, all users would continue to inherit Read permission because of their automatic membership in the Authenticated Users group.

At your next logon using one of the Read-disabled user accounts, you'll find that you're no longer encumbered by Group Policy settings. Without Read permission, however, you'll find that you're also unable to run Group Policy—so you can't view or modify Group Policy settings. To regain that power, you need to revisit the GroupPolicy Properties dialog box and grant yourself Full Control permission.

Keep in mind that, even without the aforementioned security shenanigans, the default security settings effectively produce two groups of users. Although the local Group Policy settings apply to all users (clarification: all users who have Read access to the local Group Policy object), only members of the local Administrators group can view or change these settings. Therefore, if you want to lock down a computer using Group Policy settings, you can do so—and still have a back door by which you can change the settings when you need to. Simply use the Run As command whenever you need to run Group Policy. You can do that in any of the following ways:

- At a command prompt, type *runas /u:administrator gpedit.msc.*
- Hold down the Shift key while you right-click Gpedit.msc or a shortcut to it, and then choose Run As.
- If you need to run Group Policy frequently, create a shortcut to Gpedit.msc. Right-click the shortcut, choose Properties, and select the Run As Different User check box (on the Shortcut tab).

If customizing the effects of Group Policy settings based on group membership is important to you, you should install Windows 2000 Server and set up Active Directory. But the methods described in this section can provide an easy compromise solution.

Using System Policy Editor

System Policy Editor, the predecessor to Group Policy, offers another way to make different policy settings for different users. With it, in fact, you can tailor your settings to individual users or groups, unlike local Group Policy, which, at best, allows you to make settings for two different types of users. Not all of the same policy settings are available with System Policy Editor, however.

Obtaining System Policy Editor is easy if you have Windows 2000 Server. (Of course, if you have Windows 2000 Server, Active Directory–based Group Policy should serve all your Group Policy needs, but that's another story.) If you have the Windows 2000 Server CD, open a Command Prompt window, navigate to the CD's \I386 folder, and enter the following commands:

```
expand -r poledit.ex_ %systemroot%
expand -r poledit.ch_ %systemroot%\help
expand -r common.ad_ %systemroot%\inf
expand -r winnt.ad_ %systemroot%\inf
```

Then type *poledit* at any command prompt to launch System Policy Editor.

If you don't have Windows 2000 Server, you can obtain System Policy Editor as part of the Office Resource Kit. Although it's a big download that includes a lot besides System Policy Editor, it's free. Go to *www.microsoft.com/office/ork.*

Chapter 19

Customizing User Work Environments

In This Chapter

Understanding User Profiles 312
Working with User Profiles 316
Using Scripts That Run at Logon, Logoff, Startup, and Shutdown 320
Using IntelliMirror Features Without Windows 2000 Server 322

Like earlier versions of Microsoft Windows, Microsoft Windows 2000 Professional offers users all manner of customization possibilities. Using various settings in Control Panel and elsewhere, users can control the appearance of their desktop, taskbar, Start menu, folder windows, and other items; specify sounds that play when certain events occur; add or remove programs; and so on. This is terrific for a single computer operated by a single user who wants to master his or her working environment. You can find detailed information about such settings in *Running Microsoft Windows 2000 Professional* (Microsoft Press, 2000).

But if you have to keep more than one computer humming along and keep more than one user productive, you as an administrator might want to perform some of this customization for the user. With tools provided by Windows 2000, you can make settings for users who lack the knowledge, experience, or time to make settings on their own. Just as important, you can impose restrictions that prevent inexperienced or devious users from damaging their setup.

Windows 2000 Professional, managed locally (that is, as a stand-alone computer or a member of a workgroup, not a domain), offers the following administrative customization features:

- Unattended installation. *(See "Using Answer Files for Automated Installation," page 16.)*
- Sysprep, a tool for duplicating installed systems. *(See "Using Disk Imaging," page 23.)*

- Administrative templates for making registry-based settings using the local Group Policy object. *(See Chapter 18, "Using Group Policy.")*
- Security settings. *(See Table 18-2, page 306, for references to information about security settings.)*
- Scripts. *(See "Using Scripts That Run at Logon, Logoff, Startup, and Shutdown," page 320.)*
- Internet Explorer maintenance. *(See "Configuring Internet Explorer with Group Policy," page 450.)*
- User profiles. *(See "Working with User Profiles," page 316.)*

The following user configuration settings can be made on computers running Windows 2000 Professional—but only when they're part of a Microsoft Windows 2000 Server domain that uses Active Directory and domain-based Group Policy. Because of their reliance on Windows 2000 Server, we don't describe them further in this book. However, you can enjoy *some* of these features, albeit in greatly limited form:

- Software Installation and Maintenance (Assign and Publish), which causes software and optional features to be automatically installed as needed and where needed; Software Installation and Maintenance is a component of the IntelliMirror management technologies
- User Data Management (another IntelliMirror component), which allows data and documents to follow a user from one computer to another on the network, using Server-only technologies that include folder redirection, offline folders, and domain-based Group Policy
- User Settings Management (the other IntelliMirror component), which allows users to see their preferred desktop arrangement from any computer, using Server-only technologies that include roaming user profiles and domain-based Group Policy
- Remote operating-system installation, which allows an administrator to set up a server that responds to remote-boot–enabled computers so that the server installs Windows 2000 Professional on the computers' local disk

For details, see "Using IntelliMirror Features Without Windows 2000 Server," page 322.

Understanding User Profiles

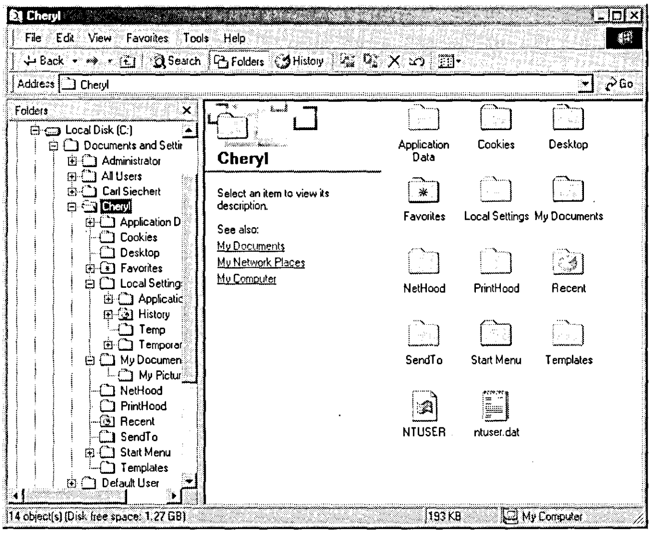
A *user profile* contains all the desktop settings for a user's work environment. But it's much more than that. In addition to storing the user's personal registry settings for everything from desktop wallpaper to the author initials used in Microsoft Word, the profile contains a number of files that are specific to a user, such as cookies the user receives while using Microsoft Internet Explorer, documents in the My Documents folder and its subfolders, and shortcuts to network places.

Location and Content of User Profiles

By default, each user who logs on to a computer has a local user profile, which is created when the user logs on for the first time. Local user profiles are stored in %SystemDrive%\Documents And Settings. Each user's profile is stored in a subfolder with the user name as the folder name. The full path of one of the profiles on a computer in our office is C:\Documents And Settings\Cheryl, for example. (The entire path for the current user's profile is stored in another commonly used environment variable, %UserProfile%.)

Note If you upgraded from Windows NT 4 (instead of performing a clean installation or upgrading from another version of Windows), user profiles are stored in %SystemRoot%\Profiles. If the computer mentioned in the previous paragraph had been upgraded from Windows NT 4, for example, Cheryl's local user profile would have been stored in C:\Winnt \Profiles\Cheryl.

Within a user's profile folder, you'll find a hierarchy of folders, as shown in Figure 19-1. The "root" of the profile (that is, the subfolder of Documents And Settings with the user name as the folder name) contains Ntuser.dat, which is the user portion of the registry (in other words, the HKCU hive). In addition, a computer that's a member of a Microsoft Windows NT Server domain might have an Ntuser.pol file, a file that has system policy settings. (System policy is the Windows NT predecessor to Group Policy.)



Select an item to view its description.

See also:
My Documents
My Network Places
My Computer

Figure 19-1
Each user profile contains a number of folders.

The folders in the profile contain the following information:

- **Application Data.** This hidden folder contains application-specific data, such as a custom dictionary for word processing programs, junk sender lists for an e-mail program, a CD database for a program that plays music CDs, and so on. Application vendors decide what information to put in this folder.
- **Cookies.** This folder contains Internet Explorer cookies.
- **Desktop.** This folder contains all items stored on the user's desktop, including files and shortcuts.
- **Favorites.** This folder contains Internet Explorer favorites.
- **Local Settings.** This hidden folder contains settings that don't roam with the profile, either because they're machine-specific or because they're so large that it's not worthwhile to include them in a roaming user profile, which must be copied from and to a network server at each logon and logoff. The Local Settings folder contains four subfolders:
    - **Application Data.** This hidden folder contains machine-specific application data.
    - **History.** This folder contains the user's Internet Explorer browsing history.
    - **Temp.** This folder contains temporary files created by applications.
    - **Temporary Internet Files.** This folder contains the offline cache for Internet Explorer.
- **My Documents.** This folder is the default target for the My Documents desktop icon. In Windows 2000, My Documents is the default location for storing user documents in most applications.
- **NetHood.** This hidden folder contains the shortcuts that appear in My Network Places.
- **PrintHood.** This seldom-used hidden folder can contain shortcuts to items in the Printers folder.
- **Recent.** This hidden folder contains shortcuts to the recently used documents; the most recent of these appear on the Documents submenu of the Start menu.
- **SendTo.** This hidden folder contains shortcuts to the folders and applications that appear on the Send To submenu. Send To is a command that appears on the File menu in Windows Explorer when you select a file or folder; it also appears on the shortcut menu when you right-click a file or folder.
- **Start Menu.** This folder contains the items (such as shortcuts to applications and documents) that appear at the top of the Start menu and in the Programs submenu.
- **Templates.** This hidden folder contains shortcuts to document templates. These templates are typically used by the New command (on the File menu and the

shortcut menu) in Windows Explorer and are referenced by the FileName value in the HKCR*class*\ShellNew key.

Note Group Policy settings always take precedence over user settings in user profiles. This allows administrators to foil users who have the knowledge and permissions to make changes directly in their own user profile.

Types of Profiles

Windows 2000 supports three types of profiles:

- **Local user profiles.** A local user profile is stored in the %SystemDrive%\ Documents And Settings (or %SystemRoot%\Profiles) folder on the local hard drive. Windows creates a local user profile the first time a user logs on to the computer. If the user makes changes to the profile, the changes affect only the computer where the changes are made.
- **Roaming user profiles.** A roaming user profile is stored on a network server, which makes it available when a user logs on to any computer on the network. Windows creates a local copy of the user profile the first time a user logs on to a computer. If the user makes changes to the profile, Windows merges the changes into the server copy when the user logs off; therefore, the revised profile is available the next time the user logs on to any computer. Roaming profiles are easily managed by and are ideally suited to Windows 2000 Server. With some extra effort, however, you can achieve some of the benefits even without Windows 2000 Server; *for details, see "Using Roaming User Profiles," page 323.* (In some texts, you'll see the acronym RUP for roaming user profiles. Suffering from an overload of TLAs—three-letter abbreviations—we eschew that acronym in this book.)
- **Mandatory user profiles.** A mandatory user profile is one that can be changed only by an administrator. Like a roaming user profile, a mandatory profile is stored on a network server, and Windows creates a local copy when a user who has been assigned a mandatory profile logs on for the first time. Unlike a roaming user profile, a mandatory profile is not updated when the user logs off. This makes mandatory profiles useful not only for individual users whom you want to severely restrict, but also for multiple users (for example, all users in a certain job classification) to whom you want to apply consistent job-specific settings. Multiple users can share a mandatory user profile without affecting others. Users who have been assigned a mandatory profile can make profile changes while they're logged on (unless prevented by policy settings), but the network copy remains unchanged. Although a copy of the profile—changes and all—remains on the computer after a user logs off, at the next logon Windows recopies the original profile from the network share. *For information about assigning a mandatory user profile, see "Using Mandatory User Profiles," page 327.*

Common Profiles

In the profiles folder (%SystemDrive%\Documents And Settings or %SystemRoot%\Profiles), you'll find two profiles that aren't associated with a particular user account: All Users and Default User. (The Default User folder is hidden.)

The content of the All Users folder appears for all users who log on to a workstation in addition to the content of each user's own profile folder. For example, items in the All Users\Desktop folder appear on the desktop along with items that the current user has saved on the desktop. Similarly, the Start menu shows the combined contents of the All Users\Start Menu folder and the current user's Start Menu folder. (In Windows NT, the Start menu items were segregated. Items from the All Users profile were often identified on the menu as "common.") By default, only members of the Administrators group and the Power Users group can add items to the All Users profile.

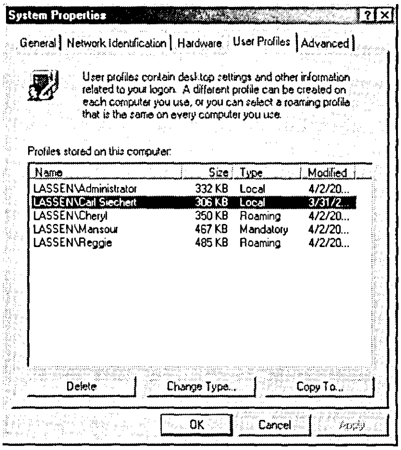
Note Windows offers a simple way to get directly to either branch of the Start menu hierarchy. Right-click the Start button and choose Open or Explore if you want to look at the Start Menu folder within the current user's profile; choose Open All Users or Explore All Users to view the All Users\Start Menu folder in Windows Explorer.

When a user logs on to a computer for the first time (and his or her account is not set up to use a roaming profile or mandatory profile), Windows creates a new local profile by copying the content of the Default User folder to a new folder and giving it the user's name. Therefore, you can configure the Default User profile the way you want new users' initial view of Windows to appear. With the default security settings, only members of the Administrators group can make changes to the Default Users profile.

Working with User Profiles

Armed with the knowledge of where profiles reside and what they contain, you might be tempted to manipulate them directly from Windows Explorer or a command prompt. Although you can safely add, modify, or remove items such as the Start menu and desktop items, you should not move, copy, or delete entire profiles in this manner. Instead, you should use the User Profiles tab in the System Properties dialog box, shown in Figure 19-2. To get there, right-click My Computer and choose Properties | User Profiles. Alternatively, choose Start | Settings | Control Panel | System | User Profiles.

From this dialog box, you can recover disk space by removing profiles you no longer use; simply select a profile and click Delete. Deleting profiles in this manner (instead of using Windows Explorer, for example) ensures that the appropriate profile also gets removed from the registry. (Each user profile occupies a subkey of HKLM \Software\Microsoft\Windows NT\CurrentVersion\ProfileList.)



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

Profiles stored on this computer:

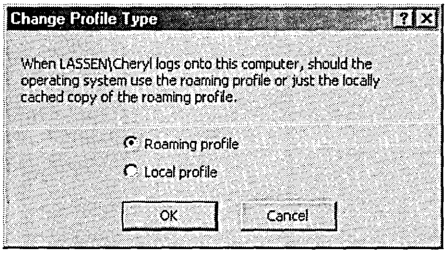
Name	Size	Type	Modified
LASSEN\Administrator	332 KB	Local	4/2/20...
LASSEN\Carl Siechert	306 KB	Local	3/31/2...
LASSEN\Cheryl	350 KB	Roaming	4/2/20...
LASSEN\Mansour	467 KB	Mandatory	4/2/20...
LASSEN\Reggie	485 KB	Roaming	4/2/20...

Figure 19-2
Use System Properties to copy or delete a user profile.

Note If you use roaming user profiles, Windows ordinarily saves the copy of the profile that has been copied to the local hard drive. Windows uses this local copy if the network copy happens to be unavailable the next time the user logs on. If you have a computer that's available to many users, this occasional convenience can cost a lot of disk space. You can force Windows to automatically delete the local copy of a roaming profile when a user logs off. To do that, open Group Policy (Gpedit.msc), go to Computer Configuration\Administrative Templates\System\Logon, and enable the policy named Delete Cached Copies Of Roaming Profiles. Other policies in the same folder also affect how roaming profiles are applied. *For more information, see Chapter 18, "Using Group Policy."*

Copying a user profile (by selecting a profile and clicking Copy To) doesn't add the profile to the registry; that happens the first time a user who has been assigned the profile you copy logs on. But copying from the System Properties dialog box instead of using Windows Explorer has an important advantage: Windows assigns the proper permissions to the copy. That is, it gives Full Control permission to the user or group you specify and removes permissions for other nonadministrative users. Such permissions are necessary to allow a user access to his or her own profile—but no one else's.

The other button on the User Profiles tab of the System Properties dialog box—Change Type—lets you decide whether a user who has been assigned a roaming user profile should use the roaming profile or the locally cached copy when he or she logs on. Making the change in the dialog box that appears in Figure 19-3 doesn't alter the roaming user profile on the network drive or the user account's link to it. Instead, it merely sets the UserPreference value in the selected profile's subkey of HKLM \Software\Microsoft\Windows NT\CurrentVersion\ProfileList.



When LASSEN\Cheryl logs onto this computer, should the operating system use the roaming profile or just the locally cached copy of the roaming profile.

● Roaming profile

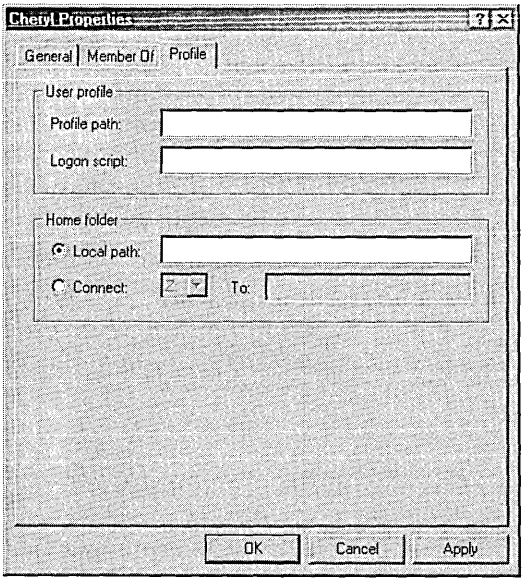
○ Local profile

Figure 19-3
The Change Profile Type options are available only for user accounts that have been assigned a roaming user profile.

Note Users who are not members of the Administrators group can't see other user profiles in the System Properties dialog box, nor can they delete, copy, or change their own profile.

Assigning a Profile

If you want to assign a profile to a user account, you use Microsoft Management Console with the Local Users And Groups snap-in. You can find it under System Tools in Computer Management, or you can launch it in its own window by typing *lusrmgr.msc* at a command prompt. In the Users folder, double-click the name of the user you want to assign the profile to and click the Profile tab. See Figure 19-4.



● Local path:

○ Connect: Z To:

Figure 19-4
Use the Profile tab to specify a user profile, a logon script, and a home folder.

On the Profile tab, you can specify the following:

- **The location of the user profile.** (Note that you need to do this only if you want to use a profile that's not stored in the default location, such as a roaming user profile or a mandatory user profile.) *For more information, see "Using Roaming User Profiles," page 323.*
- **The location and file name of a logon script—a program that runs each time the user logs on.** *For more information, see "Using Scripts That Run at Logon, Logoff, Startup, and Shutdown," page 320.*
- **The path to the user's home folder.** The *home folder* is a folder in which a user can store his or her files and programs. In some programs, the home folder is the default folder for the Open and Save As dialog boxes; others use the My Documents folder. The home folder is also the initial current folder for Command Prompt sessions. The home folder can be a local folder or on a shared network drive, and multiple users can share a common home folder. To specify a local home folder, enter a path specification in the Local Path text box. To use a folder on a network server as a home folder, select a drive letter (Windows maps the folder to this letter at each logon) and specify the full network path to the folder. (If you don't specify a home folder, Windows uses %SystemDrive%\ as the home folder.)

Troubleshooting

If you get a profile-related error when you try to log on or if you notice such an error in the Application event log, it could be caused by one or more of the following conditions:

- Your account doesn't have sufficient access permissions. Your account must have (at least) Read access to the profile folder, whether it's a local profile or a roaming or mandatory profile stored on another computer.
- Your account doesn't have sufficient access permissions to the profiles folder—the folder that contains the individual profiles. The Everyone account should have Full Control access to the folder. In addition, if it's a shared folder on a network drive, the Everyone account should have Full Control access to the share.
- Your system is low on hard drive space.
- The profile has been corrupted. In most cases, the only solution is to delete the profile.
- Your registry size limit has been reached. To increase the limit, right-click My Computer, choose Properties | Advanced | Performance Options | Change, and specify a new value in the Maximum Registry Size box.

Using Scripts That Run at Logon, Logoff, Startup, and Shutdown

A *logon script* is a program that runs whenever a user logs on. Any executable file—that is, a batch program (.bat or .cmd extension), a Windows Script Host (WSH) script (.vbs, .js, or .wsf extension), or a program (.exe or .com extension)—can be used as a logon script. *(For information about batch programs and WSH scripts, see Chapter 37, "Using Batch Programs," and Chapter 38, "Using Windows Script Host.")*

Logon scripts are commonly used to map network drives to a drive letter, to start certain programs, and to perform other similar tasks that should happen at each logon. As with most tasks in Windows, you can use other methods to perform each of these—but a logon script offers a convenient, flexible method. Here is a simple example, which is saved as a batch program:

```
@echo off
rem Logon script
echo Welcome %username%
rem Map drives
rem Public documents
net use g: \\glacier\document
rem Personal documents
net use h: \\glacier\users\%username%
rem Shared programs
net use p: \\glacier\programs
rem Start a program
start /min notepad.exe timelog.txt
```

Note The use of system environment variables—such as %UserName% in the sample logon script shown here—makes it easy to use the same script for different users. Windows substitutes the correct user name when it runs the script.

To use a logon script for a local user account:

1. Store the script in the %SystemRoot%\System32\Repl\Import\Scripts folder.
2. On the Profile tab of the user's properties dialog box (shown earlier in Figure 19-4), specify the name of the script in the Logon Script box. (If you store the script in the default scripts folder as described in step 1, you don't need to specify the complete path; the file name alone is sufficient.)

Using Group Policy Scripts

In addition to the so-called "legacy" logon scripts, which were a feature of every version of Windows NT, Windows 2000 offers support for four other types of scripts:

- Group Policy logon scripts, which run whenever a user logs on
- Group Policy logoff scripts, which run whenever a user logs off
- Group Policy startup scripts, which run whenever the computer starts up
- Group Policy shutdown scripts, which run whenever the computer shuts down

You can use the same types of files for any of these scripts as you can for legacy logon scripts. Though you're free to store scripts anywhere you like, each type of script has a default location: %SystemRoot%\GroupPolicy\User\Scripts\Logon, %SystemRoot%\GroupPolicy\User\Scripts\Logoff,%SystemRoot%\GroupPolicy \Machine\Scripts\Startup, and %SystemRoot%\GroupPolicy\Machine\Scripts \Shutdown.

To implement any of these scripts, start Group Policy (Gpedit.msc) and go to Computer Configuration\Windows Settings\Scripts (for startup and shutdown scripts) or User Configuration\Windows Settings\Scripts (for logon and logoff scripts). See Figure 19-5.

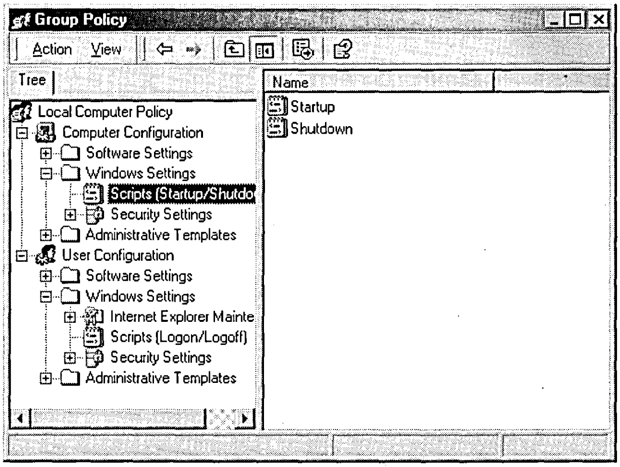
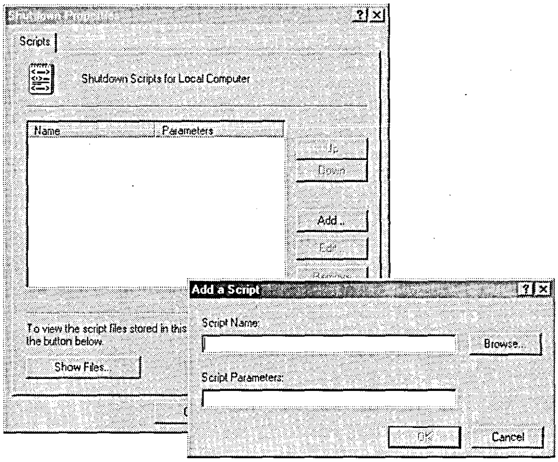


Figure 19-5
With Group Policy, you can specify scripts to run at startup, logon, logoff, and shutdown.

When you double-click an entry in one of these folders (as shown in Figure 19-6), you'll notice some additional improvements over legacy logon scripts:

- You can specify more than one script for each of these events, and you can specify the order in which they run.
- You can specify command-line parameters for each script.



To view the script files stored in this
the button below.

Figure 19-6
Click Add to add a script and its command-line parameters to the list.

Making Other Group Policy Settings

In Group Policy, you specify which scripts you want to run for various events. Group Policy also offers a number of policy settings that affect how scripts run—synchronously or asynchronously, hidden or visible. (In this case, *synchronously* means that, in effect, nothing else runs until the script finishes running.)You'll find these settings, along with more complete explanations of their effects, in Computer Configuration \Administrative Templates\System\Logon and in User Configuration \Administrative Templates\System\Logon/Logoff. Some policies appear in both places; if the settings are configured differently, the one in Computer Configuration takes precedence.

Using IntelliMirror Features Without Windows 2000 Server

Even on a network that does not use Windows 2000 Server and Active Directory, you can use some IntelliMirror-like features. For example, you can have your settings appear when you log on at different workstations. Some key aspects differentiate how these features work in a Windows 2000 workgroup environment as opposed to a Windows 2000 Server–based domain:

- In a domain environment, user accounts and computer accounts are centrally managed at the domain level, so you need to make settings only one time and in only one place. Accessing a profile for the first time from a new computer happens automatically. By contrast, with a Windows 2000 workgroup, you must explicitly create similar user accounts on each computer where you want to log on before you're allowed to log on.

- In a domain environment, Group Policy enables an administrator to apply policy settings and restrictions to users and computers (and groups of each) in one fell swoop. With a workgroup, you must make similar Group Policy settings on each computer where you want such restrictions imposed. In addition, domain-based Group Policy provides a convenient tool for setting up folder redirection from a central location.

The bottom line is that central administration adds significant convenience, automation, and control. But if you have a small number of users and computers to manage, the time and patience to make settings on each computer throughout your network, and you don't have Windows 2000 Server, the procedures in the following sections can give you a taste of the benefits that IntelliMirror provides.

Caution Our own experimentation showed that configuring roaming profiles and mandatory profiles in a Windows 2000 Professional–only workgroup environment is difficult, at best. Interactions with local Group Policy, the ability to update profiles, and the ability to adequately secure profile information make operation somewhat unpredictable if you don't configure everything correctly. Bear in mind that these features are properly part of Windows 2000 Server, and the workarounds described here might be impractical to implement. If such features are important to you and your business, you should seriously consider upgrading to Windows 2000 Server, which makes user configuration much easier.

Using Roaming User Profiles

A roaming user profile allows a user to log on to a workstation and see his or her familiar settings on the desktop, the Start menu, and so on. Roaming user profiles, which are the key enabling technology behind User Settings Management, work by storing the user profile in a shared network folder. When the user logs on, the profile information is copied from the shared network folder to the local hard drive. When the user logs off, the profile information—which might have changed during the computing session—is then copied back to the shared folder.

To make this work in a workgroup environment, each user whom you want to set up with a roaming profile must have an account on each computer where that user will log on, plus an account on the computer that contains the shared profiles folder. The user account on each computer must have the same user name and password.

Setting Up the Shared Folder for Roaming Profiles

To set up the shared folder:

1. Log on to a computer on your network as a member of the computer's Administrators group.
2. Using Windows Explorer, create a folder called Profiles.
3. In Windows Explorer, right-click the folder and choose Sharing.
4. On the Sharing tab of the properties dialog box that appears, select Share This Folder. The default sharing permissions, which provide Full Control share access to Everyone, are appropriate.
5. Click the Security tab (if you created the folder on an NTFS volume), and be sure that Everyone has Full Control permission.

Setting Up User Accounts

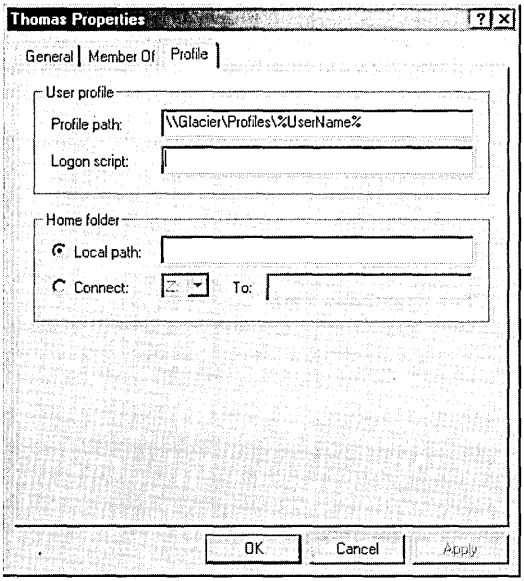
To set up the user accounts:

1. On each computer (including the "server" that you set up in the preceding procedure), log on as a member of the Administrators group.
2. Right-click My Computer and choose Manage.

Note As an alternative to logging in at each computer, you can connect to each one using Computer Management—as long as the account you're logged on with uses the same name and password as an administrative account on the target computer. To connect to a different computer, in Computer Management right-click Computer Management (Local) and choose Connect To Another Computer. Then proceed with the following steps.

3. In Computer Management, go to System Tools\Local Users And Groups\Users.
4. If the user account you want doesn't already exist, choose Action | New User and create a user account. Be sure to use the same user name and password on each computer. Clear the User Must Change Password At Next Logon check box before you click Create.
5. On the right side of the Computer Management window, double-click the name of the user to display the properties dialog box.
6. Click the Profile tab. In the Profile Path box, type the network path to the shared profiles folder, as shown in Figure 19-7. The %UserName% environment variable gets expanded to the user name so that, in this case, the profile gets stored in the shared Profiles\Thomas folder on the computer named Glacier. The

advantage of using the environment variable is merely convenience: you can use the same string for every user, without having to pause to figure out the correct name of the profile folder.



Profile path: \\Glacier\Profiles\%UserName%

Logon script:

● Local path:

○ Connect: Z: To:

Figure 19-7
Setting Profile Path to a shared network folder lets you use roaming user profiles.

Note If you forget to set up a user account on the computer with the shared profiles folder, Windows displays a warning when the user attempts to log on. If a local copy of the user profile already exists, Windows uses that copy; if not, Windows creates a temporary profile (based on the Default User profile) in a folder called Temp, which is not saved when the user logs off.

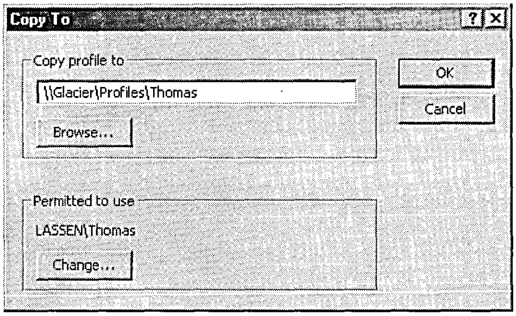
Creating the Profile

To create a profile to be used as a roaming user profile and copy it to the shared profiles folder:

1. Create a profile by logging on (ideally with a temporary user account you create for the purpose) and making the settings you want.
2. Log off and then log back on as a member of the Administrators group.

Note If you are copying a profile from a computer other than the one that contains the shared profiles folder, the account you log on with must have the same name and password as an account that has administrative privileges on the target computer.

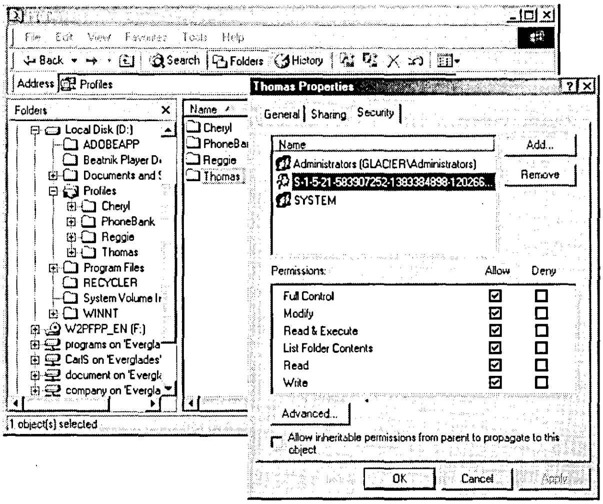
3. Right-click My Computer and choose Properties | User Profiles.
4. Select the profile you created and click Copy To.



5. In the Copy Profile To box, type the full path of the destination profile folder. For example, if you want to create a profile for a user named Thomas in the Profiles share on the computer named Glacier, type *\\glacier\profiles\thomas*. Be sure the destination folder you specify doesn't exist; if it does, Windows deletes its contents before copying the profile.
6. In the Permitted To Use box, click Change and then select the name of the user who will use the profile.

When you click OK in the Copy To dialog box, Windows copies the user profile to the specified folder and sets permissions on the destination folder and its contents. Windows gives Full Control permission to the Administrators group, the user or group you selected in the Permitted To Use box, and the System account. This prevents nonadministrative users from accessing a profile other than their own.

If you copied the profile from one computer to a shared folder on another computer, the permissions that Windows creates are not exactly right, and you must take one more step to correct them. On the computer with the shared profiles folder, right-click the new profile folder and choose Properties | Security. If one of the names shows the security identifier of an unknown user (as shown in Figure 19-8), you must add the correct user account (Thomas, in this case) and give it Full Control permission. You can remove the unknown user, although it's not necessary to do so. (The unknown account is actually the correct user name, but it's the account from the source computer, not the account on the local computer. This is one of the hazards and annoyances of relying on separate security databases—the workgroup model—rather than using the centralized security database used by Windows 2000 Server domains. *For more information, see "Local Accounts vs. Domain Accounts," page 283.*)



Name

Administrators (GLACIER\Administrators)

S-1-5-21-583907252-1383384898-120266...

SYSTEM

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

□ Allow inheritable permissions from parent to propagate to this object

Figure 19-8
If the permissions for the profile folder don't include the local user account, the user won't be able to log on.

Troubleshooting

You might encounter problems if certain user profile settings rely on files that are stored on the local hard drive. For example, you might set the desktop wallpaper to a file stored on drive C. When you log on at another computer, the wallpaper doesn't appear (unless the same file happens to be in the same location on the other computer). You can alleviate such problems by redirecting My Documents to a shared network folder and then using it to store documents and other files that you want to access from different computers.

Using Mandatory User Profiles

A mandatory user profile works much like a roaming user profile: when a user logs on, the profile is copied from a network location to a local folder, thereby providing familiar settings. The difference is that a mandatory profile isn't updated with user changes when the user logs off.

To assign a mandatory user profile to one or more users, follow the same procedures as described in the previous section for using roaming user profiles. Then, on the computer where the shared profile is stored, make the following changes:

1. Change the folder permissions to remove Full Control, Modify, and Write permissions for the user account (or accounts) that will use the profile—leaving them with only Read & Execute, List Folder Contents, and Read permissions.
2. Change the name of the hidden Ntuser.dat file (in the profile's top-level folder) to Ntuser.man.

Using Folder Redirection

In a Windows 2000 Server–based network, Group Policy settings allow an administrator to use folder redirection to store on a network server the data files from a user's profile. Storing such data on a network server apart from the user profile offers two important benefits:

- Storing user data in a central location can make backup easier.
- Separating user data from the user profile speeds up the logon and logoff process for users with roaming profiles. (If all a user's documents are stored within the profile, they are copied from the network server to the local computer at each logon, and then copied back at each logoff. By storing them apart from the profile, each file is fetched only as it's needed.)

The Folder Redirection extension in Group Policy for domain-based accounts lets administrators easily change the actual location of the Application Data, Desktop, My Documents, and Start Menu components of the user profiles—and users won't even notice the difference.

Windows 2000 Professional doesn't offer an easy way to apply such changes to all the computers on a network, or even to all the users on a computer. However, the effort of configuring each user account might be worthwhile, particularly if you use roaming user profiles (because doing so speeds up logon and logoff) or if you want to back up user documents from a single location. To redirect the My Documents folder:

1. Log on to the network computer where you want to store each user's My Documents folder as a member of the computer's Administrators group.
2. Using Windows Explorer, create a folder named Documents.
3. In Windows Explorer, right-click the folder and choose Sharing.
4. On the Sharing tab of the properties dialog box that appears, select Share This Folder. Click Caching and then select Automatic Caching For Documents.
5. At the computer that you want to configure for one or more users, log on using the account you want to change.
6. Right-click My Documents and choose Properties.
7. On the Target tab, type the network path of the folder where you want to keep My Documents. For example, if the Documents share is on a computer named Glacier, you can create a named subfolder for a user named Thomas by typing *\\glacier\documents\thomas*.
8. Click OK. Click Yes to create a new folder, and then click Yes if you want to move the existing documents to the new target location.
9. Right-click My Documents and choose Make Available Offline. While not strictly necessary, this step ensures that the documents are available even if the network location is unavailable for some reason.

10. In Windows Explorer, right-click the new folder on the server and choose Properties | Security. Add the current user and assign Full Control permission; delete the Everyone group.
11. Repeat steps 5 through 10 for each user account that you want to change.
12. Log on as a member of the Administrators group.
13. Open Group Policy and go to User Configuration\Administrative Templates\Desktop. Enable the Prohibit User From Changing My Documents Path policy.

Chapter 20

Managing Services

In This Chapter

Using the Services Snap-In 331

Managing Services from a Command Prompt 341

Adding and Removing Services 341

Services Included with Windows 2000 Professional 342

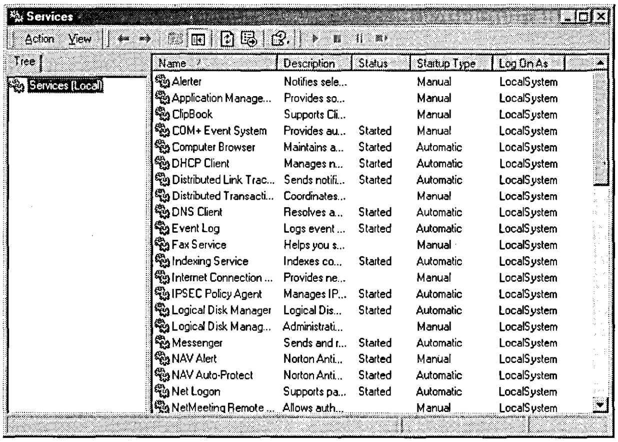
A *service* is a specialized program that performs a function to support other programs. Many services operate at a very low level (by interacting directly with hardware, for example); for this reason, they are often run by the System account (which has such privileges) rather than by ordinary user accounts (which do not). Microsoft Windows 2000 includes services as varied as the Event Log service, which keeps a database of event messages, and the Telnet service, which allows remote users to log on to your computer using a command-line interface.

Services have other advantages over ordinary programs. Services can start when the computer starts, which means that they can be running even when no user is logged on. And they don't stop when a user logs off; they remain running until the system is shut down.

In this chapter, we explain how to view the installed services; start, stop, and configure them; and install or remove them. Then we take a closer look at some of the services used in Windows 2000, showing how you can configure them to your advantage.

Using the Services Snap-In

You manage services with the Services snap-in for Microsoft Management Console (MMC), shown in Figure 20-1. To view this snap-in, choose Start | Settings | Control Panel | Administrative Tools | Services or simply run Services.msc. The Services snap-in is also a component in the Computer Management console (under Services And Applications) if you prefer the all-in-one approach.



Name	Description	Status	Startup Type	Log On As
Alerter	Notifies sele...		Manual	LocalSystem
Application Manage...	Provides so...		Manual	LocalSystem
ClipBook	Supports Cli...		Manual	LocalSystem
COM+ Event System	Provides au...	Started	Manual	LocalSystem
Computer Browser	Maintains a...	Started	Automatic	LocalSystem
DHCP Client	Manages n...	Started	Automatic	LocalSystem
Distributed Link Trac...	Sends notifi...	Started	Automatic	LocalSystem
Distributed Transacti...	Coordinates...		Manual	LocalSystem
DNS Client	Resolves a...	Started	Automatic	LocalSystem
Event Log	Logs event ...	Started	Automatic	LocalSystem
Fax Service	Helps you s...		Manual	LocalSystem
Indexing Service	Indexes co...	Started	Automatic	LocalSystem
Internet Connection ...	Provides ne...		Manual	LocalSystem
IPSEC Policy Agent	Manages IP...	Started	Automatic	LocalSystem
Logical Disk Manager	Logical Dis...	Started	Automatic	LocalSystem
Logical Disk Manag...	Administrati...		Manual	LocalSystem
Messenger	Sends and r...	Started	Automatic	LocalSystem
NAV Alert	Norton Anti...	Started	Manual	LocalSystem
NAV Auto-Protect	Norton Anti...	Started	Automatic	LocalSystem
Net Logon	Supports pa...	Started	Automatic	LocalSystem
NetMeeting Remote ...	Allows auth...		Manual	LocalSystem

Figure 20-1
Use the Services console to start, stop, and configure services.

The Services console offers plenty of information in its clean display. You can sort the display on the contents of any column by clicking the column title, as you can do with other similar lists. To sort in reverse order, click the column title again. In addition, you can:

- Start, stop, pause, resume, or restart the selected service, as described in the following section
- Display the properties dialog box for the selected service, in which you can configure the service and learn more about it

Starting and Stopping Services

Most of the essential services are set to start automatically when your computer starts, and the operating system stops them as part of its shutdown process. But sometimes you might need to manually start or stop a service. For example, you might want to start a seldom-used service on the rare occasion when you need it. (Because running services requires system resources such as memory, running them only when necessary can improve performance.)

You might want to stop a service because you're no longer using it—but a more common reason for stopping a service is because it isn't working properly. For example, if print jobs get stuck in the print queue, sometimes the best remedy is to stop and then restart the Print Spooler service. (If the service is one that allows pausing, try to pause and then continue the service as your first step instead of stopping. Pausing can solve certain problems without canceling jobs in process or connections.) Another reason to stop a service—particularly a network service—is to enhance security. You might want to stop the Server service while you're connected to the Internet, for example; doing so prevents malicious users from using remote administration tools to access your computer. (We mention this only as an example, not as a recommendation. With other security measures in place, stopping the Server service shouldn't be necessary.)

To change a service's status, select it in the Services console. Then click one of the following toolbar buttons, or right-click and choose the corresponding command:

▶ **Start, Resume.** Starts a service that isn't running, or resumes a service that has been paused.

■ **Stop.** Stops a running service.

❚❚ **Pause.** Pauses a running service. Pausing a service doesn't remove it from memory; it continues to run at a level that varies depending on the service. With some services, pausing allows users to complete jobs or disconnect from resources but does not allow them to create new jobs or connections, for example.

■▶ **Restart.** Stops a running service and then restarts it.

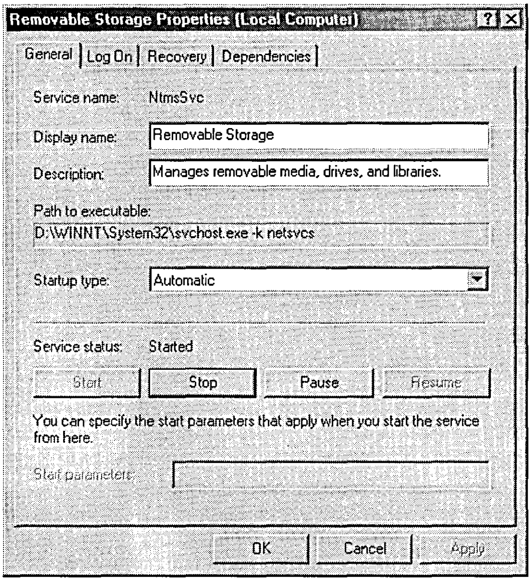
You can also change a service's status by opening its properties dialog box and then clicking one of the buttons on the General tab. Taking the extra step of opening the properties dialog box has only one advantage: you can specify start parameters when you start a service using this method. This is a rare requirement.

Note that not all services permit you to change their status. Some prevent stopping and starting altogether, whereas others permit stopping and starting but not pausing and resuming. Some services allow these permissions to only certain users or groups. Which status changes are allowed and who has permission to make them are controlled by each service's discretionary access control list (DACL), which is established when the service is created on a computer. The Windows user interface doesn't provide any means for viewing or changing the DACL, although it can be changed programmatically.

Most services allow only members of the Power Users and Administrators groups to start or stop them.

Configuring Services

To review or modify the way a service starts up or what happens when it doesn't start properly, view its properties dialog box. To do that, simply double-click the service in the Services console. Figure 20-2 shows an example.



Service name: NtmsSvc

Display name: Removable Storage

Description: Manages removable media, drives, and libraries.

Path to executable:
D:\WINNT\System32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 20-2
You specify the startup type on the General tab, where you can also find the actual name of the service above its display name.

Setting Startup Options

On the General tab of the properties dialog box (see Figure 20-2), you specify the startup type:

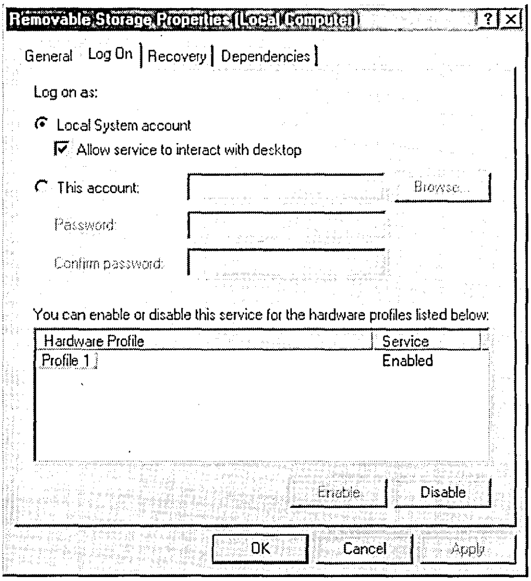
- **Automatic.** The service starts when the computer starts.
- **Manual.** The service doesn't start automatically at startup, but it can be started by a user, a program, or a dependent service.
- **Disabled.** The service can't be started.

You'll find other startup options on the Log On tab of the properties dialog box, as shown in Figure 20-3.

Note If you specify a logon account other than the local System account, be sure that account has the requisite rights. Go to Start | Settings | Control Panel | Administrative Tools | Local Security Policy. In the Local Security Settings console, go to Security Settings\Local Policies\User Rights Assignment and assign the Log On As A Service right to the account.

Specifying Recovery Actions

For a variety of reasons—hardware not operating properly or network connection down, to name a few—a happily running service might suddenly stop. Settings on the Recovery tab of the properties dialog box, shown in Figure 20-4, allow you to specify what should happen if a service fails.



Log on as:

● Local System account

☑ Allow service to interact with desktop

○ This account:

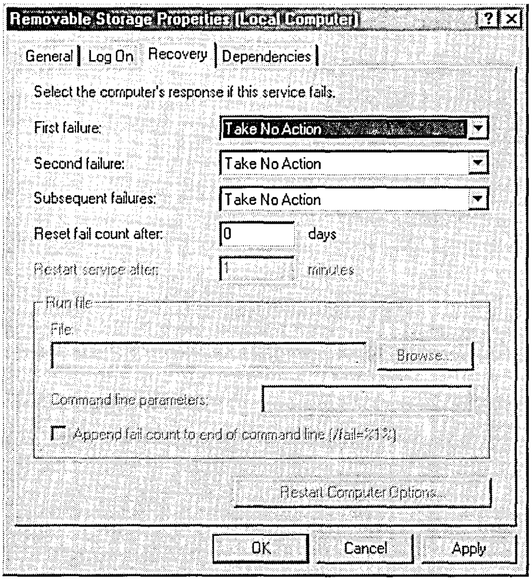
Password:

Confirm password:

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

Figure 20-3
On the Log On tab, you specify which user runs the service, and you can also specify which hardware profiles use the service.


Removable Storage Properties (Local Computer)
General
Log On
Recovery
Dependencies
Browse...
Restart Computer Options...
OK
Cancel
Apply

Select the computer's response if this service fails.

First failure: Take No Action

Second failure: Take No Action

Subsequent failures: Take No Action

Reset fail count after: 0 days

Restart service after: 1 minutes

Run file

File:

Command line parameters:

□ Append fail count to end of command line (/fail=%1%)

Figure 20-4
Use the Recovery tab to specify what should happen if the service fails.

For the first failure, second failure, and subsequent failures, you can choose one of these options:

- **Take No Action.** The service gives up trying. In most cases, the service places a message in the event log. (Use of the event log depends on how the service was programmed by its developers.)
- **Restart The Service.** The computer waits for the time specified in the Restart Service After box to elapse and then tries to start the service.
- **Run A File.** The computer runs the program that you specify in the Run File box. This could be a program that attempts to resolve the problem or one that alerts you to the situation, for example.
- **Reboot The Computer.** Drastic but effective, this option restarts the computer after the time specified in the Restart Computer Options dialog box elapses. In that dialog box, you can also specify a message to be broadcast (using the Messenger service) to other users on your network, warning them of the impending shutdown.

Troubleshooting

If you set up a service to log on using an account other than the local System account and the service fails, you won't get the Dr. Watson log or dump file that the failed service would otherwise generate. This occurs because Dr. Watson attempts to access the desktop of the service's logon account and it's unable to do so. To work around this problem, reconfigure the service to use the local System account and select the Allow Service To Interact With Desktop. (Of course, this workaround doesn't help if the only way to *run* the service is by allowing it to log on with a different account.)

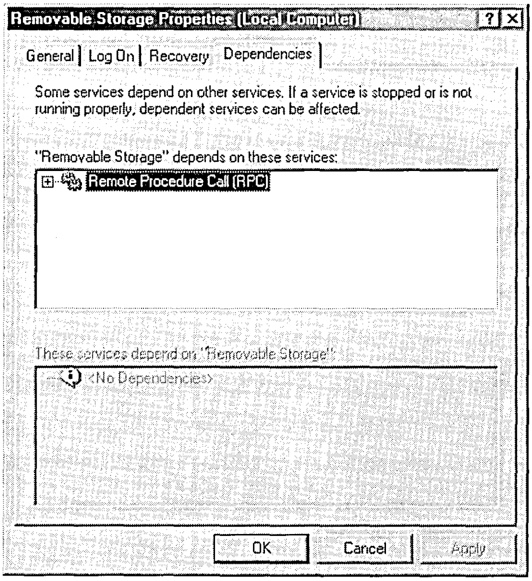
Viewing Dependencies

Many services rely on the functions of another service. If you attempt to start a service that depends on other services, Windows first starts the others. If you stop a service upon which others are dependent, Windows also stops those services. Before you either start or stop a service, therefore, it's helpful to know what other services your action might affect. To obtain that information, visit the Dependencies tab of a service's properties dialog box, shown in Figure 20-5.

Determining a Service's Name

As you view the properties dialog box for different services, you might notice that the service name (shown at the top of the General tab) is often different from the name that appears in the Services console (the display name) and that neither name matches the name of the service's executable file. (In fact, the executable for many services is Services.exe; this process runs the Service Control Manager itself along with several services, including Alerter, Computer Browser, Event Log, and Windows Time.) The General tab shows all three names.

So what? When you work in the Services console, you don't need to know anything other than a service's display name to find it and work with it. But if you use the Net command to start and stop services (as explained in the following section), you might find using the service name more convenient; it is often much shorter than the display name. You'll also need the service name if you're ever forced to work with a service's registry entries, which can be found in the HKLM\System\CurrentControlSet\Services *service* subkey (where *service* is the service name).



Removable Storage Properties (Local Computer)

Some services depend on other services. If a service is stopped or is not running properly, dependent services can be affected.

"Removable Storage" depends on these services:

Remote Procedure Call (RPC)

These services depend on "Removable Storage":

<No Dependencies>

Figure 20-5
The Dependencies tab shows which services depend on other services.

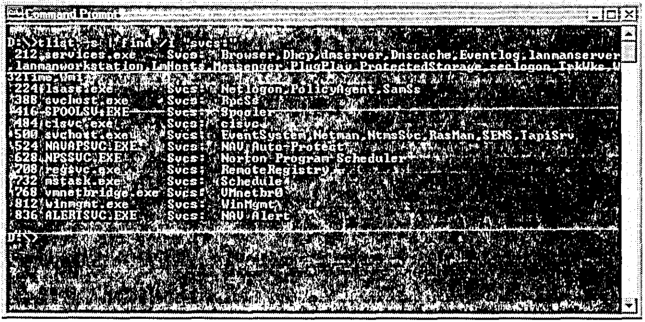
And what about the executable name? You might need it if certain users have problems running a service; in such a case, you need to find the executable and check its permissions. Knowing the executable name can also be useful, for example, if you're using Task Manager to determine why your computer seems to be running so slowly. The Processes tab shows only executable names, many of which are, well, inscrutable.

Troubleshooting

The support tools included with Windows 2000 Professional provide a nifty command-line utility called Tlist.exe that shows exactly which services are associated with each process (executable) name. (Tlist, short for Task List Viewer, can also display a lot of other information about running processes, or tasks.) Armed with this knowledge, you can return to Task Manager to determine whether it's a service that's causing your woes and, if so, which one.

To install Tlist.exe (and the other support tools), navigate to *d*:\Support\Tools (where *d* is your CD-ROM drive) and run Setup. After you've installed Tlist, you can display a list of services that are active in each currently running process by typing *tlist -s* at a command prompt. This shows *all* processes, including many that aren't related to services; the processes that include one or more services show "Svcs:" in the third column. The other columns show the process identifier (PID), the process name, and the window title (if any). Tlist shows the names (not the display names) of all active services in each process.

If your primary interest is services, combine the Tlist command with the Find filter to include only the service-related processes. At a command prompt, type *tlist -s | find /i "svcs:"* to filter the list, as shown in Figure 20-6. This illustration shows, for example, that the second Svchost.exe process is running the EventSystem, Netman, NtmsSvc, RasMan, SENS, and TapiSrv services. If Task Manager shows that process taking an inordinate amount of processor time, you can use this list to hone in on the possible suspects.



```
D:\>tlist -s | find /i "svcs:"
 212 services.exe      Svcs:  Browser,Dhcp,dmserver,Dnscache,Eventlog,lanmanserver
,lanmanworkstation,LmHosts,Messenger,PlugPlay,ProtectedStorage,seclogon,TrkWks,W
32Time,Wmi
 224 lsass.exe         Svcs:  Netlogon,PolicyAgent,SamSs
 388 svchost.exe       Svcs:  RpcSs
 416 SPOOLSV.EXE       Svcs:  Spooler
 484 cisvc.exe         Svcs:  cisvc
 500 svchost.exe       Svcs:  EventSystem,Netman,NtmsSvc,RasMan,SENS,TapiSrv
 524 NAVAPSVC.EXE      Svcs:  NAV Auto-Protect
 628 NPSSVC.EXE        Svcs:  Norton Program Scheduler
 708 regsvc.exe        Svcs:  RemoteRegistry
 732 mstask.exe        Svcs:  Schedule
 768 vmnetbridge.exe   Svcs:  VMnetbr0
 812 winmgmt.exe       Svcs:  WinMgmt
 836 ALERTSVC.EXE      Svcs:  NAV Alert

D:\>
```

Figure 20-6
When used with the –S switch and filtered with the Find command, Task List Viewer shows all active services along with their executable names.

As mentioned earlier, you can find the actual name of each service and its executable name by looking at the General tab of the service's properties dialog box. For your reference, Table 20-1 shows the names for all the services that are commonly installed with Windows 2000 Professional. Your system might have other services installed—from Microsoft or from another publisher—or it might not have all of these installed.

Table 20-1. Names of Services

Display Name	Service Name	Executable
Alerter	Alerter	Services.exe
Application Management	AppMgmt	Services.exe
ClipBook	ClipSrv	Clipsrv.exe
COM+ Event System	EventSystem	Svchost.exe
Computer Browser	Browser	Services.exe
DHCP Client	Dhcp	Services.exe
Distributed Link Tracking Client	TrkWks	Services.exe
Distributed Transaction Coordinator	MSDTC	Msdtc.exe
DNS Client	Dnscache	Services.exe
Event Log	Eventlog	Services.exe
Fax Service	Fax	Faxsvc.exe
FTP Publishing Service	MSFTPSVC	Inetinfo.exe
IIS Admin Service	IISADMIN	Inetinfo.exe
Indexing Service	cisvc	Cisvc.exe
Internet Connection Sharing	SharedAccess	Svchost.exe
IPSEC Policy Agent	PolicyAgent	Lsass.exe
Logical Disk Manager	dmserver	Services.exe
Logical Disk Manager Administrative Service	dmadmin	Dmadmin.exe
Messenger	Messenger	Services.exe
Net Logon	Netlogon	Lsass.exe
NetMeeting Remote Desktop Sharing	mnmsrvc	Mnmsrvc.exe
Network Connections	Netman	Svchost.exe
Network DDE	NetDDE	Netdde.exe
Network DDE DSDM	NetDDEdsdm	Netdde.exe
NT LM Security Support Provider	NtLmSsp	Lsass.exe
Performance Logs and Alerts	SysmonLog	Smlogsvc.exe
Plug and Play	PlugPlay	Services.exe
Print Spooler	Spooler	Spoolsv.exe
Protected Storage	ProtectedStorage	Services.exe
QoS RSVP	RSVP	Rsvp.exe

(continued)

Table 20-1. Names of Services *(continued)*

Display Name	Service Name	Executable
Remote Access Auto Connection Manager	RasAuto	Svchost.exe
Remote Access Connection Manager	RasMan	Svchost.exe
Remote Procedure Call (RPC)	RpcSs	Svchost.exe
Remote Procedure Call (RPC) Locator	RpcLocator	Locator.exe
Remote Registry Service	RemoteRegistry	Regsvc.exe
Removable Storage	NtmsSvc	Svchost.exe
Routing and Remote Access	RemoteAccess	Svchost.exe
RunAs Service	seclogon	Services.exe
Security Accounts Manager	SamSs	Lsass.exe
Server	lanmanserver	Services.exe
Simple Mail Transport Protocol (SMTP)	SMTPSVC	Inetinfo.exe
Smart Card	ScardSvr	Scardsvr.exe
Smart Card Helper	ScardDrv	Scardsvr.exe
System Event Notification	SENS	Svchost.exe
Task Scheduler	Schedule	Mstask.exe
TCP/IP NetBIOS Helper Service	LmHosts	Services.exe
TCP/IP Print Server	LPDSVC	Tcpsvcs.exe
Telephony	TapiSrv	Svchost.exe
Telnet	TlntSvr	Tlntsvr.exe
Uninterruptible Power Supply	UPS	Ups.exe
Utility Manager	UtilMan	Utilman.exe
Windows Installer	MSIServer	Msiexec.exe
Windows Management Instrumentation	WinMgmt	Winmgmt.exe
Windows Management Instrumentation Driver Extensions	Wmi	Services.exe
Windows Time	W32Time	Services.exe
Workstation	lanmanworkstation	Services.exe
World Wide Web Publishing Service	W3SVC	Inetinfo.exe

Note Like file names, the names of services are not case sensitive. In Table 20-1, we capitalize the service names exactly as they appear in the registry. Although the Windows programmers are obviously not very consistent in applying a capitalization style, you're likely to see this same capitalization whenever a particular service name is mentioned in documentation.

Managing Services from a Command Prompt

If you want to control services via a batch program—or if you simply prefer working at a command prompt—you can use variants of the Net command. Don't be dissuaded by the name; the Net command manages all services, not only network services. Table 20-2 shows the Net commands to use for managing services.

Table 20-2. Net Commands for Managing Services

Command	Description
Net Start	Displays a list of running services.
Net Help Services	Displays a list of services that you can use with the Net Start *service* command. Unfortunately, the list is incomplete and the syntax it shows is incorrect. (Service names that include one or more spaces must be enclosed in quotation marks.)
Net Start *service*	Starts the *service* service. For *service*, you can use either the service name or its display name. (For example, *net start schedule* and *net start "task scheduler"* are equivalent.) For a list of services installed by default with Windows 2000 Professional, see Table 20-1. Surround multiword service names with quotation marks, as shown in the preceding example.
Net Stop *service*	Stops the *service* service. The service must be started before you can stop it.
Net Pause *service*	Pauses the *service* service. The service must be started before you can pause it. Many services don't permit pausing.
Net Continue *service*	Resumes the *service* service. The service must be paused before you can resume it.

Adding and Removing Services

Installing a service involves creating a number of arcane registry keys and values. Fortunately, applications that provide services install them as part of their setup program, and you don't need to concern yourself with this problem. If you're developing your own services, your best bet is to use one of the tools in the *Microsoft Windows 2000 Professional Resource Kit*. Instsrv.exe is a service installer that runs at a command prompt. Service Installation Wizard (Srvinstw.exe) is a graphical tool to perform the same function.

Not every program can run as a service. However, another Resource Kit tool, Srvany.exe, provides a wrapper that lets you run (almost) any application as a service. This allows you to enjoy the advantages of services, such as their ability to run when no one is logged on, to persist through logoff/logon cycles, and to be run as another user.

Removing a service is much easier, and you don't need any special tools to do it. Before you remove a service, however, *be absolutely certain* that it's what you want to do. Be sure that you won't need the service again, and be sure that no other services are dependent on it. (Check the Dependencies tab of its properties dialog box.) If you accidentally delete the wrong service, you might have to reinstall Windows 2000 to get it working again.

To permanently remove a service, you must first stop it. Use the Services snap-in or the Net Stop command to stop the service if it's running. If you can't stop it, configure its startup type as disabled and then restart the computer. After the service has been successfully stopped, use a registry editor to navigate to HKLM\System \CurrentControlSet\Services. If you can't find the service's subkey within the Services key, search for its display name (the name that appears in the Name column in the Services console), which is a value within the service's subkey. When you've located the correct service, you can delete its entire subkey.

Services Included with Windows 2000 Professional

As you peruse the list of services in the Services console, you'll recognize many that relate to features described elsewhere in this book, such as Event Log, Indexing Service, Internet Connection Sharing, and so on. Although those sections of the book don't specifically describe the function of the service (because there's usually no reason to mess with the default settings), now you know where to look. In the remaining sections of this chapter, we explain the use of a few services that aren't described elsewhere—and that often go unmentioned in discussions of Windows 2000. Nonetheless, you might find them useful.

Windows Time Service

Windows 2000 includes a new service, Windows Time or W32Time, that synchronizes the time and date of computers on a network. This is more than a convenience: synchronized time is critical because the Kerberos version 5 protocol uses workstation time as part of the authentication process. Windows Time uses the Simple Network Time Protocol (SNTP) to synchronize a computer's time with a designated time server, known as the *inbound time partner*.

In a Microsoft Windows 2000 Server–based network, workstations and member servers use their authenticating domain controller as their inbound time partner. (This happens automatically, and you don't need to do anything to configure the workstations other than ensuring that the Windows Time service is running.) In an enterprise with multiple domains and multiple domain controllers in each domain, the domain controllers follow the domain hierarchy to find their inbound time partner. The domain controller at the root of the forest is typically configured by the network administrator to synchronize its time with an authoritative outside time source, such as the United States Naval Observatory (USNO).

All well and good, but how do computers in a workgroup environment synchronize their clocks? You can set up a computer to synchronize with an external time server—exactly as you would on the domain controller of a Windows 2000 Server–based network. You can find lists of Network Time Protocol (NTP) servers (along with a lot of other information about NTP) at *www.eecis.udel.edu/~ntp*. The USNO maintains a number of time servers around the country, including *ntp2.usno.navy.mil* and *tick.usno.navy.mil*. To set a computer to use the USNO servers, type the following at a command prompt:

```
net time /setsntp:"ntp2.usno.navy.mil tick.usno.navy.mil"
```

Note As you can see in the example, you can include more than one SNTP server, which provides a backup if your first choice is unavailable. If you specify more than one server, you must separate the servers with a space and enclose the list in quotation marks. You can specify servers either by their DNS name, as we did in the example, or their IP address.

Assuming that the Windows Time service has been started (set its startup type to Automatic if it isn't already), your computer should periodically synchronize its clock with the NTP server.

Note SNTP uses port 123 to communicate with the time server. If you use an IPSec policy or a firewall for port blocking, be sure that port 123 is open.

Using the Windows Time service might not be convenient if you don't have a full-time connection to the Internet. In that case, you might prefer to run W32tm.exe, a program that can synchronize the computer's clock with the server specified by the Net Time /Setsntp command. It can do this "on demand"—simply type *w32tm-once* at a command prompt—or periodically, just like the Windows Time service. To have W32tm synchronize periodically, type *w32tm* without parameters; it continues running until you press Ctrl+C or log off. With either of these commands, W32tm.exe doesn't let you know what's going on; if you're interested, append a –V switch to the command to have W32tm provide a "verbose" listing of its actions.

After you have one computer synchronizing with a reliable external time source, you can then set the other computers on your network to synchronize to that computer, which becomes the inbound time partner for the rest of the computers. If the computer is not a domain controller running Windows 2000 Server, you'll need to use the Net Time /Setsntp command on each of the other computers to direct them to your internal time server. (Use its local IP address or DNS name.) Thereafter, the Windows Time service should keep all the computers in synch.

Note If you have trouble synchronizing computers using the Windows Time service or the W32tm command, you can still use the Net Time /Set command, which was the commonly used method of performing a one-time synchronization in earlier versions of Windows. To synchronize your computer's clock with the clock on the computer named Glacier, for example, type *net time /set \\glacier /y* at a command prompt. Better yet, put this command in your logon script or set it up as a scheduled task.

The process of setting the time on a computer is an iterative one at several levels. When the computer contacts its inbound time partner, the two computers exchange packets until they determine the transmission latency between them. Then the client computer adjusts its clock. The amount of adjustment depends on how far off the clock is initially. If it's less than two minutes fast, the time is adjusted over a 20-minute period until the clock is synchronized; otherwise, it's immediately set to the correct time. Thereafter, the client computer periodically contacts its inbound time partner to resynchronize. The period is adjusted from 45 minutes through 8 hours, depending on how far off the clock drifts between synchronizations. Windows Time attempts to minimize the number of synchronizations while still keeping the clock within two seconds of its inbound time partner.

This iterative process, along with an explanation of the hierarchy of inbound time partners in an enterprise environment, is explained in Microsoft Knowledge Base article Q224799.

Messenger and Alerter Services

The Messenger service and the Alerter service provide a means of sending messages from one computer to another on your network.

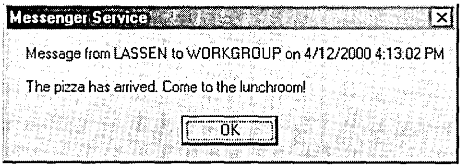
Using the Messenger Service

The Messenger service allows you to receive pop-up messages sent from other computers on your network using the Net Send command. It's a crude but effective communication system that you can use for instantly alerting others. The receiving system doesn't need to have its e-mail client running; in fact, it doesn't need an e-mail client at all. The only prerequisite on the receiving end is that the Messenger service is running.

To send a message, you use the Net Send *recipient message* command. Replace *recipient* with the user name of the person you want to reach or the name of the computer where you want the message displayed. If you want to send a message to all users currently connected to your computer's shared resources (perhaps to warn them that you're going to shut down the computer), replace *recipient* with */users*. And if you want to send a message to all users in your workgroup or domain, replace *recipient* with an asterisk (*). You should, of course, replace *message* with the text you want to send. For example, at a command prompt, you could type the following:

```
net send * The pizza has arrived. Come to the lunchroom!
```

A message like the one shown in Figure 20-7 appears on the screen of every computer where the Messenger service is running and someone is logged on. (If nobody is logged on, the Messenger service displays the message as soon as somebody logs on.)



Message from LASSEN to WORKGROUP on 4/12/2000 4:13:02 PM

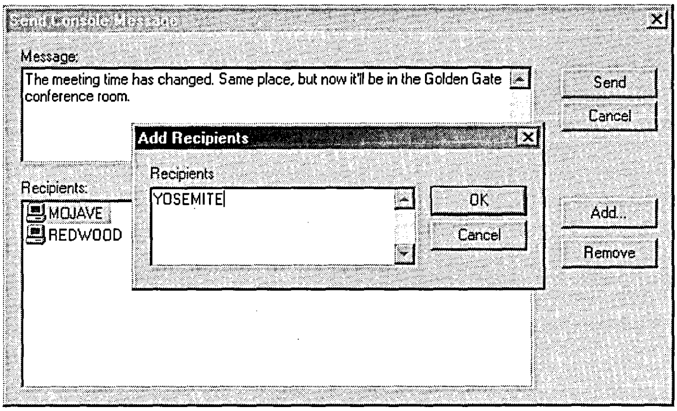
The pizza has arrived. Come to the lunchroom!

Figure 20-7
The Messenger service allows you to receive pop-up messages from other computers.

If you send a message to a computer on which the Messenger service is not running, Net Send reports its inability to send the message. In such a case, you'll see an error message whether you address your message to a computer, to a user, or to /Users. However, if you send a message to everyone in your workgroup or domain using an asterisk as the recipient, Net Send does not let you know who received the message and who did not.

Some programs other than Net Send rely on the Messenger service. For example, messages from a network printer that is configured to send notification of completed print jobs appear on your computer only if the Messenger service is running. *For information about printer notification, see "Setting Server Properties," page 232.*

Several MMC snap-ins, including Computer Management, Shared Folders, and Services, have a graphical interface for sending messages that allows you to send a message to multiple specific computers. To use it, right-click one of these folders in the console tree and choose All Tasks | Send Console Message. A dialog box like the one shown in Figure 20-8 appears. Because it doesn't have a browse capability and you can enter only one computer name at a time, it's cumbersome to use—but for the occasional urgent message, you might find it useful. When you click Send in the Send Console Message dialog box, it reports the success or failure for each recipient and lets you resend the message to others without retyping. The list of computers that you send to persists from one session to another, so you don't need to reenter them each time you use this dialog box.



Send Console Message

Message:

The meeting time has changed. Same place, but now it'll be in the Golden Gate conference room.

Recipients:

MOJAVE
REDWOOD

Add Recipients

Recipients

YOSEMITE

Figure 20-8
You can send a message to multiple recipients with this feature of the Services snap-in.

Using the Alerter Service

The Alerter service uses the same mechanism as the Messenger service, but it's used by Windows to send administrative alerts. Alert messages warn about security, access, printer, and other problems. To set up a computer so that it sends administrative alerts to another computer, follow these steps:

1. On the computer where the administrative alerts will originate (that is, a computer that you want to notify you when a problem arises), start Regedt32.exe, the registry editor.
2. In the HKLM\System\CurrentControlSet\Services\Alerter\Parameters key, create a REG_MULTI_SZ value named AlertNames if it doesn't already exist.
3. Set the AlertNames data to the name of the computer that you want to receive the administrative alerts. You can specify multiple names if you want; type each name on a new line.
4. Use the Services console to set the Alerter service for automatic startup and start the service.
5. On the computer where you want to receive the alerts, use the Services console to set the Messenger service for automatic startup and start the service.

Note

You don't actually need to physically go to each computer to complete this process. As long as you have administrative privileges on both computers, you can make all settings from either computer—or from a third computer. To open another computer's registry in Regedt32, choose Registry | Select Computer. The easiest way to open the Services snap-in for another computer is to use Computer Management; right-click Computer Management (Local) and choose Connect To Another Computer.

Chapter 21

Administering Remote Systems

In This Chapter

Requirements for Remote Administration 347
Using Computer Management 348
Using Other MMC Consoles and Snap-Ins 351
Managing Printers Remotely 354
Editing a Remote Registry 354
Setting Up Scheduled Tasks 354
Using Command-Line Utilities 355
Administering a Domain 356

Whether you have a two-node network with workstations spaced only a few feet apart, an enterprise-scale network that spans the globe, or something in between, you'll sometimes find it more convenient to manage another computer from your own desk. Although some of the most powerful remote administration features rely on Microsoft Windows 2000 Server, you can use Microsoft Windows 2000 Professional by itself to control many options without so much as ambling across the room.

In general, features that you can configure locally on a computer running Windows 2000 Professional can be configured across the network. The rest of this book explains how to use various snap-ins and other configuration tools to manage a computer locally. This chapter shows how to use the same tools to manage other computers on your network.

Requirements for Remote Administration

Lest you fear that this freedom to poke around on other computers without the user's knowledge puts your own system in jeopardy, worry not. For most of these tasks—and certainly for anything potentially invasive or destructive—you must have an account with sufficient privileges on the computer you're attempting to administer.

If your network is set up as a workgroup, you need to log on using an account that's a member of the Administrators group on the computer you're trying to administer (or an account that has otherwise been granted the necessary rights and permissions). Some administrative tasks (managing a printer, for example) don't require Administrators membership, however.

If your network is set up as a Windows 2000 Server–based domain, you must log on using a domain account with sufficient rights and permissions. Members of the Domain Admins group have such privileges on all computers in the domain. Alternatively, you can add your domain user account to the target computer's local Administrators group; to do that, however, you need to visit the computer to add your account to its local security database.

In addition to using an administrative account, you must also be sure that the target computer is properly configured for remote administration. Specifically, the Server service and the Remote Procedure Call (RPC) service must be running. (Because so many other services depend on the RPC service, it's almost certainly running on all the computers on your network.) Some remote management tasks require access to the computer's administrative shares (C$, ADMIN$, and so on)—so those shares must exist on the target computer. In addition, of course, the target computer's network connection must be working properly.

Troubleshooting

Remote administration capability also provides a nifty troubleshooting tool that can save you from reinstalling Windows. If you somehow manage to clobber a computer's setup in such a way that you can no longer log on—believe us, it's possible!—you can sometimes repair the computer (by restoring an essential registry key that you inadvertently changed, for example) from another computer. Simply turn on the computer and let it boot to its logon screen (which you might not be able to see because the video setup is corrupt, for example). Then connect from another computer to commence your repairs.

Using Computer Management

The Computer Management console incorporates the functionality of several Microsoft Management Console (MMC) snap-ins—many of which are also available as separate consoles. Because of its extensive collection of snap-ins, Computer Management might be the only tool you need for managing other computers (depending on what you want to do with them). Specifically, Computer Management includes the capabilities of these snap-ins and extensions:

- Device Manager (also available separately in Devmgmt.msc)
- Disk Defragmenter (Dfrg.msc)
- Disk Management (Diskmgmt.msc)

- Event Viewer (Eventvwr.msc)
- Indexing Service (Ciadv.msc)
- Local Users And Groups (Lusrmgr.msc)
- Logical And Mapped Drives
- Performance Logs And Alerts (Perfmon.msc)
- Removable Storage Management (Ntmsmgr.msc)
- Services (Services.msc)
- Shared Folders (Fsmgmt.msc)
- System Information (Msinfo32.msc)
- WMI Control (Wmimgmt.msc)

If you need to use any of these snap-ins to administer another computer, Computer Management might be your best ticket. Not only do you get all the other snap-ins without creating a custom console, but with a single command you can switch the attention of all the included snap-ins to a different computer. If you use separate snap-ins for each function, you need to redirect each one when you want to switch to a different computer.

To use Computer Management to view information for another computer:

1. Start Computer Management. (Right-click My Computer and choose Manage; from Control Panel, choose Administrative Tools | Computer Management; or type *compmgmt.msc* at a command prompt.)
2. In the console tree, right-click Computer Management (Local) and choose Connect To Another Computer.

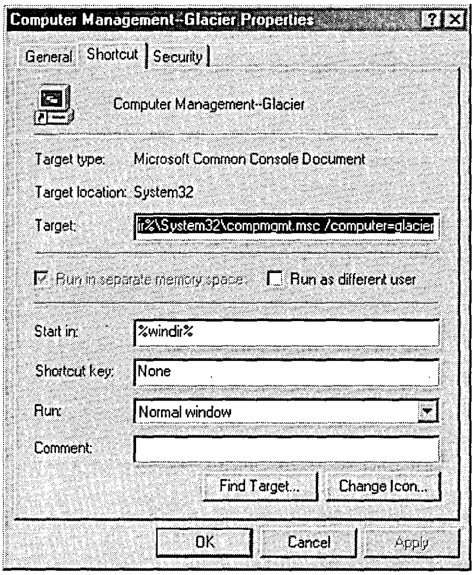
This method provides ad hoc access to another computer. If you want to set up a console that automatically links to one or more computers, create a shortcut or create a new console.

Creating a Shortcut

You can create a shortcut that uses the /Computer command-line parameter. Many MMC consoles—including Computer Management—recognize this command-line parameter, which causes the console to open with its attention focused on another computer rather than on your own local computer. For example, to start a Computer Management window for the computer named Glacier, create a shortcut with *compmgmt.msc /computer=glacier* as its target, as shown in Figure 21-1.

Creating a New Console

Creating a new console allows you to add the Computer Management snap-in for one or more computers. This way, you can create a single console to manage several computers, as shown in Figure 21-2.



Computer Management--Glacier

Target type: Microsoft Common Console Document

Target location: System32

Target: ir%\System32\compmgmt.msc /computer=glacier

☑ Run in separate memory space □ Run as different user

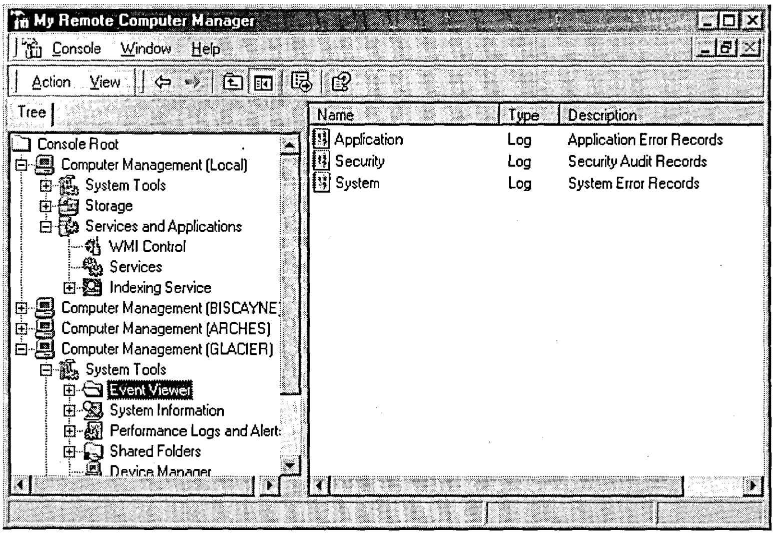
Start in: %windir%

Shortcut key: None

Run: Normal window

Comment:

Figure 21-1
A shortcut lets you automatically connect to another computer.



- Console Root
  - Computer Management (Local)
    - System Tools
    - Storage
    - Services and Applications
      - WMI Control
      - Services
      - Indexing Service
  - Computer Management (BISCAYNE
  - Computer Management (ARCHES)
  - Computer Management (GLACIER)
    - System Tools
      - Event Viewer
      - System Information
      - Performance Logs and Alert
      - Shared Folders
      - Device Manager

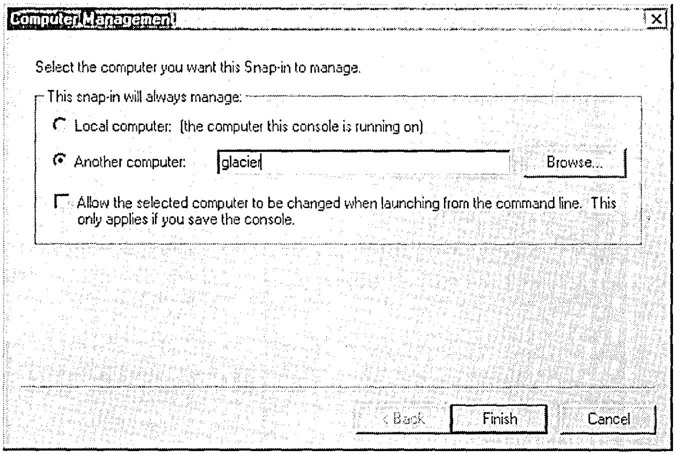
Name	Type	Description
Application	Log	Application Error Records
Security	Log	Security Audit Records
System	Log	System Error Records

Figure 21-2
This console provides access to several computers.

To create such a console:

1. Start MMC. (Type *mmc* at a command prompt.)
2. Choose Console | Add/Remove Snap-In.

3. In the Add/Remove Snap-In dialog box, click Add.
4. In the Add Standalone Snap-In dialog box, select Computer Management and click Add.
5. In the Computer Management dialog box, select Another Computer and type the name of the computer you want. Click Finish.



Computer Management

Select the computer you want this Snap-in to manage.

This snap-in will always manage:

○ Local computer: (the computer this console is running on)

● Another computer: glacier

☐ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

6. If you want to add other computers to the console, repeat steps 4 and 5.
7. Click Close and then click OK.

Make any other changes you want to the console and be sure to save it. *For more information about MMC, see Chapter 4, "Using and Customizing Microsoft Management Console."*

Using Other MMC Consoles and Snap-Ins

Many MMC consoles recognize the /Computer command-line parameter for directing a console to another computer. You can use this parameter at a command prompt or, for a more lasting solution, in a shortcut. For example, to start a Shared Folders window for the computer named Glacier, type *fsmgmt.msc /computer=glacier* at a command prompt.

Note Not all consoles observe the /Computer switch. Those that don't recognize the switch start as if you haven't included it: they operate on the local computer.

Table 21-1 shows the predefined consoles and snap-ins included with Windows 2000 Professional. For each one, the table specifies whether the /Computer switch is functional and how to use the snap-in to work with another computer.

Table 21-1. Remote Administration Capabilities of Predefined Consoles

Console or Snap-In	File Name	/Computer Switch	Remote Access Method
Certificates	Certmgr.msc	No	Create a new console. When you add the Certificates snap-in, select Service Account or Computer Account in the Certificates Snap-In dialog box. *(See "Using the Certificates Snap-In," page 592.)*
Component Services	Comexp.msc	No	Right-click Component Services \Computers and choose New | Computer. (Adding a computer here doesn't affect the Event Viewer and Services snap-ins, which are also part of this console.)
Computer Management	Compmgmt.msc	Yes	Right-click Computer Management (Local) and choose Connect To Another Computer.
Device Manager	Devmgmt.msc	No	Create a new console. (When run remotely, Device Manager is read-only. To install, uninstall, or modify devices or drivers, you must run Device Manager on the computer where you're making changes.) *(See Chapter 16, "Using Device Manager and Hardware Profiles.")*
Disk Defragmenter	Dfrg.msc	No	Disk Defragmenter works only on local hard drives. *(See "Optimizing Disk Performance with Disk Defragmenter," page 672.)*
Disk Management	Diskmgmt.msc	No	Create a new console. *(See "Using Disk Management to Manage Remote Computers," page 199.)*
Event Viewer	Eventvwr.msc	Yes	Right-click Event Viewer (Local) and choose Connect To Another Computer. *(See Chapter 5, "Monitoring System and Application Activities with Event Viewer.")*
Fax Service Management	Faxserv.msc	Yes	Create a new console.
Group Policy	Gpedit.msc	No	Local Group Policy works only on the local computer. *(See Chapter 18, "Using Group Policy.")*

(continued)

Table 21-1. Remote Administration Capabilities of Predefined Consoles (continued)

Console or Snap-In	File Name	/Computer Switch	Remote Access Method
Indexing Service	Ciadv.msc	No	Create a new console. *(See Chapter 6, "Finding Files with the Indexing Service.")*
Internet Information Services	Iis.msc	No	Right-click Internet Information Services and choose Connect. *(See Chapter 27, "Managing a Web Server.")*
IP Security Policy Management	(snap-in)		Create a new console. *(See "Using IPSec," page 490.)*
Local Security Settings	Secpol.msc	No	Local Security Settings works only on the local computer. *(See "Setting Security for Users and Groups," page 293.)*
Local Users And Groups	Lusrmgr.msc	Yes	Create a new console. *(See "Local Users And Groups MMC Snap-In," page 287.)*
Performance	Perfmon.msc	No	Specify a computer when you add counters. *(See Chapter 43, "Monitoring System Performance.")*
Removable Storage	Ntmsmgr.msc	No	Create a new console. You'll need to log on using an account that has the necessary permissions for Removable Storage, for each library, and for each media pool you want to control. *(See Chapter 14, "Using Removable Storage.")*
Removable Storage Operator Requests	Ntmsoprq.msc	No	Create a new console.
Security Configuration and Analysis	(snap-in)		This snap-in works only on the local computer.
Services	Services.msc	No	Create a new console. *(See "Using the Services Snap-In," page 331.)*
Shared Folders	Fsmgmt.msc	Yes	Create a new console. *(See "Using the Shared Folders Snap-In," page 371.)*
System Information	Msinfo32.msc	Yes	Choose Action | Properties. *(See Chapter 41, "Viewing System Information.")*
Windows Management Infrastructure (WMI)	Wmimgmt.msc	No	Right-click WMI Control (Local) and choose Connect To Another Computer.

Some snap-ins don't have a provision for switching to a different computer after they're placed in a console. For these snap-ins, Table 21-1 suggests creating a new console to access another computer. To do that, simply follow the steps in the preceding section, "Creating a New Console." Of course, in the Add Standalone Snap-In dialog box (step 4), you select the snap-in of interest instead of the Computer Management snap-in.

Creating a console this way allows you to set up consoles so that they automatically display another computer (or computers). When you add a snap-in to a console, most snap-ins are set up to ask which computer you want to view. If you save the console, it always opens to the computer you specify here. You can then copy the saved console to other computers; regardless of where you run it from, it will open to the computer you initially specified.

Managing Printers Remotely

You can manage printers anywhere on the network from your computer. Enabling remote administration is a simple matter of setting permissions. By default, the Everyone group has Print permission; members of the Power Users group and the Administrators group also have Manage Printers and Manage Documents permissions. Log on using an account that's a member of either group on the print server, and you have full management control. *For more information, see Chapter 13, "Managing a Print Server."*

Editing a Remote Registry

Both registry editors included with Windows 2000, Regedit.exe and Regedt32.exe, allow you to view and edit the registry on another computer. To work with another computer's registry, the Remote Registry Service must be running on that computer and on your own computer.

In Regedit, choose Registry | Connect Network Registry and then type the name of the computer you want. The new computer appears in the tree pane, as shown in Figure 21-3.

To work with another computer's registry in Regedt32, choose Registry | Select Computer. Regedt32 provides access only to the HKLM and HKU hives. Regedit also enables editing the HKCR hive. *For more information about the registry, see Chapter 39, "Working with the Registry."*

Setting Up Scheduled Tasks

You can set up scheduled tasks on another computer on your network by navigating to its Scheduled Tasks folder. When you connect (via Windows Explorer) as a member of that computer's Administrators group, the Scheduled Tasks folder appears because of your permitted access to the computer's administrative shares.

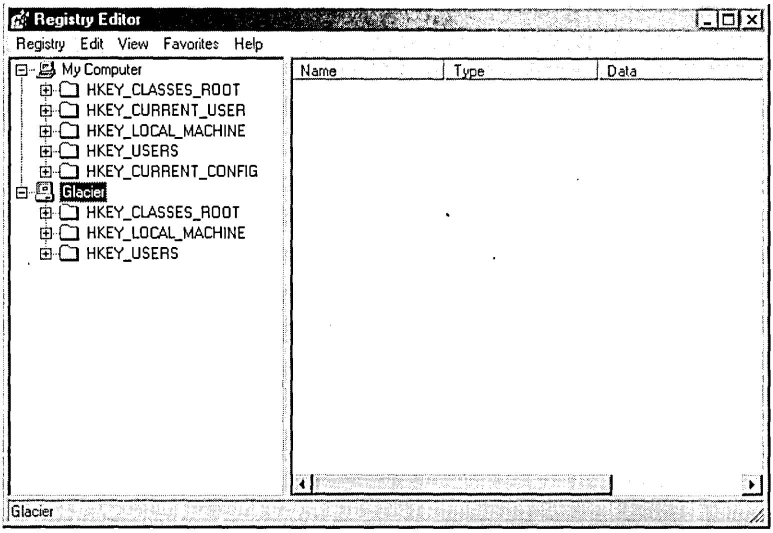


Figure 21-3
Regedit provides access to another computer's HKCR, HKLM, and HKU hives.

When you do this, you won't see an Add Scheduled Task icon, as you do when you display your local Scheduled Tasks folder. However, you can add a task by right-clicking in the folder and choosing New | Scheduled Task (or choosing the same command from the File menu). Adding a task this way doesn't open the Scheduled Task Wizard, so after you create a new task you must open its properties dialog box and specify the program, schedule, and other details.

Aside from the lack of an Add Scheduled Task icon, you might notice one other difference from your local Scheduled Tasks folder: the first four commands on the Advanced menu are unavailable. Although no alternative exists for the dimmed Notify Me Of Missed Tasks command, you can perform the other tasks via the Services snap-in for MMC. The Task Scheduler service controls scheduled tasks. *For more information, see "Scheduling Tasks," page 137.*

Using Command-Line Utilities

It's possible to run command-line programs on another computer. The Remote command, which is included with Windows 2000 Support Tools, lets you actually run a particular program *on* the other computer instead of tying up your own processor. Telnet goes a step further and provides command-line access to another computer.

Remote Command

Remote.exe is part of Support Tools, which you can install by running \Support\Tools\Setup.exe on the Windows 2000 Professional CD. Remote allows you to start a particular text-mode program running on another computer. Remote is limited in capability: it runs only simple 32-bit text-based programs, not programs for MS-DOS or programs for Windows. You must specify the program you're going to run at the remote computer, not at the computer where you plan to launch the program. And Remote is not very secure. Despite these limitations, it can be a useful tool in certain situations. For example, if you develop software, you can use a remote computer to compile code while you use your computer for other tasks.

To use Remote, install Remote.exe on both computers. Then start the server end on the computer where you want to run the program. Finally, start the client end, which starts the remote program running. For details about using Remote, go to Start | Programs | Windows 2000 Support Tools | Tools Help.

Telnet

Through terminal emulation, the Telnet protocol provides the ultimate control for those who prefer to do all their work in a Command Prompt window. The prerequisites for using Telnet are simple, but Windows 2000 is not set up by default to use Telnet.

- First, both computers must be using TCP/IP, the default protocol for Windows 2000 networks.
- The Telnet service must be running on the remote computer. *For details, see "Running a Telnet Server," page 521.*
- You must have an account on the remote computer.

With those prerequisites in place, you simply use any telnet client to connect to the other computer. *(For details, see "Using the Telnet Clients," page 516.)* After you log on by sending your user name and password, you see what appears to be an ordinary command prompt. It's actually the command prompt for the remote computer. You can run all manner of command-line programs as if you were sitting at that remote computer. You can't, however, run Windows-based graphical programs.

Administering a Domain

If your computer is part of a Windows 2000 Server–based domain, you can run all the domain administration tools from a computer running Windows 2000 Professional; you don't need to work at the domain controller. Installing the domain administration tools—the same ones that appear in the Administrative Tools folder of the domain controller—is a simple matter. Install Adminpak.msi, which you can find in the \I386 folder of a Windows 2000 Server CD or in the %SystemRoot%\System32 folder of a computer running Windows 2000 Server. (It's installed on all servers, not just domain controllers.) After you do that, take a look at the Administrative Tools folder. As shown in Figure 21-4, you'll find all kinds of new goodies. For information about using these tools, find a good book about Windows 2000 Server; Microsoft Press publishes several.

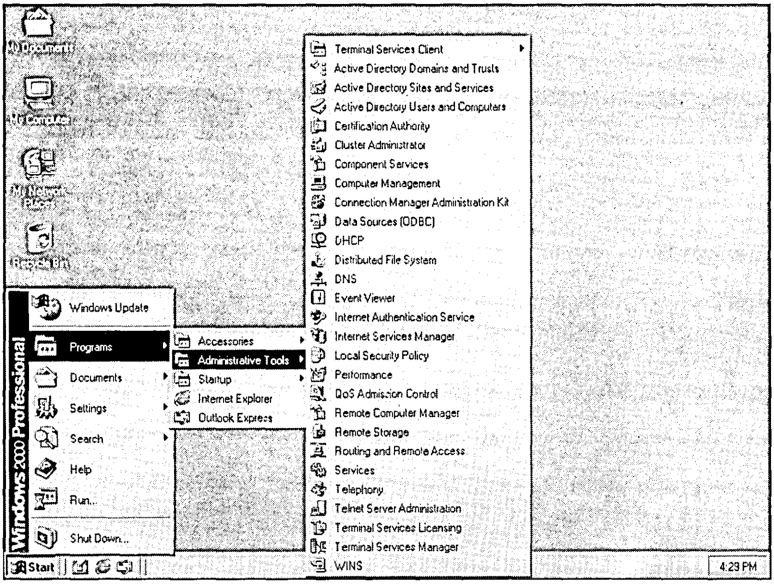


Figure 21-4
Installing Adminpak.msi adds a number of domain administration tools to your Administrative Tools folder.

Note If you have a Windows 2000 domain, another tool you might want to investigate is Terminal Services—a feature available only with Windows 2000 Server. Terminal Services allows many types of computers, including thin clients, older computers, or clients not running Windows, to run Windows-based programs via terminal emulation. You can also use this capability to remotely administer any Windows 2000 Server and, by extension, the other computers on your network.

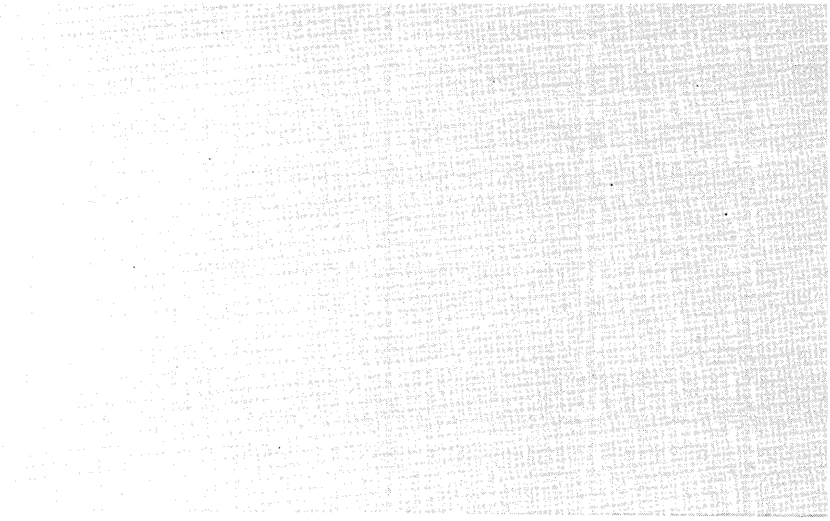
Part 6

Managing Networks

Chapter 22
Making Network Connections 361

Chapter 23
Working with Shared Folders 371

Chapter 24
TCP/IP Core Networking Guide 387



Chapter 22

Making Network Connections

In This Chapter

Setting Up a Peer-to-Peer Network 361
Securing a Peer-to-Peer Network 368

In the previous five sections of this book, the topics we've covered apply, for the most part, to stand-alone computers and networked computers. Part 6, however, describes network-related topics exclusively. It seems only natural, then, to describe in short order how to set up a small network if you don't already have one in place. A network of computers running Microsoft Windows 2000 Professional provides a simple and inexpensive way to share files, Internet connections, printers, and other peripherals.

Setting Up a Peer-to-Peer Network

Peer-to-peer networks are good for small workgroups that don't need the capacity of a dedicated server. They don't require an administrator, because each user decides what information on his or her computer is shared on the network. However, peer-to-peer networks are not always as secure as networks with dedicated servers, because the peer-to-peer setup has no central administration.

To set up a peer-to-peer network, all you need is a network interface card (NIC) for each computer and a network hub if you are connecting more than two computers. All the software you need is included with Windows 2000 Professional. The following sections provide additional details for these steps in setting up a network:

1. Install a NIC in each computer.
2. Connect the cables.
3. Configure the network connection.
4. Configure the workgroup.
5. Begin sharing!

Installing NICs

The first step is to install a network interface card in each computer. Before you purchase a NIC, be sure that it's included on the Hardware Compatibility List for Windows 2000; you can find an updated version online at *www.microsoft.com/hcl*. Follow your computer manufacturer's instructions for installing an expansion card.

When you start Windows 2000 after installing a NIC, Plug and Play detects the NIC. Windows 2000 then installs the necessary software. In many cases, the required files are already on your hard drive (all the driver files that ship with Windows 2000, including those provided as part of a service pack, are stored in %SystemRoot%\Driver Cache\I386\Driver.cab), so the installation proceeds without further ado. In other cases, Windows prompts you for the driver files provided with the NIC.

Connecting the Cables

The next step is to connect all the computers with cables. In this section, we describe 10Base-T wiring, which is generally the most practical option for a small network in an office or a home. 10Base-T is twisted-pair wire with what look like oversized telephone connectors on each end. It's cheap, it's widely available, and it's the most-used network wiring.

Alternatives to 10Base-T

Alternatives to 10Base-T include 100Base-T, which is 10 times as fast as 10Base-T. (10Base-T is nominally designed to carry 10 megabits per second [Mbps]; 100Base-T carries, you guessed it, 100 Mbps.) 100Base-T is rapidly replacing 10Base-T in large network installations. Its improved speed is probably not necessary for small networks, but if you think you might need more speed in the future, it doesn't cost much more to use 100Base-T. To use 100Base-T, use 100Base-T NICs and hubs, and be sure that all your cables are at least Category 5. Many 100Base-T components sold today can switch between 10 Mbps and 100 Mbps, allowing you to gradually convert your network to the higher speed; until all your components run at 100 Mbps, you'll continue to run at 10 Mbps.

Another alternative is Home Phoneline Networking Alliance (HomePNA), which uses existing telephone wiring to carry network traffic—without interfering with your phone use. HomePNA is often the least expensive alternative because the wiring is already in place. Even if you need to add wiring—to add a jack where you currently lack a telephone extension, for example—the cable and the connectors are inexpensive. In addition, you don't need a hub, even if you connect more than two computers. So what's the downside? HomePNA version 1 carries data at only 1 Mbps. The next generation, HomePNA version 2, promises 10 Mbps data rates and should be a serious challenger to 10Base-T in home office environments.

Connecting Two Computers

To network two computers, you can simply connect them with a crossover cable. A crossover cable is usually used to connect two hubs together, so you should be able to find such cables commercially. In case you prefer to make your own cables, Figure 22-1 shows how a crossover cable is wired. By contrast, normal 10Base-T cables are wired straight through, pin 1 to pin 1, pin 2 to pin 2, and so on, as shown in Figure 22-2. The connectors on all 10Base-T cables—crossover or normal—are RJ-45 connectors, as shown in Figure 22-3.

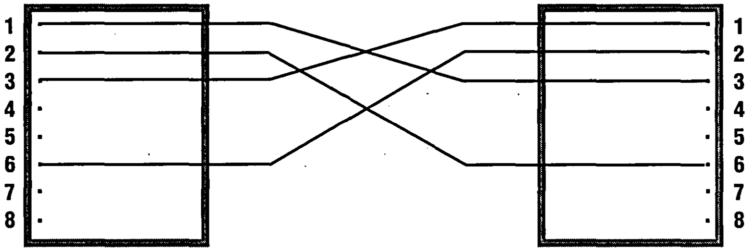


Figure 22-1
Use a crossover cable wired this way to connect two computers directly.

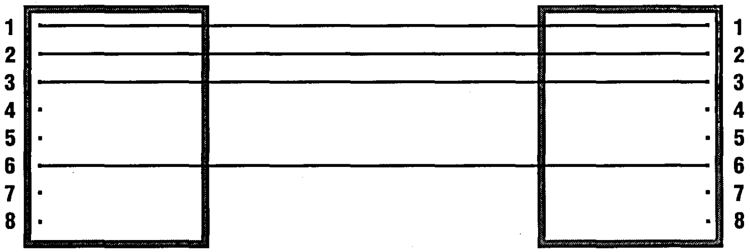


Figure 22-2
Use a straight-through cable to connect a computer to a hub.

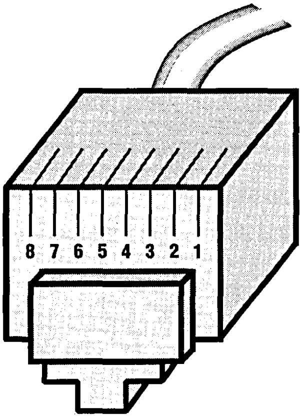


Figure 22-3
If you make your own cables, you need to know the pin-numbering scheme for RJ-45 connectors.

Connecting More Than Two Computers

If you are connecting more than two computers to your network, you need a 10Base-T network hub. This is a small box with a row of jacks for 10Base-T cables, called *ports.* You can get hubs with as few as 4 ports and as many as 24. Place the hub in a central location, because you must run a cable from the hub to each computer you want to network.

It usually doesn't matter which ports you use on the hub, unless one is identified as *uplink.* Uplink ports are used to connect between hubs, and on some hubs they cannot be used to connect to a computer.

Configuring the Connection

When you install a NIC (or when you set up Windows 2000, if the NIC is already installed), Windows creates a local connection that includes the following components:

- **Client for Microsoft Networks.** A *network client* provides access to computers and resources on a network; this client works with Windows-based networks.
- **File and Printer Sharing for Microsoft Networks.** This service allows other computers on your Windows-based network to access shared resources on your computer.
- **Internet Protocol (TCP/IP).** A *network protocol* is the set of rules that computers on a network use to communicate. TCP/IP is the default protocol in Windows 2000 and provides easy connectivity across a wide variety of networks, including the Internet. Although TCP/IP has plenty of options you *can* configure, the default settings mean that you don't *need* to make any configuration changes. *For details, see "Modifying Your TCP/IP Configuration," page 397.*

This default collection of clients, services, and protocols is generally all you need for working with a Microsoft network (that is, one where all computers are running Windows 2000, Windows NT, Windows 98, or Windows 95).

Managing Network Connections

To work with network connections, open the Network And Dial-Up Connections folder, which contains an icon for each of your connections—local area network, dial-up, direct cable connection, and so on. You can get there by clicking Start | Settings | Network And Dial-Up Connections. You can also get there from Control Panel or, if you use Web view, via a link that appears at the left side of many folder windows. If none of those methods suits your fancy, right-click My Network Places and choose Properties.

(continued)

Managing Network Connections *(continued)*

In the Network And Dial-Up Connections folder, you can do the following:

- **Create a new connection.** Double-click the Make New Connection icon.
- **Open (that is, connect using) a dial-up or direct connection.** Double-click its icon.
- **Check an active connection's status.** (Active connections are shown in full color; icons for connections that are currently disconnected are dimmed.) Double-click its icon.
- **Create a desktop shortcut for a connection.** Right-click its icon and choose Create Shortcut.
- **Copy a connection so that you can make changes to the copy.** Right-click its icon and choose Create Copy.
- **View or modify a connection's properties.** Right-click its icon and choose Properties. (You must be logged on as a member of the Administrators group to modify connection properties.)
- **Change your computer's name or join a different workgroup or domain.** Choose Network Identification from the Advanced menu. (You must be logged on as a member of the Administrators group to make these changes.)

Naming Your Workgroup

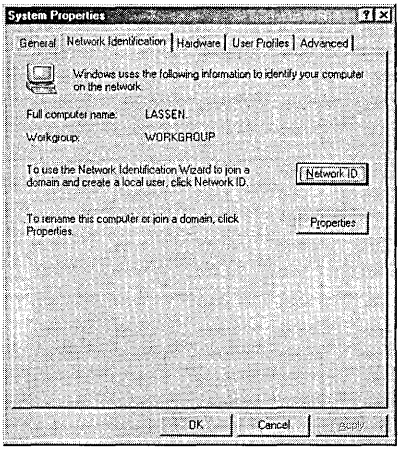
You should now be able to see all the computers on your network by launching My Network Places and double-clicking Computers Near Me. (Computers Near Me appears in My Network Places only if your computer is not in a domain—that is, it's not part of a centrally administered network that uses a domain controller running Microsoft Windows 2000 Server or Microsoft Windows NT Server. If your computer is in a domain, you navigate through My Network Places\Entire Network\Microsoft Windows Network*domainname* to see the other computers in your domain.)

All the computers on your peer-to-peer network must be members of the same workgroup. When you install the NIC, Windows 2000 makes the computer a member of a workgroup called WORKGROUP. You might want to change the name of your workgroup to something a little more appropriate to your situation or to join a different workgroup if your network has more than one.

To "join" a workgroup or to rename your workgroup:

1. Go to System Properties | Network Identification. You can get there in any of the following ways:
   - Right-click My Computer and choose Properties | Network Identification.

- In Network And Dial-Up Connections, choose Advanced | Network Identification.
- In Control Panel, choose System | Network Identification.



Windows uses the following information to identify your computer on the network.

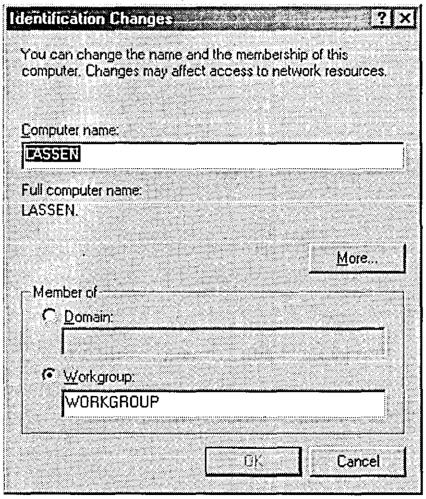
Full computer name: LASSEN.

Workgroup: WORKGROUP

To use the Network Identification Wizard to join a domain and create a local user, click Network ID.

To rename this computer or join a domain, click Properties.

2. Click Properties.



You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name:
LASSEN

Full computer name:
LASSEN.

Member of

○ Domain:

● Workgroup:
WORKGROUP

3. Select Workgroup and enter the workgroup name. A workgroup name can contain up to 15 characters. It cannot be the same as the name of any computer in the workgroup, and it cannot contain any of the following characters:

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

Sharing Printers

Although you can see other computers in My Network Places\Computers Near Me, you won't be able to access anything on those computers until something is shared. The first thing you might want to share is a printer. To share a printer with other users on your peer-to-peer network:

1. Click Start | Settings | Printers.
1. Right-click the printer you want to share and choose Sharing.
3. Select Share As. Change the name if desired.

Your printer is now shared with everyone. This might be appropriate, but you can restrict the use of the printer to certain users by making settings on the Security tab of the printer's properties dialog box. *For more information, see "Setting Printer Permissions," page 223.*

Sharing Folders

To allow other users access to information on your computer, you must share the folders where the information is stored. Doing so makes them visible to others on the network. Follow these steps to share a folder:

1. In Windows Explorer, right-click the folder you want to share and choose Sharing.
2. Select Share This Folder. Change the share name if desired.

This gives everyone full control over the folder and its contents. In many cases, this is appropriate on small networks. You can restrict access to the folder to specific users; the following section provides an overview of the process. *For details, see Chapter 23, "Working with Shared Folders."*

It's important to differentiate between these *share permissions,* which control access to a folder via network connection, and *NTFS permissions,* which control all use of files and folders, whether they're accessed locally or over a network. In effect, these two types of permissions are combined, so network users need both types of permission to use a particular network file. You specify share permissions by clicking the Permissions button on the Sharing tab, as explained in the final section of this chapter; you specify NTFS permissions on the Security tab. *For more information about NTFS, see "Securing Folders and Files," page 544.*

Note NTFS permissions are available only on NTFS-formatted volumes. For shared folders on FAT-formatted or FAT32-formatted volumes, CD drives, and floppy drives, you must rely exclusively on sharing permissions to limit access to your computer's resources.

Securing a Peer-to-Peer Network

Even though you cannot establish the tight security that is possible with dedicated servers, you can still establish reasonable levels of security on a peer-to-peer network. You can control who uses particular shared resources, and you can control what users are allowed to do with shared resources.

You establish control using the same tools that are used on dedicated servers, but the centralized management that servers provide is not available on a peer-to-peer network. This means that you have to make the changes to every computer on the network instead of doing it once on a server. For small networks, this is usually not an insurmountable problem.

To secure resources, you create user accounts, and then you give those accounts permission to use specific resources.

Adding User Accounts on Each Computer

On each computer on the network, add a user account for each user who needs access to the computer's shared resources. If you use the same user name and password on each computer on the network, users won't have to log on to each machine individually. Logging on to their local machine allows them to access all the resources for which they have permission.

Follow these steps to add a user account:

1. In Computer Management, go to System Tools\Local Users And Groups. Alternatively, type *lusrmgr.msc* at a command prompt to open the Local Users And Groups snap-in in its own window.
2. Right-click Users and choose New User.
3. Enter a user name and password. Enter any other information you like.
4. Clear the User Must Change Password At Next Logon check box.
5. Select the User Cannot Change Password and Password Never Expires check boxes.

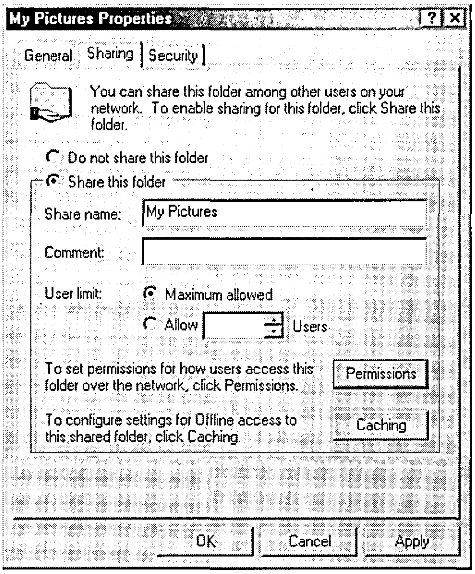
The reason to prevent changing passwords is so that they do not become out of sync on the different computers on the network. The passwords must match on all the computers, or separate logons will be required. *For more information, see Chapter 17, "Managing Users and Groups."*

Adding Permissions to Protect Shared Resources

To restrict access to some resources, you need to give permission to the users who need access to the resource—and be sure that other users do not have permission.

To change permissions on a shared folder, follow these steps:

1. In Windows Explorer, right-click the shared folder and choose Sharing.



My Pictures Properties

General | Sharing | Security

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: My Pictures

Comment:

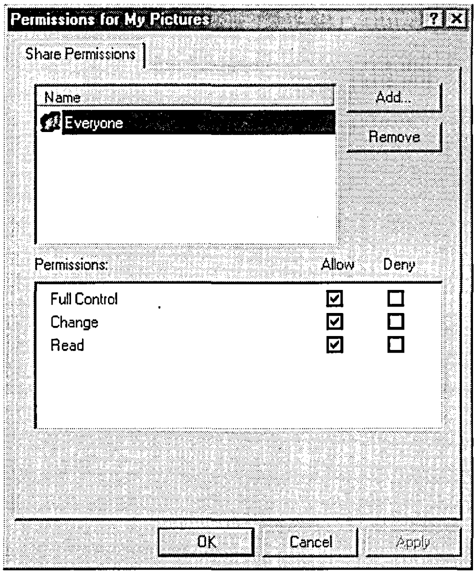
User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

2. Click Permissions. The Permissions For dialog box appears.



Permissions for My Pictures

Share Permissions

Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

3. In Share Permissions, select Everyone and click Remove.

4. Click Add. The Select Users, Computers, Or Groups dialog box appears.

5. Select the user or group to which you want to give permission and click Add. Repeat this step if you want to add permissions for multiple users. Then click OK.
6. Under Allow, select the permissions you want to grant to the selected user or group.

The users or groups in the Share Permissions list are now the only ones who can access this folder across the network. *For more information, see Chapter 23, "Working with Shared Folders."*

Chapter 23

Working with Shared Folders

In This Chapter

Using the Shared Folders Snap-In 371

Offline Files and Caching 376

Command-Line Utilities 380

By sharing resources, you let other people on your network use them. Although you can manage your shared folders from Windows Explorer, the Shared Folders snap-in for Microsoft Management Console (MMC) provides a more centralized approach. This chapter explains how to use the Shared Folders snap-in.

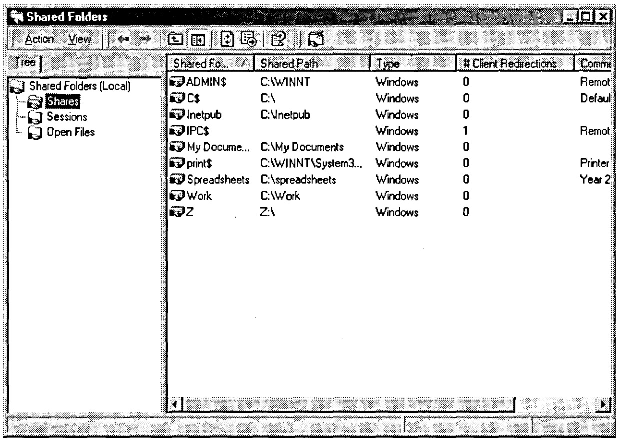
In addition, this chapter explains how to use offline files. At first glance, the connection between shared folders and offline files isn't clear. But for a file to be available offline, it must be stored in a shared folder, and the two features are tightly intertwined.

Finally, this chapter describes some command-line utilities that are useful for managing shared folders.

Using the Shared Folders Snap-In

The Shared Folders snap-in for MMC provides a centralized place to manage all the shared folders on your computer. Start the Shared Folders snap-in by expanding the Shared Folders item in Computer Management (right-click My Computer and choose Manage); you'll find it under System Tools. For the uncluttered view, type *fsmgmt.msc* at a command prompt. Figure 23-1 shows the Shared Folders snap-in.

Note To use the Shared Folders snap-in, you must be a member of the Administrators or Power Users group.

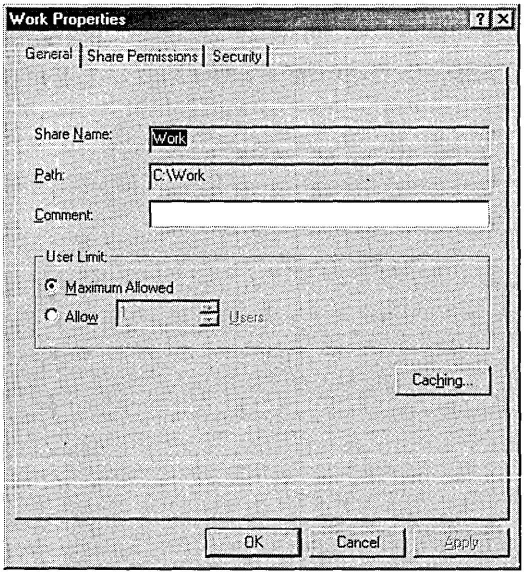


Shared Fo...	Shared Path	Type	# Client Redirections	Comm
ADMIN$	C:\WINNT	Windows	0	Remot
C$	C:\	Windows	0	Defaul
Inetpub	C:\Inetpub	Windows	0	
IPC$		Windows	1	Remot
My Docume...	C:\My Documents	Windows	0	
print$	C:\WINNT\System3...	Windows	0	Printer
Spreadsheets	C:\spreadsheets	Windows	0	Year 2
Work	C:\Work	Windows	0	
Z	Z:\	Windows	0	

Figure 23-1
You can open Shared Folders in its own console window by running Fsmgmt.msc.

Viewing and Changing Share Properties

When you open Shared Folders, all the shared folders on your computer are visible in the Shares folder. You can modify the properties of any folder by right-clicking it and choosing Properties. The associated properties dialog appears, as shown in Figure 23-2.



Share Name: Work

Path: C:\Work

Comment:

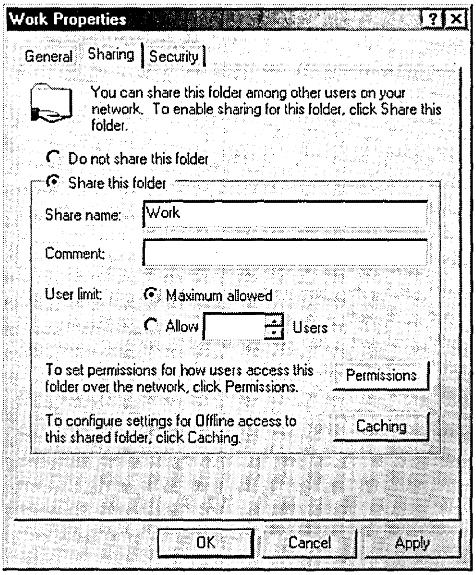
User Limit

● Maximum Allowed

○ Allow 1 Users

Figure 23-2
Choosing Properties in the Shared Folders snap-in produces a dialog box like this.

Note that if you right-click the shared folder in Windows Explorer and choose Sharing, you'll see nearly identical controls, as shown in Figure 23-3. The Permissions button shown in Figure 23-3 serves the same purpose as the Share Permissions tab shown in Figure 23-2.



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder
● Share this folder

Share name: Work
Comment:
User limit: ● Maximum allowed
○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

Figure 23-3
The Sharing tab of a folder's properties dialog box in Windows Explorer provides nearly the same functionality as the General tab in Shared Folders.

Understanding Administrative Shares

Some of the shares you see in the Shared Folders list are created by the operating system. Most of these share names end with a dollar sign ($), which makes them "invisible" because they do not appear in the browse list when another user looks at the shares on your computer. They are not inaccessible, however. Any user who knows these names can connect to these shares simply by typing the share name rather than selecting it from the browse list. You can't view or set permissions on most of these shares, as you can for shares you create; the operating system restricts access to them to accounts with administrative privileges.

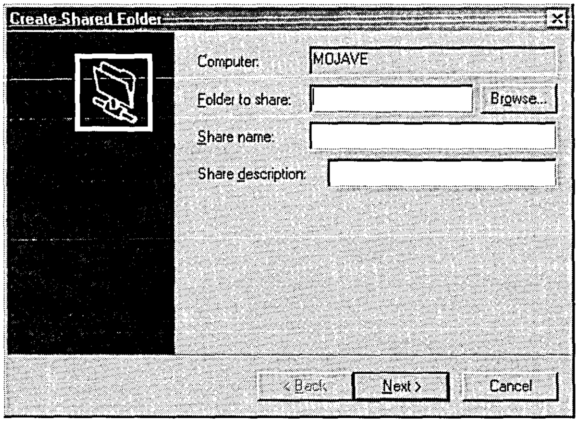
You can stop sharing administrative shares only temporarily. The share reappears the next time the Server service starts or you restart your computer. Table 23-1 describes the administrative shares that appear on most systems.

Table 23-1. Special Shares

Share Name	Description
C$, D$, E$, and so on	Each of these shares allows members of the Administrators and Backup Operators groups to connect to the root folder of a hard drive. You will see one of these (with the appropriate drive letter) for each hard drive on your computer. These shares are often used by backup programs.
ADMIN$	This share is used during remote administration. It maps to the %SystemRoot% folder (C:\Winnt on most systems).
IPC$	This share provides the named pipes that programs use to communicate with your computer. It is used during remote administration and when viewing a computer's resources.
PRINT$	This share is used for remote administration of printers.
FAX$	This share appears on fax servers and is used by clients to send faxes and access cover pages stored on the server.

Creating a New Share

To share a folder, right-click Shares in the console tree and choose New File Share. The Create Shared Folder Wizard appears, as shown in Figure 23-4. This wizard helps you find the folder you want to share and assists in setting up basic security options.



Create Shared Folder

Computer: MOJAVE

Folder to share:

Share name:

Share description:

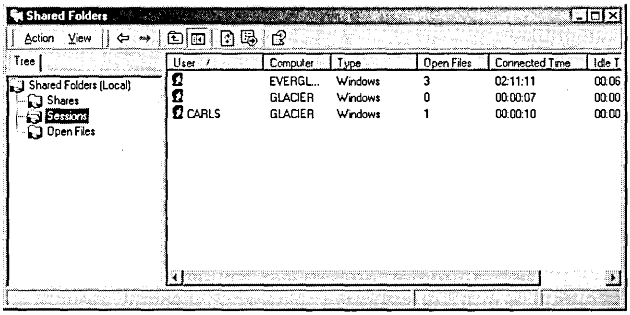
Figure 23-4
The Create Shared Folder Wizard provides an alternative to sharing a folder from Windows Explorer.

Removing a Share

Removing a share is as easy as right-clicking the share and choosing Stop Sharing. To close unnecessary security leaks, periodically opening the Shared Folders snap-in and deleting the "temporary" shares that seem to appear by magic is a good idea.

Viewing and Disconnecting Sessions

Each user who connects to your computer creates a session. You can use Shared Folders to see who is currently connected to the computer as well as what files they have open. Click Sessions in the console tree to have the current sessions appear in the details pane, as shown in Figure 23-5.



User	Computer	Type	Open Files	Connected Time	Idle T
	EVERGL...	Windows	3	02:11:11	00:06
	GLACIER	Windows	0	00:00:07	00:00
CARLS	GLACIER	Windows	1	00:00:10	00:00

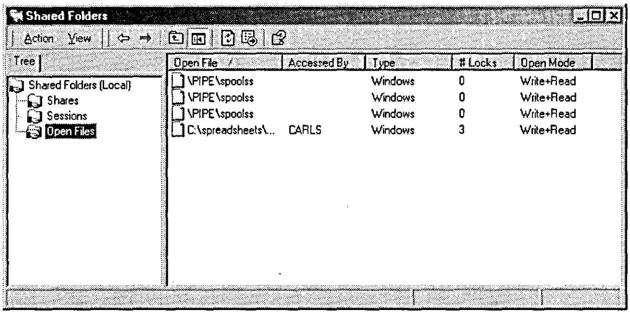
Figure 23-5
The Sessions folder shows all open connections.

Besides seeing who is connected, you can disconnect any or all sessions. Right-click a session and choose Close Session to close a single session. Right-click Sessions in the console tree and choose Disconnect All Sessions to close all the open sessions. Don't do this capriciously; you can cause users to lose information by closing a session while they have documents open.

Viewing and Closing Files

Click Open Files in the Shared Folders console tree to see a list of shared files that are currently open for other users. See Figure 23-6.

You can close an individual file by right-clicking it and choosing Close Open File. You can close all the open files at once by right-clicking Open Files in the console tree and choosing Disconnect All Open Files. If you close a document file while the user has unsaved information, you might cause the information to be lost.



Open File	Accessed By	Type	# Locks	Open Mode
\PIPE\spoolss		Windows	0	Write+Read
\PIPE\spoolss		Windows	0	Write+Read
\PIPE\spoolss		Windows	0	Write+Read
C:\spreadsheets\...	CARLS	Windows	3	Write+Read

Figure 23-6
The Open Files folder shows all files that have been opened by all users.

Warning Other Users

Because closing sessions and files can cause a loss of information, you should warn users who have open sessions and files before you close them. You can send a console message directly from Shared Folders, but the command to do so doesn't appear on the shortcut menu at the location you most expect it. Because Sessions and Open Files are the places where you can most easily disrupt others' work—and therefore are the places where you'd want a way to warn users of an impending shutdown—you might expect to be able to send a message from one of those folders. You can't.

To send a console message, right-click Shared Folders or Shares in the console tree and choose All Tasks | Send Console Message. This command does not appear when you right-click Sessions or Open Files.

When the Send Console Message dialog box appears, the names of all the computers with open sessions (which includes all computers with open files) are in the Recipients list. Simply type your warning message and click Send. *For more information, see "Using the Messenger Service," page 344.*

Offline Files and Caching

Local caching and offline files are two different but intertwined subjects. Caching can provide faster access to network files. Offline files are available even when your network connection is broken. You use the same tools to control both.

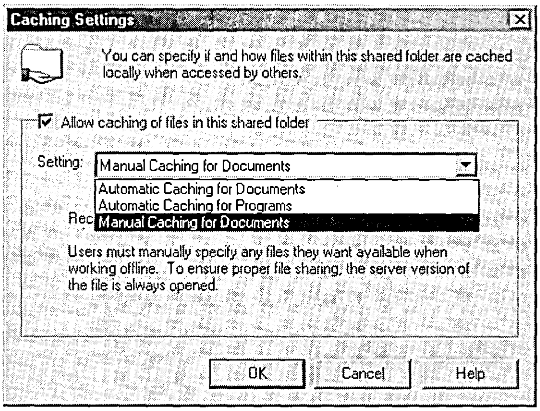
Some of the pieces involved in these processes are on the computer that contains the files (that is, the computer with the shared folder). Because it is acting as one, in this discussion we call that computer the *server*. Other pieces are on the computer that accesses the files, which we call the *client*.

Our discussion here focuses on the server side of the equation. You can find information about the client side—enabling offline files, making folders and files available offline, and synchronizing your offline files with their server-side originals—in *Running Microsoft Windows 2000 Professional* (Microsoft Press, 2000).

Controlling Caching for Offline Use

On the server, one of the properties of a share is the method of local caching for clients that connect to the share. A *cache* stores a copy of a file from a server's shared folder on the client's local hard drive, providing faster access and, more important, the ability to keep using the file even when the server is unavailable.

In the Shared Folders snap-in, right-click the share, choose Properties, and then click Caching. Alternatively, right-click the shared folder in Windows Explorer, choose Sharing, and then click Caching. Either method displays a dialog box like the one shown in Figure 23-7, which offers three options for caching. The following sections describe these options.



Caching Settings

You can specify if and how files within this shared folder are cached locally when accessed by others.

☑ Allow caching of files in this shared folder

Setting: Manual Caching for Documents

Automatic Caching for Documents
Automatic Caching for Programs
Manual Caching for Documents

Rec

Users must manually specify any files they want available when working offline. To ensure proper file sharing, the server version of the file is always opened.

Figure 23-7
You select a caching type for each shared folder.

Manual Caching for Documents

The default caching method is manual caching for documents. When this option is selected, only files that are specifically identified by a client for caching are cached. When you select a file for caching, you are guaranteed that it will be available when you are offline. When you view your Offline Files folder, these files show Always Available Offline in the Availability column.

Note To identify a file for caching, on the client computer, right-click the file and choose Make Available Offline.

Automatic Caching for Documents

Automatic caching for documents is the easiest option to use. Windows decides, on the basis of usage, which files are cached and thus available for offline use. When a file is opened over the network, it is automatically cached. As the cache fills up, documents that have not been used recently are discarded to make room for new documents.

When you open a cached document on a client computer, the cached copy is used, but the original document on the server is also opened to prevent other people from changing the file while you have it open.

Although easy to use, automatic caching for documents does not guarantee that a document will be in the offline cache when you need it. When you view your Offline Files folder, these files show Temporarily Available Offline in the Availability column.

Note If you identify a document for caching from a client computer that is sometimes offline, you can guarantee that the document will be available when you are offline, regardless of the cache setting on the sharing server.

Automatic Caching for Programs

Automatic caching for programs is for folders that contain programs and documents that are read but not changed. In fact, you should restrict permissions on folders with automatic caching for programs to read-only. Automatic caching for programs can speed up access to programs and documents, because after the file is cached, your system does not have to retrieve it from the server; only the local copy is opened. Because of this, automatic caching for programs can speed up access to files, even on computers that are always attached to the network.

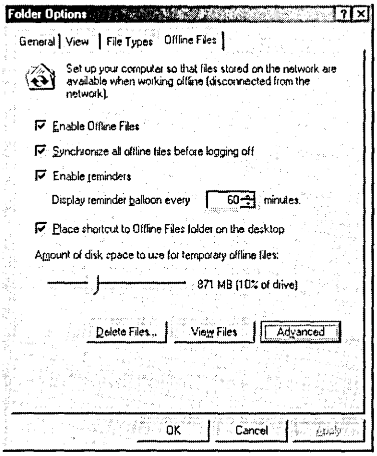
Only files that are used are cached. For example, if you run Microsoft Word from a folder with automatic caching for programs, but you never run the spell-checker, the Word program will be available offline, but the spell-checker will not, because it was never run and thus never cached.

Controlling Caching on the Client

To work with your offline files cache on the client computer, choose Folder Options from the Tools menu in Windows Explorer. Click the Offline Files tab, shown in Figure 23-8.

You can control the maximum size of the cache and other options. If you want to be able to easily view your Offline Files folder, select Place Shortcut To Offline Files Folder On The Desktop.

If you never work offline, but you do want to take advantage of local caching, click Advanced, which opens the Advanced Settings dialog box. See Figure 23-9.



Set up your computer so that files stored on the network are available when working offline (disconnected from the network).

☑ Enable Offline Files

☑ Synchronize all offline files before logging off

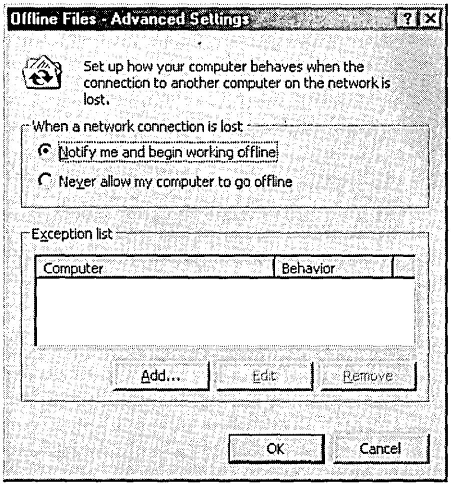
☑ Enable reminders

Display reminder balloon every 60 minutes.

☑ Place shortcut to Offline Files folder on the desktop

Amount of disk space to use for temporary offline files: 871 MB (10% of drive)

Figure 23-8
Use the Folder Options dialog box to configure offline files on the client computer.



Set up how your computer behaves when the connection to another computer on the network is lost.

When a network connection is lost

● Notify me and begin working offline

○ Never allow my computer to go offline

Exception list

Computer	Behavior

Figure 23-9
"Never Allow My Computer To Go Offline" really means "Stop using all network files if my network connection is lost; don't use the local versions."

If you select Never Allow My Computer To Go Offline, network files will become unavailable when you go offline. This might be an advantage if you are always supposed to be connected to a network and want to know immediately if a problem develops. The exception list makes it possible to make these settings on a server-by-server basis.

Troubleshooting

We recently made a network folder available offline, which allowed us to keep working on those documents even when the server was unavailable. This folder contained only a handful of Word documents—the ones we were working with day in and day out. But the folder was deeply nested under the server's share point, and this caused an unexpectedly large collection of files to be cached locally. The network share was set up as \\Acadia\Documents—a shared network drive with several gigabytes of data in addition to the megabyte or so in the folder that we made available offline, \\Acadia\Documents\MSPress\Expert\Manuscript. The problem arose when we used files from other folders on \\Acadia\Documents; they were also added to the local cache. We soon had over 500 MB of data cached locally, and this really slowed access to the network drive.

This happened because the cache settings apply from the share point—not the folder that you make available offline. And caching every file that gets accessed on the server (the same as the Automatic Caching For Documents setting) is the default behavior when the shared folder is on a computer that's not running Microsoft Windows 2000. To avoid this problem, use one or both of these solutions:

- If the server is running Windows 2000, set its caching to Manual Caching For Documents. That way, only the documents that you explicitly make available offline are cached—not all the documents you access from the share.
- Set up a share at the point you want to make files available offline. In the situation described here, sharing the Manuscript folder directly (instead of the Documents folder three levels up) prevents unwanted files from being cached.

Command-Line Utilities

Some users prefer a terse command prompt to an MMC window. If you're in that group, you'll want to use Net.exe for managing resource sharing.

In the following sections, we describe only the most common Net commands (and their most common parameters) for managing network connections. This isn't an exhaustive reference, however. You can get more information from online help or by typing *net help command*, replacing *command* with the word that follows Net in the examples. For example, to get more information about the Net Use command, type *net help use*. This provides more help than typing *net use /?*, which shows only the command syntax.

Net Share

The Net Share command lets you view, create, modify, or delete shared resources on your computer.

Viewing Share Information

Typing *net share* with no parameters causes the program to display a list of the shared resources on your computer, as shown in the following sample:

```
C:\>net share

Share name   Resource                        Remark

-----------------------------------------------------------------------------
print$       C:\WINNT\System32\spool\drivers Printer Drivers
IPC$                                         Remote IPC
ADMIN$       C:\WINNT                        Remote Admin
C$           C:\                             Default share
Inetpub      C:\Inetpub
My Documents C:\My Documents
Work         C:\Work
Z            Z:\
HPLJ4KPS     LPT1:                  Spooled  HP LaserJet 4000 PS
The command completed successfully.
```

If you follow Net Share with the name of a local shared resource, it displays information about that share. For example, the command *net share inetpub* displays the following:

```
C:\>net share inetpub
Share name                                        Inetpub
Path                                              C:\Inetpub
Remark
Maximum users                                     No limit
Users
The command completed successfully.
```

Adding or Modifying a Share

You can share the folder C:\Spreadsheets, for use by an unlimited number of users, and add the comment "Budgets" with the following command:

```
C:\>net share Spreadsheets=C:\spreadsheets /unlimited /remark:"Budgets"
Spreadsheets was shared successfully.
```

Setting a *sharename* "equal" to a folder creates a share. To modify an existing share, you use only the *sharename* (and no folder), as in the following command, which changes the remark on the Spreadsheets share to "Year 2001 Budgets":

```
C:\>net share Spreadsheets /remark:"Year 2001 Budgets"
The command completed successfully.
```

Several parameters can be used with the Net Share command, as shown in Table 23-2.

Table 23-2. Useful Parameters for the Net Share Command

Parameter	Description
/Users:*number*	Sets the maximum number of concurrent users
/Unlimited	Lets the maximum number of users connect to the share at one time
/Remark:"*text*"	Adds or changes a comment that appears in Details view in Windows Explorer
/Cache:automatic or /Cache:no	Sets the document caching option /Cache:manual or to automatic, manual, or no caching

Deleting a User Share

To remove a share, simply use the /Delete switch with the Net Share *sharename* command:

```
C:\>net share spreadsheets /delete
spreadsheets was deleted successfully.
```

Net Use

The Net Use command connects your computer to shared resources on other computers. It can also disconnect, or display, all the resources to which you are connected.

Viewing Connections

Type *net use* with no parameters to display the resources to which you are currently connected:

```
C:\>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           G:        \\EVERGLADES\programs     Microsoft Windows Network
OK           H:        \\EVERGLADES\ChrisW       Microsoft Windows Network
OK           K:        \\EVERGLADES\document     Microsoft Windows Network
OK           P:        \\EVERGLADES\company      Microsoft Windows Network
Disconnected S:        \\Olympic\Perforce        Microsoft Windows Network
The command completed successfully.
```

This maps the network share \\Everglades\ChrisW to the local drive letter E. If you want to use the next available drive letter, use an asterisk (*) instead of the drive letter and colon. You can add any of the parameters shown in Table 23-3.

Table 23-3. Useful Parameters for the Net Use Command

Parameter	Description
password	Enter your password following the share name if a password is required.
/User:*domain* \username	To connect using a user name that is different from the one you are currently logged on with, you can use the /User parameter. The domain name is necessary only if you are not in the same domain as the resource you're connecting to. You can also enter the domain and user name in the format of an e-mail address (for example, *user@domain*).
/Delete	Disconnects the connection. You need only the drive letter and /Delete to disconnect.
/Persistent:yes or Persistent:no	The yes option causes connections to persist so that they / are reconnected the next time you log on.

Disconnecting a Mapped Drive

To disconnect a mapped drive, simply use the /Delete switch with the Net Use *devicename* command:

```
C:\>net use e: /delete
e: was deleted successfully.
```

Net Session

The Net Session command lets you view or disconnect connections between your computer and clients that are accessing it.

Viewing Session Information

Type *net session* with no parameters to display the current connections to your computer:

```
C:\>net session

Computer            User name          Client Type        Opens Idle time

-------------------------------------------------------------------------------
\\EVERGLADES                           Windows NT 1381        1 01:20:24

\\GLACIER                              Windows 2000 2195      0 00:00:07

\\GLACIER           CARLS              Windows 2000 2195      1 00:00:04

The command completed successfully.
```

Disconnecting a Session

Following Net Session \\computername, append /Delete to disconnect a session. If you don't include \\computername, all active sessions are disconnected.

Net File

The Net File command lets you view or close the open shared files on your computer. Typing *net file* with nothing following it causes the program to list all the open files, including a file ID, the user name of the person who has the file open, and the number of locks each has:

```
C:\>net file

ID          Path                                   User name         # Locks

-------------------------------------------------------------------------------
108980      \PIPE\spoolss                                                0
109011      C:\spreadsheets\Q1 Budget.xls          CARLS                 3
The command completed successfully.
```

You can close a file by following Net File with the ID of the file and /Close:

```
C:\>net file 109011 /close
The command completed successfully.
```

Net Statistics

The Net Statistics command displays the statistics log for the local Workstation or Server service. Type *net statistics workstation* to view the Workstation statistics. Type *net statistics server* to view the Server statistics.

The workstation statistics log looks like this:

```
C:\>net statistics workstation
Workstation Statistics for \\MOJAVE


Statistics since 4/21/2000 4:06 PM


  Bytes received                              232765115
  Server Message Blocks (SMBs) received       394263
  Bytes transmitted                           65653800
  Server Message Blocks (SMBs) transmitted    393773
  Read operations                             187879
  Write operations                            1258
  Raw reads denied                            0
  Raw writes denied                           0

  Network errors                              0
  Connections made                                    20
  Reconnections made                                  24
  Server disconnects                                  7

  Sessions started                                    102
  Hung sessions                                       0
  Failed sessions                                     0
  Failed operations                                   0
  Use count                                           126
  Failed use count                                    2

The command completed successfully.
```

Chapter 24

TCP/IP Core Networking Guide

In This Chapter

Introduction to TCP/IP 387

Modifying Your TCP/IP Configuration 397

Using Tools for Network Troubleshooting 406

Setting Advanced Options 409

Setting Up Non-TCP/IP Connections 411

The day of the stand-alone computer is long gone. Even a single home computer will almost always be connected to the Internet, and many homes now network two or more computers together. Microsoft Windows 2000 is steeped with internetworking capabilities. To make the best use of these capabilities, or to create an other than standard network configuration, it is helpful to understand some internetworking concepts. This chapter provides an introduction to some low-level aspects of internetworking. You can find a library of books on any one of these topics, but unless you are a systems or network administrator, you don't need to get out your library card. After presenting the theory, we discuss your network settings—where they are and what you can do with them.

Introduction to TCP/IP

TCP/IP stands for Transmission Control Protocol/Internet Protocol. This is the last time you'll need to know that. Contrary to what the name suggests, TCP/IP is actually a suite of protocols that make up a layered model of internetworking functionality. At the bottom layer of the model is the physical connection between computers. This connection might be Ethernet, 10Base-T, or some other cable or even radio specification. Just above that layer is the data link, the way the network interface card sends and receives bits along the physical medium. The layers go all the way up to the top layer, where applications make networking calls.

Strictly speaking, TCP/IP refers to two intermediate layers in this model. (In common usage, TCP/IP is used to refer to the entire model.) TCP operates at the transport layer and is responsible for the end-to-end network connection. This layer ensures that messages get from the source to the destination without errors. IP operates at the network layer. The network layer handles routing between the source and the destination, including the important issue of addressing.

Many networking decisions and problems involve one or more levels of IP addressing. When you set up a new network, you might need to configure addresses and subnets. In this section, we discuss the basic concepts of addressing, subnets, and domain name servers.

IP Addresses

Each network interface card (NIC) ever made has a unique hardware address. If you want, you can find out the address of the NIC in your computer, but you don't have to. (If you're consumed by curiosity, type *ipconfig /all* at a command prompt and look for Physical Address.) Your computer is assigned an IP address, which is what the outside world is interested in. At some point, your computer translates its IP address to the hardware address of your NIC, but we won't concern ourselves with physical NIC addresses here.

IP addresses are 32-bit numbers composed of four 8-bit bytes. IP addresses are normally viewed by the decimal representation of each byte delimited by periods. This is sometimes called the *dotted-decimal IP address* or the *dotted quad format*. For example, the address 169.254.0.10 is the dotted quad format of the 32-bit binary address 10101001 11111110 00000000 00001010.

IP addresses include a network ID followed by a host ID. The network ID component of the address identifies the network the computer is on, and the host ID component identifies a particular computer on that network. The combination of bits that compose these two parts is determined by the IP address class. Three classes are in common use: class A, class B, and class C. Classes D and E also exist, but they are used for special purposes.

The address class system allows for an efficient allocation of addresses to networks in blocks. For example, if there were only two networks in the world, each with a huge number of computers on it, then the first bit of the first byte could be used as the network ID and the remaining 31 bits of the address could be used for host IDs. In this case, one of the networks would have network ID 0 and the other would have network ID 1. With the remaining 31 bits, each network could address 2,147,483,648 computers. But more than two networks exist in the real world. And networks have a range of computers they contain. This is where the address class system comes in.

For example, class A addresses use the first byte as the network ID and the remaining three bytes as the host ID. Class B addresses use the first two bytes as the network ID. Classes are distinguished by their value in the first byte; for class A addresses, the first byte is in the range 1 through 126; the first byte of class B addresses is in the range 128 through 191. Table 24-1 shows the class ranges and the use of bytes for network and host IDs.

Table 24-1. Address Classes for IP Addresses of the Form B0.B1.B2.B3

Address Class	First Byte Range	Network ID Bytes	Host ID Bytes	Networks Available	Hosts Available
Class A	1–126	B0	B1.B2.B3	126	16,777,214
Class B	128–191	B0.B1	B2.B3	16,384	65,534
Class C	192–223	B0.B1.B2	B3	2,097,152	254

Note If you're fluent in binary arithmetic, you might have calculated that the number of available hosts in each of the address classes is two more than the value shown in Table 24-1. These values shown are correct, however, because two values (0 and 255) are not permitted in the last byte.

Private Reserved Addresses

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets:

10.0.0.0–10.255.255.255

172.16.0.0–172.31.255.255

192.168.0.0–192.168.255.255

If you are setting up a small business or a home network that will not be connected to the Internet, or that will be connected through a single proxy server, you can freely use these addresses without concern for conflicts. If your network is not connected to the Internet, you can use any IP addresses you please, but if you ever do connect to the Internet, you will need to readdress your network computers lest confusion reign.

Anyone who decides to use IP addresses from the preceding ranges can do so without any coordination with IANA or an Internet registry. These addresses are thus used on many networks. Addresses within this private address space will be unique only within the given network.

Subnets

Although the computers can be connected in physically different ways, each network is a set of computers directly connected to each other. Networks are separated from each other by some form of router. A computer on one network is connected to a computer on another network through one or more routers. When a router receives an IP packet, it checks the network ID portion of the packet's destination address. If the network ID is for a network connected to the router, the router broadcasts a message over that network to see whether the host ID corresponds to a computer on that network. If it does, that computer gets the packet.

When you are assigned a network ID, that ID applies to your entire organization, no matter what your organization's network configuration looks like. If your network is actually composed of multiple networks connected by routers, you need some way to forward network traffic to the correct network so that it reaches the correct destination. This is because all IP packets with your organization's network ID will be sent to a single router. If you have only one network at your organization—that is, all your computers are connected to the one receiving router—you have no problem. But if some of your computers are removed from the receiving router by another router, when the receiving router broadcasts a message looking for the computer with the matching host ID, it won't be found.

Subnets fix this problem by allowing you to divide your network into multiple smaller pieces using subnet masks. A *subnet mask* is a 32-bit number that, when ANDed with an IP address, gives the network ID portion of the address. For a class C address, where the network ID is in the first three bytes, the subnet mask would be 255.255.255.0 (11111111 11111111 11111111 00000000). Because the outside world is concerned only with the network ID portion of any address on your network, you are free to use the host ID bits in any way you choose. You can use some of those bits to designate subnets. For example, if you had a class C network with 100 computers on three subnets, you could use two bits of the host ID to designate the three subnets. You would then tell your routers and all computers on your network to use a subnet mask of 255.255.255.192 (11111111 11111111 11111111 11000000). That mask would hold the network ID in the first three bytes, plus two more bits to identify the subnets on your network. You would then use the last six bits of the IP address for host IDs on each subnet, giving 64 unique host IDs per subnet.

Table 24-2 shows the addresses for the example just described. In the table, the subnet ID portion of each subnet address is underlined. Routers on the Internet would recognize the address as a class C address and use the subnet mask 255.255.255.0 to determine the network ID of 192.222.111.0. The Internet routers would then send the data packets to your router, which would use the subnet mask 255.255.255.192 to determine where to forward the packets.

Table 24-2. Sample Subnet Addresses

	Binary Representation	Dotted Quad
Net ID	11000000 11011110 11011111 00000000	192.222.111.xxx
Subnet 1	11000000 11011110 11011111 00000000	192.222.111.0
Subnet 2	11000000 11011110 11011111 01000000	192.222.111.64
Subnet 3	11000000 11011110 11011111 10000000	192.222.111.128
Subnet mask	11111111 11111111 11111111 11000000	255.255.255.192

Subnet masks are an integral part of your TCP/IP configuration, even if you don't use subnets. The class of network you have (determined by the value of the first byte in the address) and any subnets you define determine the value of the subnet mask that you enter in your TCP/IP settings.

Gateways

The preceding description of routing concerns incoming data packets. Another set of addressing issues concerns outgoing data packets. When a data packet is sent out from your computer, your computer compares the packet's network address against its own subnet address to see whether the packet destination is on the same subnet. If the destination is on the same subnet, your computer broadcasts a message to see which machine has the corresponding host ID. That computer sends back a message containing its hardware address, and a session is established.

If the destination address is not within the local subnet, your computer forwards the packet on to a gateway router. This router then determines whether the network ID in the packet is for one of the networks to which it is directly connected. If it is, the gateway router sends the packet to that network. If the gateway router determines that the network is not local, it forwards the packet to its own gateway. Eventually, the packet either makes it to its destination, dies (times out), or gets returned as undeliverable.

You need to know the address of your gateway router. If you are connected by modem to an Internet service provider (ISP), your gateway will probably be at your ISP, and the ISP should be able to provide you with that information.

Routing

Typically, you allow your default gateway to handle all network routing matters. Windows 2000 Professional cannot act as a router in the sense of accepting and forwarding IP packets. But it does handle routing of data packets originating from your computer.

Routing relies on tables. Whether you are using a hardware router dedicated to this one task, a software routing server on a network server, or a Windows 2000 Professional system sending its own data packets over a network, tables are used to determine where to send the data packets. Windows 2000 allows you to set up a routing table on your system that it references before sending packets to the default gateway.

Routing tables can be maintained as static or dynamic. Static routing tables must be updated manually, whereas dynamic tables use a protocol to automatically update routes based on routing information sent out by other routers. Windows 2000 Professional allows one dynamic routing protocol, Routing Information Protocol (RIP) Listening. RIP Listening adds dynamic updates to your routing table. *For more information, see "RIP Listening," page 405.*

The routing table maintains four types of routes, listed as follows in the order in which they are searched for a match:

1. Host (a route to a single, specific destination IP address)
2. Subnet (a route to a subnet)
3. Network (a route to an entire network)
4. Default (used when no other match is found)

When you use the Route Print command at a command prompt, a listing of the current routing table is displayed. It looks something like the following:

```
C:\>route print
============================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 c0 f0 2b 03 55 ...... Intel DC21041 PCI Ethernet Adapter
============================================================================
Active Routes:
Network Destination        Netmask          Gateway        Interface  Metric
          0.0.0.0          0.0.0.0       10.0.0.241       10.0.0.241       1
         10.0.0.0    255.255.255.0       10.0.0.241       10.0.0.241       1
       10.0.0.241  255.255.255.255        127.0.0.1        127.0.0.1       1
   10.255.255.255  255.255.255.255       10.0.0.241       10.0.0.241       1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
        224.0.0.0        224.0.0.0       10.0.0.241       10.0.0.241       1
  255.255.255.255  255.255.255.255       10.0.0.241       10.0.0.241       1
============================================================================
Persistent Routes:
  None
```

The Interface list shows all the network interfaces on your computer, including one for loopback testing. This list shows the hardware addresses of the physical devices. The Active Routes list shows all routes configured by Windows. This routing table is for a computer with IP address 10.0.0.241, indicating that it is on a private network.

The first line with destination 0.0.0.0 is the default gateway. The second line is for the network (or subnet) for this computer (10.0.0.0). The subnet mask of 255.255.255.0 indicates that the host ID is in the fourth byte, which means that this is a class C network with network ID 10.0.0 and host IDs from 1 through 254. (Host ID 0 is reserved for the network itself, and 255 is reserved for network broadcasts.) This subnet mask also tells us that the network is not subdivided. The third line is the host route for this computer. The destination of the host route is the host ID, but the interface is the loopback address, which keeps data packets from attempting to go out and in at the same place. Typically, the loopback comes into play only when you're doing troubleshooting.

The fourth line is for network broadcasting. It is defined by default. The fifth line is the loopback route with the destination loopback address defined by default as

127.0.0.0. The loopback route is similar to the host route. Both use the loopback interface, but the address of 127.0.0.0 is always self-referential. If you send a packet to host ID 127.0.0.0 on any computer, it will always be sent to that computer's loopback adapter. However, if you send a message to host ID 10.0.0.241, it will be sent out on the network unless the computer sending the message is assigned 10.0.0.241 as its own ID. In that case, the message will be sent to the loopback adapter. The sixth line is for subnet broadcasting. The seventh line is for IP multicasting.

In looking at this table, it's important to note that, except for the loopback connection, both the interface and the gateway are defined as the host computer. This means that the host computer handles routing for anything going out from the host to anywhere on its own private network. Also notice the metric in the table. The *metric* is a measure of how far a network is from you. The unit of measure is arbitrary, but it is usually taken to be the number of routers between two networks. The metric for each of these connections is 1, which makes sense because the host is its own router.

Domain Name System

All of this is fine and good, but who wants to remember and enter IP addresses like 169.254.0.10, let alone 10101001 11111110 00000000 00001010, for each computer they want to reach? Hence the use of host names. Host names are easy-to-remember (usually), real-language names such as accounting1, gandalf, or neptune. Every computer on a network is assigned a host name. When you attempt to connect to another computer on your network or an outside network using its name rather than its IP address, that name has to be translated to an IP address (which in turn gets translated to a hardware address, but we're not talking about that here). This translation is called *name resolution*.

Things get a little complicated here. Older Windows systems used a name resolution scheme designed for small local networks. These systems use NetBIOS host names and a resolution scheme called Windows Internet Name Service (WINS). Meanwhile, the Internet developed a resolution scheme called Domain Name System (DNS). Windows 2000 uses DNS by default but can also use WINS to support computers on a network that uses NetBIOS names.

NetBIOS names use a flat structure, which can be described by tables that simply map NetBIOS names to IP addresses. If you want to know the IP address of the computer at the next desk or one across the world, you need to have a line in your table with its name and IP address. In fact, this involves not one table but as many as three: a NetBIOS name cache in your computer's memory, a table of registered names on a WINS server, and a local file on your hard disk called Lmhosts. In addition to the tables, the WINS client can broadcast a message to all other computers on its local network asking for a name resolution. A broadcast query is the default setting for Windows 2000.

DNS uses a hierarchical structure. Your computer has its own name, but in the network world, your computer name has your network's domain name appended to it, which describes the hierarchy. Most domains belong to one of a handful of top-level domains (TLDs). Each domain is then subdivided into second-level domains. These second-level domains can be further divided. Figure 24-1 shows a sample of top-level and lower-level domains.

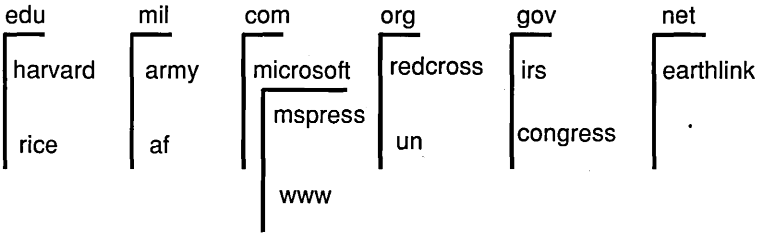


Figure 24-1
In the Internet Domain Name System, top-level domains (such as edu, mil, and com) are subdivided into second and third levels.

Other top-level domains are primarily for countries (au for Australia, uk for the United Kingdom, and so on). A large set of new top-level domains such as firm, nom (for individuals), store, and arts has been proposed. These have not yet been approved.

Domain names are constructed by starting with a host name (hosts are typically analogous with computers, but not always), adding a period (dot), and then adding domain names up the chain, each separated by a period. So, if you wanted to identify the mspress computer at Microsoft, you would use a domain name of mspress.microsoft.com. A complete domain name is called a Fully Qualified Domain Name (FQDN).

The leftmost name in the domain name can be a server rather than a host name. To address the World Wide Web server at Microsoft, for example, you use the FQDN *www.microsoft.com.* Domain names can be longer than three terms. So, for instance, if mspress was a subdomain of the microsoft domain, and bill was the name of a computer on the mspress subdomain, its FQDN would be bill.mspress.microsoft.com.

Domain name resolution is handled in a couple of ways. Individual computers can keep a table of domain names and IP addresses. This text file is named Hosts (with no file name extension), and in Windows 2000 it is kept in the %SystemRoot% \System32\Drivers\Etc folder. Microsoft has kindly supplied a sample Hosts file, which can be edited with any standard text editor.

Unfortunately, it is not practical to keep a table with all the computers in the world listed. Fortunately, the designers of the Internet provide a solution.

The Internet is littered with DNS servers whose only mission in life is to resolve domain names into IP addresses. The DNS servers constitute a distributed network. That is, no DNS server contains records for all FQDNs, only for a subset. If you query a DNS server and it doesn't have a record for the system you're trying to reach, it asks another server until the name is resolved. In your TCP/IP settings, you can identify one or more DNS servers to use to resolve domain names.

Windows 2000 Professional cannot be a DNS server, though Microsoft Windows 2000 Server can. Windows 2000 uses DNS as its operating system naming service. In particular, this means that Active Directory uses DNS in translating names of network resources.

Getting Your Own IP Address and Domain Name

The mechanism for allocating IP addresses and domain names is in flux, as responsibility is shifted from government and educational organizations to private companies. At this time, you will most likely obtain an IP address from an Internet service provider and your domain name from one of several name registration companies.

ISPs are allocated blocks of IP addresses, which they in turn assign to their customers. If you use a dial-up connection to connect a single computer to the Internet, the ISP dynamically assigns an IP address from its allocated block to your computer each time you connect. ISPs maintain a subset of their addresses for this purpose. If you have a persistent connection to your ISP via a cable modem or DSL modem, you might be assigned a permanent IP address by your ISP. In either of these cases, the computer you connect to the Internet might serve as a gateway for a network. For example, if you have a small office network, you might have one computer connected to the Internet that serves as a *proxy* for the rest of the network. All other computers on your office network would connect to the Internet through the proxy. Only the proxy would need a unique IP address; the others can use addresses from the private network range.

You might also have a network of your own in which you want each computer to have its own unique IP address. In this case, you need to make special arrangements with an ISP. You can also contact the Internet Assigned Number Authority directly at *www.iana.org*. From there you will be directed to a regional registry. In the United States, that is the American Registry for Internet Numbers (ARIN) (*www.arin.net*). ARIN allocates blocks of IP addresses to ISPs. It also assigns IP addresses to end users for their exclusive use in their own networks. (The smallest block of IP addresses that ARIN assigns is 4096. If you don't need that many—and most networks don't—you will need to deal with your ISP.)

(continued)

Getting Your Own IP Address and Domain Name *(continued)*

You have to handle domain names separately. A number of private companies now handle domain name registrations. A list is available from the Internet Corporation for Assigned Names and Numbers (ICANN) at *www.icann.org*. You must first decide on the domain name you want. Then you need to check to see whether it is already registered. You can go to any of the registrars listed at ICANN and find a Web page with a registry search utility that will tell you whether your desired name is available.

After you find an available domain name, you need to pick a registrar. This is where the fun begins. The use of private companies to handle domain registration is quite new, and the kinks have not yet been worked out of the system. Each company offers slightly different services at slightly different prices. You should shop around to find the best deal for the services you want. The basic service is to simply register your domain so that it is allocated to you and no one else.

You also need another service that makes the whole system work: having your domain name to IP address resolution entry placed in a DNS server. Without this, no one who uses your domain name will be able to get to your computer. ISPs typically have provided this service. Because the IP address is in their block and they handle the routing at your end, it makes sense that they would handle the DNS entry also. Some of the domain registrars might perform this service for you at a lower cost than what many ISPs charge, however. Your ISP might not like it, but going this route is perfectly legitimate.

Most ISPs are happy to handle the entire process for you, from registering your domain name to entering it into their DNS servers. They are also happy to charge you for this service. The benefit of going through an ISP is that you have only one place to call when something doesn't work.

DHCP and APIPA

Each computer on a network must know its own IP address, subnet mask, gateway address, DNS server addresses, and WINS server address. Keeping track of this information involves much more than most users are up to, and if a system administrator had to manage all those addresses for all the computers on a network, the administrator would have a management nightmare. Dynamic Host Configuration Protocol (DHCP) is designed to relieve that nightmare. DHCP provides a centralized server for managing all these configuration items for all computers on a network.

If you are using DHCP and your DHCP server is running when you boot your computer, your DHCP client sends a request to the server for an IP address. The DHCP server then automatically assigns an IP address, subnet mask, gateway address, DNS address, WINS address, and whatever else it is configured to assign. These assignments are made whenever you start your computer, so your IP address will probably be different each time.

With Windows 2000, you are not lost if you don't have a DHCP server on your network. By default, Windows 2000 Professional uses Automatic Private IP Addressing (APIPA). APIPA first tries to find a DHCP server on the network. If it can't find one, APIPA automatically generates an IP address, broadcasts a message on the network to see whether that address is being used, and then assigns it to your computer. After it assigns an IP address, APIPA continues to poll for a DHCP server to confirm the address assignment. The address that APIPA generates is in the range 169.254.0.1 through169.254.255.254 with a subnet mask of 255.255.0.0. This address range is reserved for APIPA, so the assigned ID will not conflict with any ID on the Internet.

APIPA allows you to set up a small network without a DHCP server and still receive the benefits of automatic IP addressing. A drawback is that APIPA cannot assign gateway, DNS, or WINS addresses.

If you are running Windows 2000 Server, you need to be aware of a number of configuration items; those settings are beyond the scope of this book. If you are running only Windows 2000 Professional on your network, APIPA (and therefore DHCP) is configured by default. You don't need to worry about any network IP settings—unless you want to. We discuss all these settings in the following sections.

Modifying Your TCP/IP Configuration

Windows 2000 is kind enough to offer two separate sets of advanced network properties. You get to either set from the Network And Dial-Up Connections folder. The first set, which applies to all network connections, is reached from the Advanced Settings command of the Advanced menu in the Network And Dial-Up Connections window. (To open the Network And Dial-Up Connections folder, right-click My Network Places and choose Properties. Alternatively, open Network And Dial-Up Connections in Control Panel or on the Start menu's Settings menu.)

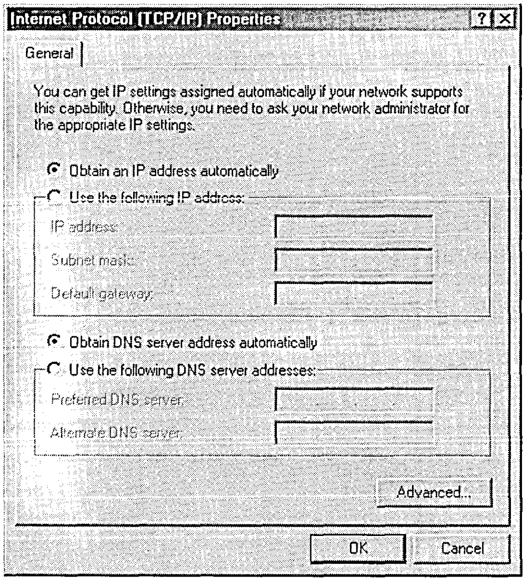
These settings control adapters and binding order and network provider order. *See "Setting Advanced Options," page 409, for details about these options.*

Note The Tools and Advanced menus in the Network And Dial-Up Connections window provide access to several configuration settings for network and dial-up connections. From the Tools menu, you can map or disconnect network drives and synchronize offline content. The Advanced menu has selections for setting dial-up preferences and network identification (host name and domain or workgroup name), configuring advanced network parameters, and adding networking tools. This is a new organizational feature of Windows 2000.

Setting Connection-Specific TCP/IP Properties

A second set of advanced properties is defined for each network connection in your system. To reach these properties:

1. Right-click a network connection in the Network And Dial-Up Connections folder and choose Properties.
2. On the General or Networking tab (depending on the connection type), select Internet Protocol (TCP/IP) and click Properties to display the Internet Protocol (TCP/IP) Properties dialog box, shown in Figure 24-2. We'll discuss these settings first.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Figure 24-2
Use the Internet Protocol (TCP/IP) Properties dialog box for basic TCP/IP configuration.

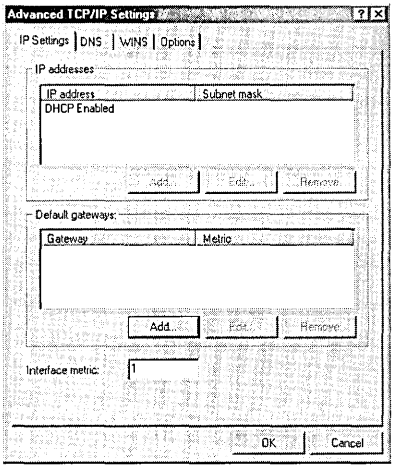
3. Click Advanced to bring up the Advanced TCP/IP Settings dialog box, as shown in Figure 24-3. We'll discuss these settings second.

In the Internet Protocol (TCP/IP) Properties dialog box, you can set a static IP address, subnet mask, and default gateway combination. Or you can choose to obtain these automatically (that is, through a DHCP server or APIPA). You have the same choices for setting primary and secondary DNS servers. By default, these are both set to obtain addresses automatically. If you want to set static addresses, this is the place to do it.

If, for example, you connect to your ISP through a cable modem or use a DSL connection that uses a static IP address (some do and some don't), your ISP assigns a static IP address, subnet mask, and two default gateway addresses. This is where you configure them. Select Use The Following IP Address and then enter the correct addresses. A nice feature of Windows 2000 is that you don't have to reboot after changing IP addresses, as you did in earlier versions of Windows and Windows NT.

When you turn off automatic IP addressing, you also turn off automatic DNS addressing. Your ISP should also tell you what IP addresses to use for primary and alternate DNS servers. Enter them in the lower portion of the Internet Protocol (TCP/IP) Properties dialog box.

Note Changes in the Internet Protocol (TCP/IP) Properties dialog box take effect as soon as you click OK in the properties dialog box for the connection. You can confirm that they have taken effect by typing *ipconfig /all* in a Command Prompt window.



IP address	Subnet mask
DHCP Enabled	

Gateway	Metric

Interface metric: 1

Figure 24-3
The Advanced TCP/IP Settings dialog box offers more esoteric options.

IP Settings Tab

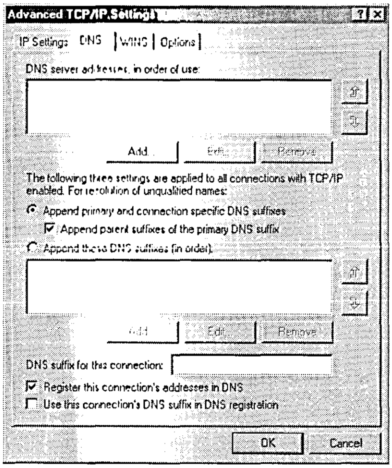
Under most circumstances, you want your NIC to respond to only one IP address. But sometimes you might need to have it respond to more than one IP address. Say that you are using your home computer to host several Web sites, and each site has been assigned its own IP address. Your home computer is connected to the Internet by a cable modem, and you want it to respond to requests for pages on each site. You need to address some DNS issues in order to have requests for those sites routed to your computer *(see the sidebar "Getting Your Own IP Address and Domain Name," page 395)*, but configuring multiple IP addresses enables your host to respond.

You can enable multiple IP addresses only if you select Use The Following IP Address in the Internet Protocol (TCP/IP) Properties dialog box. Then, in the Advanced TCP/IP Settings dialog box (see Figure 24-3), click the IP Settings tab. Click the Add button under the IP Addresses box, and enter each IP address. That's all there is to it.

You can also add secondary default gateway addresses (network routers). These addresses are used only if the primary default gateway is unavailable. Click Add to add a new gateway address. You also need to enter a metric value, which indicates the number of routers between your computer and the gateway. If the gateway is on your network, use a metric value of 1. TCP/IP uses this metric to determine which secondary gateway to try; it selects gateways with lower metric values first.

DNS Tab

To identify DNS servers, click Add and enter their IP addresses on the DNS tab of the Advanced TCP/IP Settings dialog box. TCP/IP uses them in the order they appear in this list. You can change their order using the up and down arrows to the right of the list. See Figure 24-4.



DNS server addresses, in order of use:

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

DNS suffix for this connection:

☑ Register this connection's addresses in DNS

☐ Use this connection's DNS suffix in DNS registration

Figure 24-4
On the DNS tab, you can set up more than two DNS server addresses.

The rest of this tab is taken up with a number of confusing selections relating to suffixes. Here's the deal: frequently, you might request to connect to a computer simply by its name, without all the dot extensions. For example, you might use the name bennie when the FQDN is bennie.sales.operations.company.com. In this case, .sales.operations.company.com is the suffix. Windows 2000 can resolve names without suffixes, essentially by trying different ones that it knows about until it finds one that works. You can tell Windows how you want it to go about trying different suffixes. You can use a combination of the primary DNS suffix defined for your computer and a suffix defined for this particular network connection. Or you can simply create a list of suffixes you want used.

If you use the primary and connection-specific suffixes, you can also select Append Parent Suffixes Of The Primary DNS Suffix. This selection sequentially strips off parts of the primary suffix. If this setting was selected in the preceding example, TCP/IP would first try to find bennie.sales.operations.company.com, then bennie.operations.company.com, and then bennie.company.com.

Your primary DNS suffix is the same for all network connections. The suffix might be configured by your DHCP server. (You'll find the setting in Scope Options | option 015 | DNS Domain Name on the server.) To set the primary DNS suffix manually on your computer:

1. Open System in Control Panel.
2. On the Network Identification tab, click Properties, and then click More.
3. Under Primary DNS Suffix Of This Computer, type the DNS suffix you want to use.
4. If you regularly change domains and want to use whichever domain is current as your DNS suffix, select Change Primary DNS Suffix When Domain Membership Changes.

You add a suffix specific to the network connection you have selected by entering it in the DNS Suffix For This Connection text box on the DNS tab of the Advanced TCP/IP Settings dialog box. You might want to do this if you frequently need to reach a second network from this connection or if you connect to multiple networks, each with a different domain name.

If you select Append These DNS Suffixes (In Order), the primary and connection-specific suffixes are ignored. In this case, you add your own list of suffixes, using the Add button under the text box. You should choose this option if you regularly connect to more than two networks and you would like to take advantage of this shortcut addressing method.

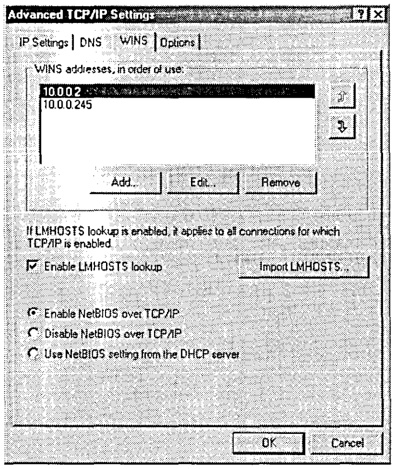
The last two check boxes on the DNS tab relate to how your computer registers its name with the DNS server. If you want your computer to attempt to register with its DNS server, select Register This Connection's Addresses In DNS. This option uses your computer's name when registering its address. If you also select Use This Connection's DNS Suffix In DNS Registration, the connection-specific suffix is added to the computer name in the DNS entry.

WINS Tab

Windows 2000 does not use a WINS server by default; you must configure it on the WINS tab of the Advanced TCP/IP Settings dialog box. WINS is used primarily to resolve NetBIOS names to IP addresses. In theory, if you have a pure Windows 2000 network, you should not need WINS because Windows 2000 uses TCP/IP by default. In reality, you probably need WINS, and you should select Enable NetBIOS Over TCP/IP on this tab.

Using a WINS server can enhance your network performance. By default, Windows 2000 broadcasts a name resolution request whenever it needs to resolve a NetBIOS name. This mode of NetBIOS operation is called *B-node broadcast*. If the broadcast request fails, Windows 2000 consults the local Lmhosts file if you select Enable LMHOSTS Lookup. With a WINS server configured, Windows 2000 requests name resolution from the WINS server before broadcasting a request. This mode of operation is called *H-node*. Consulting the WINS server before attempting a network broadcast reduces the load on your network.

If you have a WINS server on your network, click Add and enter its address. (See Figure 24-5.) DHCP can also be configured to supply the WINS server address automatically.



WINS addresses, in order of use:

10.0.0.2
10.0.0.245

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

● Enable NetBIOS over TCP/IP
○ Disable NetBIOS over TCP/IP
○ Use NetBIOS setting from the DHCP server

Figure 24-5
Use the WINS tab to specify servers for resolving NetBIOS names.

Of the three options at the bottom of this tab, you should select Disable NetBIOS Over TCP/IP only if you are using no computers or services that require NetBIOS, which is unlikely. Again, you can configure your DHCP server to supply NetBIOS settings, in which case you should select Use NetBIOS Setting From The DHCP Server. (Because DHCP is a Windows 2000 Server feature, we don't cover its configuration in this book.)

Note

NetBIOS configuration contains a Description field used to identify computers in a list of network hosts. In earlier versions of Windows, this field was easy to access through standard network configuration dialog boxes. Windows 2000 hides this field, however. Here's how to get to it:

1. Right-click My Computer and choose Manage. The Computer Management console opens.
2. In the Computer Management console, right-click Computer Management (Local) and choose Properties.
3. Click Network Identification. The Description text box on this tab is the NetBIOS description.

Note that this Network Identification tab is different from the Network Identification tab that you get by selecting Properties after right-clicking My Computer.

Options Tab

The Options tab contains settings for network security. *We discuss these options in Chapter 28, "Managing Incoming Connections."*

Setting Your Routing Options

The primary tool for setting routing options is the Route command (discussed in the following section). You can, however, set some options using the Windows 2000 interface.

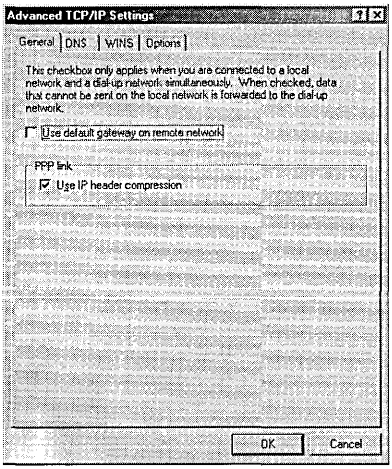
If you have a dial-up networking (DUN) connection, Windows configures the IP address of that connection as the default route. That is fine unless you also have a fast, direct connection to the Internet. For example, if you have a cable modem connection to your ISP, but you also connect by modem to a client's office, you don't want TCP/IP to use the slow dial-up connection as the default gateway for Internet access. Following are the first two lines in a routing table for such a configuration:

```
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.0.0.231      10.0.0.231       1
          0.0.0.0          0.0.0.0      137.107.1.1   131.107.1.240       2
```

In this case, two default gateways are defined. Note that the second line is for the cable modem connection and its metric has been incremented to 2, making it the second-choice gateway. This is not what you want. You can correct this by opening the Advanced TCP/IP Settings dialog box for the DUN connection and clearing Use Default Gateway On Remote Network on the General tab. (See Figure 24-6.) Clearing this option changes the first entry from a gateway to a route to the remote network and sets the metric for the cable modem connection gateway back to 1. Now the first two lines in the routing table look like this:

```
Network Destination          Netmask           Gateway        Interface  Metric
          0.0.0.0            0.0.0.0       137.107.1.1    131.107.1.240       1
         10.0.0.0          255.0.0.0        10.0.0.231       10.0.0.231       1
```

The second line now routes only data packets for the remote DUN network (10.0.0.0, in this case) through the DUN connection.



This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

□ Use default gateway on remote network

PPP link

☑ Use IP header compression

Figure 24-6
You should clear default routing for a dial-up networking connection.

Route Command

You maintain your routing tables by using the Route command in a Command Prompt window. The format of the Route command is as follows:

```
route [-f] [-p] [command [destination] [mask subnetmask] [gateway] [metric costmetric]]
```

where -F clears the routing tables of all gateway entries and -P makes an added route persistent (that is, permanent instead of going away after a reboot) or prints only persistent routes. Persistent routes are stored in the Windows registry and are loaded into the cached routing table each time your computer boots.

The available *command* values are Print (displays the routing table), Add (add a route), Delete (delete a route), and Change (change an existing route). *Destination, subnetmask,* and *gateway* are the IP addresses for these items. *Destination* can be a computer, subnet, network, or gateway. *Gateway* is the router to use to get to the destination. As discussed previously, the gateway might be the host computer, a software router server, or a hardware router. Metric is a measure of the cost of using this route. Usually, a metric of 1 is used unless you know that this route should not be attempted before another, in which case you should use a *costmetric* value greater than the one for the preferred route.

You will need to use the Route command if your network configuration is different from the scenarios Windows 2000 expects. In the preceding example, the local network ID was different from the network ID at the other end of the dial-up line. What happens if they are subnets on the same network? Say that your local network uses a network ID 10.0.1 and the remote network uses network ID 10.0.2. Both routing tables in the preceding example will try to send all packets to network 10.X.X across the DUN connection, including packets to the local network. You would need to add lines to the routing table as shown here:

```
Network Destination        Netmask          Gateway       Interface  Metric
         10.0.1.0     255.255.255.0      10.0.1.125      10.0.1.125       1
         10.0.2.0     255.255.255.0      10.0.2.231      10.0.2.231       1
```

In this example, your computer IP address is 10.0.1.125 and the remote connection has IP address 10.0.2.231. All data packets destined for computers on your local 10.0.1 subnet will be routed through your local connection (your network interface card), and all packets destined for computers on the remote 10.0.2 subnet will be routed through the DUN connection. The command to add the first route is the following:

```
route -p add 10.0.1.0 mask 255.255.255.0 10.0.1.125 metric 1
```

Use the -P switch to make the route persistent. When you manually add routes, they show up under Persistent Routes in the output from the Route Print command.

RIP Listening

Windows 2000 Professional has a service that allows its routing table to be dynamically updated: Routing Information Protocol (RIP) Listening. Routers use RIP to send route information to other routers. The RIP Listening (also called Silent RIP) service listens for these RIP messages and dynamically updates the routing table on your system. Dynamically updated routes have a predefined life span for which they are considered valid. This means that they must be refreshed periodically, reducing the chance that they become out of date. Static routes are valid forever.

RIP Listening is not installed by default in Windows 2000 Professional. To install it:

1. Open Add/Remove Programs.
2. Click Add/Remove Windows Components.
3. In the Components list, click Networking Services to highlight the line without selecting its check box, and then click Details.
4. Select the RIP Listener check box and then click OK.
5. Click Next and follow the instructions in the wizard.

If your computer is on a network with routers using RIP, RIP Listening can be useful for keeping routes up to date. If your computer is on a small network, or if the routers to which it is connected do not use RIP, you should not install this service.

Working with Several IP Configurations

Some people use several network configurations on the same computer, usually a laptop. For example, you might connect to your office LAN, a client's LAN, and a home LAN. Each network connection has different configuration items such as host IP address, DNS settings, DHCP settings, and so on. You want your computer to have a network connection defined for each location so that you don't have to reconfigure the computer each time you connect to a new network. Unfortunately, Windows 2000 does not allow for more than one Local Area Connection to be defined for any network interface card. (Conversely, you can define as many dial-up connections as you want. So if you have more than one ISP that you connect to by dial-up lines, you don't have anything to worry about.)

All is not lost. Third-party tools can alleviate some of this burden. Symantec Mobile Essentials (*www.symantec.com*) and Netswitcher (*www.netswitcher.com*) can keep track of multiple LAN configurations and let you easily switch between them.

Using Tools for Network Troubleshooting

Windows 2000 provides many tools that, along with a reasoned troubleshooting method, can help you track down most network problems. As you use these tools to solve problems, consider the following suggestions:

- Clearly identify what works and what does not.
- Make only one change at a time.
- Start at the lowest network level and work up. Many problems lie in the physical layer (cables). The list of tools below are in bottom-up order of use. Start with the first and move up until you isolate the problem.

All the tools listed in the following sections are command-line utilities that run from a command prompt. Because they're all stored in the %SystemRoot%\System32 folder, which is included in the Path environment variable, you don't need to specify the path when you launch these programs. You can find more information about each tool, including complete syntax and additional examples, in online help.

Ipconfig

Ipconfig displays the current TCP/IP configuration parameters. Use the /All switch to print a complete list and then verify that all parameters are set correctly.

Ping

Ping tests low-level connectivity by sending an echo request to a remote computer. One of the useful features of Ping is that it can accept a remote host name or IP address. Thus, if you successfully ping a remote computer using its IP address but a ping using its host name fails, you can assume that you have a problem with name resolution. If a ping to an IP address fails, your problem is either a physical problem or a routing problem. For example, if you were to try to ping the www server at Microsoft, you would see something like this.

```
C:\>ping www.microsoft.com
Pinging microsoft.com [207.46.131.30] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

With a known working remote host, this result would indicate that you were not making a connection all the way to the desired host. However, Microsoft (like many large organizations) has set up its servers so that they don't respond to Ping. With this configuration, the server is less vulnerable to denial-of-service (DoS) attacks. Note that Ping was able to resolve the name to an IP address.

You can ping your own computer using the loopback route. Use either *ping loopback* or *ping 127.0.0.1*.

Arp

When data packets are sent out of your computer, they are directed to either another computer or to a router. The process that adds the destination address to the data packets is Address Resolution Protocol (ARP). ARP maintains the routing cache used to resolve addresses. The Arp utility is used to view, add, or delete entries in the ARP cache. Arp can tell you where your computer thinks it should be sending packets.

Tracert

Tracert traces the route that a packet takes to a destination. If, for example, a ping to an IP address fails, you can run a trace to that address and see where it is failing. A lot of routing is happening on the Internet, and if one point breaks down, you will have trouble. In most cases, the problem is near one end or the other. Switching within an ISP sometimes goes awry, and Tracert is useful in finding out where the problem lies. We can use as an example the www server at Microsoft. Microsoft's public server does not answer pings, giving the appearance of a routing problem. A trace to *www.microsoft.com* might look like this:

```
C:\>tracert www.microsoft.com
Tracing route to microsoft.com [207.46.131.28]
over a maximum of 30 hops:
  1    10 ms  <10 ms   10 ms  209.178.125.1
  2    21 ms   20 ms   20 ms  s5-5-i4-br01-pas.neteng.itd.earthlink.net [207.2
17.50.25]
  3    20 ms   20 ms   10 ms  f5-1-0-cr01-pas.neteng.itd.earthlink.net [207.21
7.2.33]
  4    20 ms   20 ms   20 ms  f8-1-0-br03-pas.neteng.itd.earthlink.net [207.21
7.1.67]
  5    20 ms   20 ms   10 ms  p5-3.lsanca1-cr5.bbnplanet.net [4.24.57.13]
  6    20 ms   20 ms   20 ms  p6-0.lsanca1-ba1.bbnplanet.net [4.24.4.25]
  7    20 ms   20 ms   20 ms  p7-0.lsanca1-br1.bbnplanet.net [4.24.4.2]
  8     *      51 ms   30 ms  p4-0.evrtwa1-ba1.bbnplanet.net [4.0.6.38]
  9    50 ms   40 ms   50 ms  p1-0.evrtwa1-cr1.bbnplanet.net [4.24.5.102]
 10    50 ms   40 ms   60 ms  p0-0.mscanyonpark.bbnplanet.net [4.24.125.66]
 11    40 ms   50 ms   40 ms  icpmscomc7502-a1-00-1.cp.msft.net [207.46.129.13
2]
 12     *       *       *     Request timed out.
 13     *       *       *     Request timed out.
```

The trace by default goes on for 30 steps, but we truncated the last 17 timeouts for this list. If this were a real example, we would know that a problem existed somewhere around the router listed in line 11.

Route

The Route command is discussed in detail earlier in this chapter. You can also use the Route command for troubleshooting by creating alternate routes to a particular destination that you are having trouble reaching.

Netstat

The Netstat command displays details on current TCP/IP port connections. You can use command-line switches to view different sets of details. With no switch, Netstat output looks like this:

```
C:\>netstat
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    Biscayne:1042          EVERGLADES:netbios-ssn ESTABLISHED
  TCP    Biscayne:1058          REDWOOD:netbios-ssn    ESTABLISHED
  TCP    Biscayne:1101          YOSEMITE:3886          ESTABLISHED
```

Nbtstat

The Nbtstat command provides similar information to Netstat, but for NetBIOS names. Use Nbtstat to view the resolution tables for NetBIOS names. Use the -R switch to remove the cache and reload it from the Lmhosts file.

Nslookup

The Nslookup command looks up an IP address for a given computer name from the DNS server that your computer is configured to use. This command is useful for troubleshooting DNS problems. When you start Nslookup, it displays the host name and IP address of the DNS server and then provides its own command prompt. At this prompt, enter the name of a host and Nslookup returns its IP address.

Netsh

Netsh is a Windows 2000 utility that centralizes the control and monitoring of certain network services. Netsh is a command-line shell interface to a number of helper programs that control the configuration of specific network components. Commands entered at the shell are sent to the appropriate helper for implementation.

Netsh allows you to display or modify the configuration of another currently running computer on your network. It also provides a dump command, which creates a script to match the current settings. The script can be saved and run in batch mode or on a remote computer.

Although Netsh is a sophisticated utility, its main use is on a computer running Windows 2000 Server. Windows 2000 Professional does not run the services, such as RRAS (Routing and Remote Access Service), on which Netsh relies.

Setting Advanced Options

The Network And Dial-Up Connections window contains an Advanced menu with items for configuring a variety of network connection settings. (See Figure 24-7.) Some of these are shortcuts, so it is worth spending some time learning the ins and outs of these items.

Network Identification

Selecting the Network Identification command from the Advanced menu brings up the Network Identification tab in the System Properties dialog box. From here, you can change your computer's name or the domain or workgroup to which it is connected. You can also run the Network Identification Wizard if you need to reset your computer's LAN connection.

Advanced Settings

The order in which your computer attempts to connect to network services and protocols determines how quickly and efficiently the network runs. The computer on which Figure 24-8 was captured, for example, is configured to first try file and print sharing using NetBEUI and then TCP/IP. On a network using TCP/IP, this means that each file and print sharing attempt would first make an unsuccessful NetBEUI attempt before it used TCP/IP.

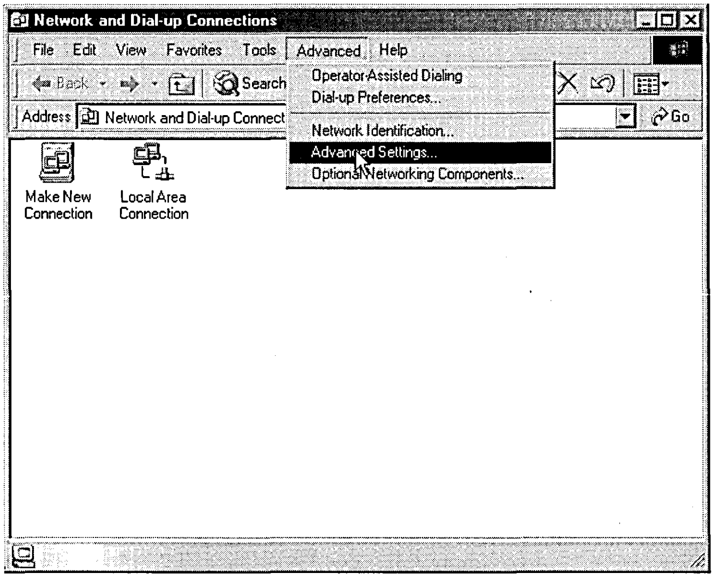
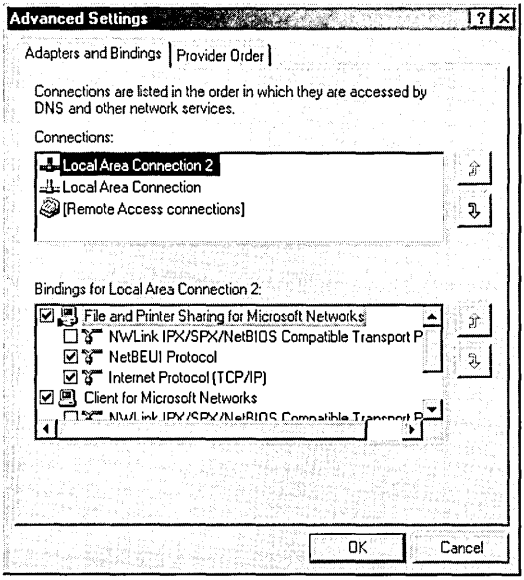

Network and Dial-up Connections
File
Edit
View
Favorites
Tools
Advanced
Help
Back
Search
Address
Network and Dial-up Connect
Go
Operator-Assisted Dialing
Dial-up Preferences...
Network Identification...
Advanced Settings...
Optional Networking Components...
Make New Connection
Local Area Connection

Figure 24-7
Network And Dial-Up Connections contains a menu that you won't see in most folders: Advanced.

To change the order of these protocols, open the Network And Dial-Up Connections folder and choose Advanced Settings from the Advanced menu. On the Adapters And Bindings tab of the Advanced Settings dialog box (shown in Figure 24-8), select the connection for which you want to make the change. Then, in the Bindings box, select one of the protocols or services that you want to reorder and move it using the arrow buttons on the right.

You can also unbind a protocol from a service by clearing the check box next to the protocol under the service. (For example, notice the unbound NWLink protocol in the figure.)



Connections are listed in the order in which they are accessed by DNS and other network services.

Connections:

- Local Area Connection 2
- Local Area Connection
- [Remote Access connections]

Bindings for Local Area Connection 2:

- ☑ File and Printer Sharing for Microsoft Networks
  - □ NWLink IPX/SPX/NetBIOS Compatible Transport P
  - ☑ NetBEUI Protocol
  - ☑ Internet Protocol (TCP/IP)
- ☑ Client for Microsoft Networks
  - □ NWLink IPX/SPX/NetBIOS Compatible Transport P

Figure 24-8
Set the adapter and bindings order in the Advanced Settings dialog box.

Optional Networking Components

Select Optional Networking Components from the Advanced menu, and the Windows Optional Networking Components Wizard opens right away. From here, you can add or remove Management And Monitoring Tools, Networking Services (such as RIP Listen), and Other Network File And Print Services.

Setting Up Non-TCP/IP Connections

Although Windows 2000 uses TCP/IP by default, you are not restricted to this one protocol. You can configure any network adapter to use other protocols, including NetBEUI (typically used on small Windows-based networks), IPX (for connecting with Novell NetWare networks), or AppleTalk (for connecting with an AppleTalk File Server) protocols. Windows 2000 allows you to use more than one protocol on any connection, but the more protocols you configure, the slower your overall performance will be.

Note Most of the Windows 2000 AppleTalk functionality is available only on Windows 2000 Server. This includes File Server for Macintosh and Print Server for Macintosh. Windows 2000 Server can also be an AppleTalk router.

To install a new protocol:

1. Open the Network And Dial-Up Connections folder.
2. Right-click the connection for which you want to add a protocol and select Properties.
3. Click Install, select Protocol, and click Add.
4. Select the desired protocol from the list and click OK.

After a protocol is installed for one adapter, it is available to all other adapters or dial-up connections. To configure a protocol:

1. Open the Network And Dial-Up Connections folder.
2. Right-click the connection for which you want to add a protocol and select Properties.
3. Select the desired protocol and click Properties. If the Properties button is not highlighted, there are no items for you to configure.

Part 7

Using the Internet

Chapter 25
Making Internet Connections 415

Chapter 26
Internet Explorer: Beyond Browsing 435

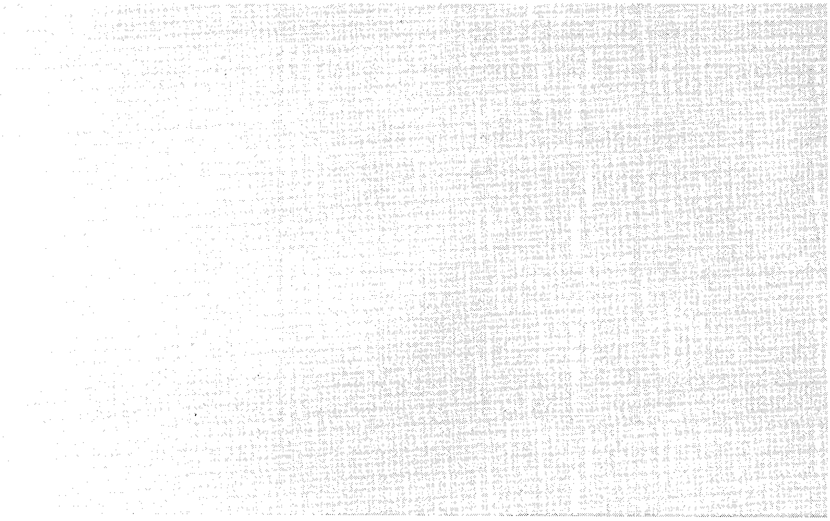
Chapter 27
Managing a Web Server 463

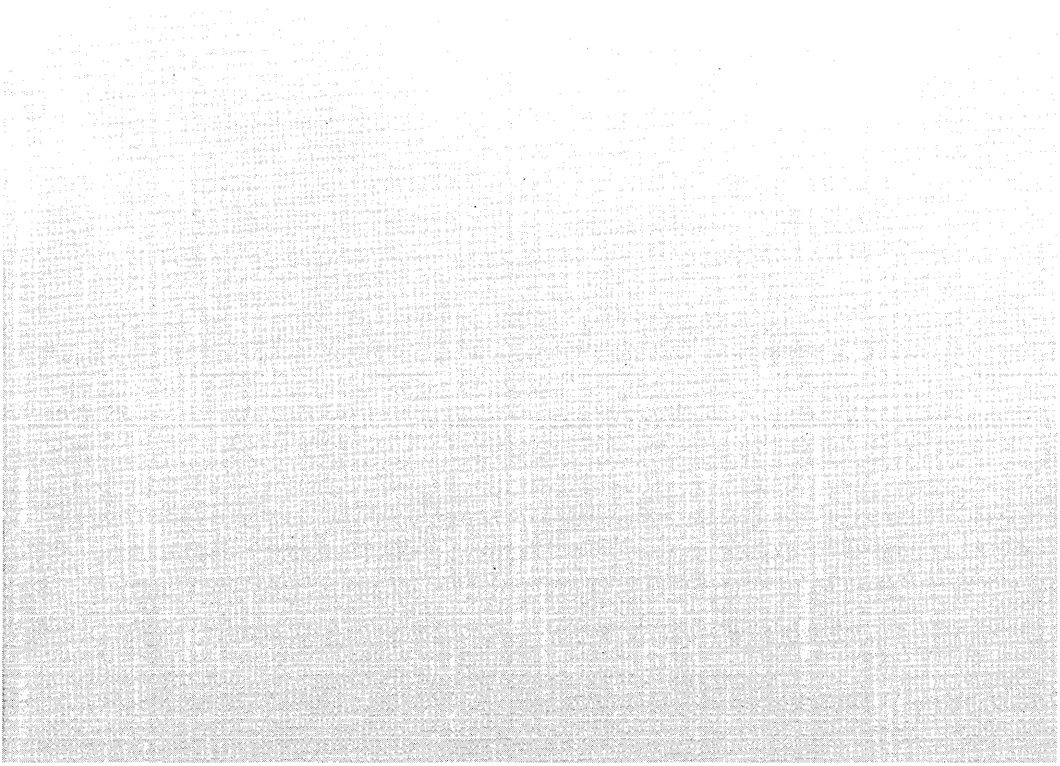
Chapter 28
Managing Incoming Connections 485

Chapter 29
Communicating Over the Internet 501

Chapter 30
Using Telnet 515

Chapter 31
Using the FTP Clients 525





Chapter 25

Making Internet Connections

In This Chapter

Creating Dial-Up Connections 416
Connecting to the Internet Through a LAN 418
Using Cable and DSL Connections 421
Configuring TCP/IP 422
Sharing an Internet Connection 423
Securing Your Internet Connection 428

With the proliferation of the Internet and the various means of accessing it, network connections have become increasingly diverse. In this chapter, we discuss ways of connecting your computer to the Internet. Connections to the Internet or to a local area network (LAN) can be made either as direct physical connections (for example, a cable modem or a network interface card) or dial-up connections (for example, an analog modem).

Variety is added to the mix by connections to the Internet through a LAN and connections to remote LANs through the Internet. The latter connections, called virtual private networks (VPNs), are introduced in this chapter. *(For more on VPNs, see Chapter 28, "Managing Incoming Connections.")* Figure 25-1 illustrates the many ways your computer can connect to the Internet and other networks.

Microsoft Windows 2000 groups all Internet connections into one of two categories: dial-up connections or network connections.

- Dial-up connections use an analog voice/fax modem or an ISDN (Integrated Services Digital Network) modem. Dial-up connections typically require explicit acts of connecting and disconnecting each time you want to go online or offline.

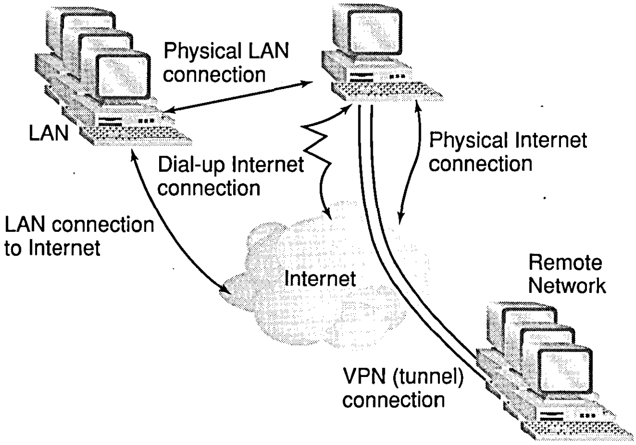

Physical LAN connection
LAN
Dial-up Internet connection
Physical Internet connection
LAN connection to Internet
Internet
Remote Network
VPN (tunnel) connection

Figure 25-1
You can connect a computer to the Internet using a variety of possible network connections.

- Network connections have more in common with the local area network in your office or home. Cable modems and DSL (digital subscriber line) connections use network connections. Typical network connections remain online all the time.

You control all your Internet connections from the Network And Dial-Up Connections folder. This folder contains an icon for each connection you create and one that starts the Network Connection Wizard. To open the Network And Dial-Up Connections folder, either right-click My Network Places and choose Properties or choose Start | Settings | Network And Dial-Up Connections. *For more information about this folder, see Chapter 22, "Making Network Connections."*

The next section deals with creating your dial-up connections. Following that, we focus on network connections to the Internet.

Creating Dial-Up Connections

In Windows 2000, making an Internet connection is easy with the Internet Connection Wizard, which you can launch in either of these ways:

- In the Network And Dial-Up Connections folder, open Make New Connection to start the Network Connection Wizard. Click Next, select Dial-Up To The Internet, and click Next again.
- Open the Internet Options dialog box. (Choose Control Panel | Internet Options; right-click the desktop icon for Microsoft Internet Explorer and choose Properties; or, in Internet Explorer, choose Tools | Internet Options.) On the Connections tab, click Setup.

The Internet Connection Wizard offers three options for setting up a connection:

- Sign up for a new dial-up account with an Internet service provider (ISP) in your area, using the Microsoft Internet Referral Service. Use this option if you do not currently have an account with an ISP and want to select one from Microsoft's list of ISPs in your area. Be aware that this list might not contain all the ISPs offering service in your area. You must have a modem connected to use this option.
- Set up an existing dial-up account on this computer. Use this option if you have established an account with an ISP. The wizard attempts to use the Microsoft Internet Referral Service to list your ISP. If your ISP is not on the list, you can enter the configuration information manually in the wizard. You must have a modem connected to use this option.
- Set up a connection to the Internet manually, or set up a connection through your LAN. Use this option to avoid the Microsoft Internet Referral Service and enter your configuration manually in the wizard. Or use this option if you connect to the Internet through a LAN. *See "Connecting to the Internet Through a LAN," page 418.*

In general, you will find that manually entering your configuration information is the approach least fraught with frustration. When setting up a dial-up connection, you need to provide the phone number of the ISP, your account name, and, optionally, your password. (If you don't enter your password here, you must enter it when you attempt to connect.) The wizard makes the selections used by virtually all ISPs. If you have different connection requirements—for example, you use a static IP address, a logon script, or SLIP—click Advanced on the wizard page on which you enter the ISP's phone number.

After a dial-up connection is created, you have several options for opening it. You can open its icon in the Network And Dial-Up Connections folder. You can also create shortcuts to open and close connections, as described in the next section.

But why should you have to manually open an Internet connection? Windows 2000 strives to merge your local computer and the Internet into a seamless whole. If you want to access a file on your hard disk, you simply open a Windows Explorer window and open folders until you get to the file you want. Why should you have to do anything more, such as establishing a connection, to access a Web resource? On the Connections tab of the Internet Options dialog box are three options that control whether and how a connection is automatically established when you try to access a resource on the Internet:

- **Never Dial A Connection.** If this option is selected, you will always have to manually open an Internet connection whenever you want to access any Internet resource. If you try to access a resource on the Internet and no connection is established, you receive a message telling you that what you want is not available.

- **Dial Whenever A Network Connection Is Not Present.** If this option is selected and you try to access an Internet resource, a connection through a LAN is attempted first. If that connection is unsuccessful, your default dial-up connection is opened. If you need to supply a password, Windows displays a dialog box in which you can do so.
- **Always Dial My Default Connection.** If this option is selected and you try to access an Internet resource, your default dial-up connection is opened. If you need to supply a password, Windows displays a dialog box in which you can do so.

Creating Shortcuts for Dial-Up Connections

If you choose to use manual connections, you might want to create desktop shortcuts to open and close individual dial-up connections. You can assign shortcut keys to make connecting and disconnecting even easier.

The easiest way to create a shortcut for opening a connection is to right-click the connection's icon in the Network And Dial-Up Connections folder and choose Create Shortcut. To disconnect, you can right-click the connection's icon in the taskbar status area or in the Network And Dial-Up Connections folder and choose Disconnect.

Here's another way to easily disconnect: use Rasphone.exe, the Dial-Up Networking application from Windows NT (also included in Windows 2000). You can create a shortcut to %SystemRoot%\System32\Rasphone.exe -v -h *"connectionname"* (where *connectionname* is the name of the dial-up connection).

Note Some people prefer the old Dial-Up Networking Monitor over Network And Dial-Up Connections for monitoring connection status. You can launch it by typing *rasphone -s* at a command prompt. For more information about Rasphone.exe, type *rasphone /?* at a command prompt.

Connecting to the Internet Through a LAN

You'll use a LAN connection to the Internet if your connection is through another computer on your network. In this case, your own computer doesn't have a direct connection to the Internet. The other computer could be running Internet Connection Sharing or a proxy server, for example.

To set up such a connection, use the Internet Connection Wizard. *(For details about launching the wizard, see "Creating Dial-Up Connections," earlier in this chapter.)* Select the third option on the first wizard page (Manual Setup). On the Setting Up Your Internet Connection page, select the second option, (LAN).

To complete the wizard, the only real choice you need to make is whether to use automatic configuration. Normally, it's best to let the connection automatically discover any proxy server. If you select Manual Proxy Server, the wizard asks you to enter the name of the proxy server. You are also given the chance to list IP addresses that should not use proxy. *For information about automatic configuration, see "Using an Automatic Configuration Script," page 421.*

Connecting to the Internet through a local area network requires a few special considerations. Most LANs are set up to use private addressing, so your computer will not have an Internet-unique IP address. *(For details about IP addresses, see Chapter 24, "TCP/IP Core Networking Guide.")* Your private network connects to the Internet through one computer on the network, which acts as the gateway for the rest of the network. This gateway computer must perform some kind of address juggling, translating the private address of your computer to a unique public address that can be used on the Internet. This juggling is usually part of a proxy service. Microsoft Proxy Server, a proxy server designed for Microsoft Windows NT Server and Microsoft Windows 2000 Server, provides a proxy service, among other things. Other Windows components can also provide proxy services. Because many corporate and small-business LANs use Proxy Server, we'll talk about it here; but because Proxy Server doesn't come with Windows 2000 Professional, we'll limit our discussion to only those details necessary to understand how to configure your computer to work with it when you are running Windows 2000 Professional.

Proxy Server is actually a combination of three services: Web Proxy, WinSock Proxy, and SOCKS Proxy. Web Proxy works with Web browsers. WinSock Proxy works with applications that use the Windows Sockets protocol, and SOCKS Proxy provides similar services for applications that use the SOCKS protocol. On a computer running Windows 2000 Professional, you will be most concerned with Web Proxy and WinSock Proxy.

Proxy Server also provides security features that protect your network from infiltration by outsiders. *For more information about security, see "Securing Your Internet Connection," page 428; and Chapter 28, "Managing Incoming Connections."*

Note If you don't use Proxy Server (or a comparable program) on your network, you can use Internet Connection Sharing, a built-in feature of Windows 2000 that lets you keep your network private and allows all computers to safely connect to the Internet. *See "Sharing an Internet Connection," page 423.*

Using WinSock Proxy Client

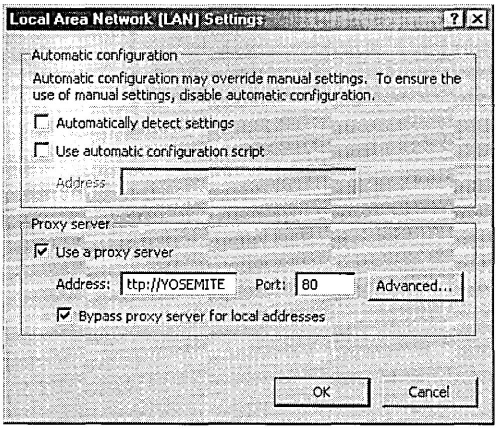
Networks that use Proxy Server have a WinSock Proxy Client (WSP Client) that runs on each client computer. WSP Client is required for applications that use Windows Sockets, such as Microsoft Outlook Express and RealPlayer.

To install WSP Client, run \\proxyserver\Mspclnt\Setup.exe, where *proxyserver* is the host name of the computer running Proxy Server. You can then go to WSP Client in Control Panel, where you can configure your computer to use or not use WSP Client and you can enter the WinSock Proxy server name.

Connecting to the Web Proxy

You need to tell your Web browser where the Web Proxy server is located. To do this for Internet Explorer:

1. Open the Internet Options dialog box (Tools | Internet Options or Control Panel | Internet Options), and click the Connections tab.
2. Be sure that Never Dial A Connection is selected, and then click LAN Settings.
3. Under Proxy Server, select Use A Proxy Server and then type the name of your proxy server in the Address text box. Use the form *http://servername*. In many cases, you also need to supply a port number. Enter 80, the TCP port designated for HTTP services. *(For more information about ports, see "Securing Your Internet Connection," page 428.)* You should also select Bypass Proxy Server For Local Addresses to prevent Internet Explorer from using the proxy server to reach other computers on your local network. See Figure 25-2.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server

Address: ttp://YOSEMITE Port: 80

☑ Bypass proxy server for local addresses

Figure 25-2
In this dialog box, you configure Internet Explorer to use a proxy server.

Note You can connect to a Web Proxy server without running WSP Client on your computer. If you are not running WSP Client, you must use Web Proxy.

Using or Not Using Web Proxy

When you configure your Web browser to not use Web Proxy (by clearing Use A Proxy Server in the dialog box shown in Figure 25-2), your computer defaults to using WSP Client and connects to the Internet through WinSock Proxy. What's the difference? Usually, not much. But each proxy service supports a slightly different set of protocols and features; you might find that one doesn't support the protocol or feature you need or want. For example, Web Proxy includes a caching feature that can speed your Internet access. Also, many applications that use the Internet, such as Outlook Express, RealPlayer, and Norton LiveUpdate, use the Internet connection settings in your Internet browser by default. If one of these programs requires a protocol or feature not supported by one of the two proxy services (Web Proxy or WinSock Proxy), you can configure your browser to use the other service.

It is beyond the scope of this book to list all the protocols and features used by these proxy services or the requirements of popular Internet applications. It's a simple matter to set or clear the use of Web Proxy if something doesn't work. In our experience, however, Web Proxy seems to be more limiting than WinSock Proxy—that is, clearing Use A Proxy Server usually works better.

Using an Automatic Configuration Script

If your computer is on a network with a Windows NT or Windows 2000 server running Proxy Server, you might have the option of using a configuration script to configure the proxy settings of your browser (Internet Explorer or Netscape Navigator). The system administrator can create a script to handle proxy interactions between proxy clients and the proxy server. The benefits of using a configuration script are easier system management (for the client and the system administrator) and improved browser performance. *For details about automatic configuration, see "Customizing Internet Explorer," page 446.*

Using Cable and DSL Connections

Cable (which transmits Internet data over cable television systems) and a variety of DSL connections (which use telephone wiring) provide a relatively inexpensive way for small businesses and home users to gain broadband access to the Internet. A great introduction to DSL is found at *www.whatis.com/dsl.htm.*

Cable and DSL connections differ from dial-up connections in one important respect. Most cable connections use a statically assigned IP address. When you get a cable connection, one of the configuration parameters your ISP provides is your IP address. In contrast, most dial-up connections use dynamically assigned IP addresses. In this case, your ISP acts as a DHCP server by assigning your computer a new IP address every time you call. DSL connections can work either way, depending on how the

ISP has configured their system. *(For information about DHCP [Dynamic Host Configuration Protocol], see "DHCP and APIPA," page 396.)*

Cable and most DSL connections are "always on." This type of connection is often called a *persistent* connection. Some ISPs configure their DSL lines to "dial up" whenever you establish a connection, mimicking the activity of an analog modem. If you use one of these dial-up DSL connections, your ISP provides a dial-up application. When an ISP uses dial-up connections for DSL, the ISP also provides temporary IP addresses via a DHCP server.

Note Thinking about getting DSL? You might have more options than you think. Check *2wire.com/dsllookup/finddsl.asp* to search for companies offering DSL in your area. This site also calculates the distance from your location to the phone provider's central office (CO), an important factor in whether DSL will work for you.

When you have a persistent connection with a static IP address, you open yourself to security problems. Hackers scan the Internet for open ports on IP addresses. When they find an open port, they attach a password breaker to the port to open it. If you have a different IP address each time you connect to the Internet, or your connection is established only for short periods, hackers don't have as much opportunity to break in. If you have a persistent connection and a static IP address, you should invest in a firewall. *For more information, see "Securing Your Internet Connection," page 428.*

Note ISPs sometimes advertise their DSL service with hyped-up language, leaving important details for the fine print. You see this most often with data rates. Fast rates are printed in bold, fluorescent colors. But check the rest of the advertisement for *guaranteed* data rates. Usually, these are much lower, if any guarantees are given at all. When you compare different services, be sure that you know whether you are comparing maximum or guaranteed rates.

Configuring TCP/IP

When configuring TCP/IP for your LAN connection, the main issue to be concerned with is whether you use a static IP address or a dynamically assigned IP address from a DHCP server. You configure your IP address on the General tab of the Internet Protocol (TCP/IP) Properties dialog box for the connection. Select Obtain An IP Address Automatically if you use a dynamically assigned IP address. Select Use The Following IP Address if you use a static IP address. Then fill in the IP Address, Subnet Mask, and Default Gateway fields. *For more information, see "Setting Connection-Specific TCP/IP Properties," page 398.*

Sharing an Internet Connection

Windows 2000 provides a mechanism for easily and securely sharing a single Internet connection on a small home or office network without using Proxy Server. Internet Connection Sharing (ICS) provides Windows 2000 Professional users with a simple way to implement many of the benefits of Proxy Server. ICS provides scaled-back versions of the IP address translation and name resolution services provided by Proxy Server and DHCP. ICS does not provide full firewall protection.

To use ICS, you must observe some restrictions:

- All the computers connecting through ICS must run TCP/IP.
- The computers can't be configured for static IP addresses; they must be set up to obtain an IP address automatically.
- There cannot be a Windows 2000 Server domain controller, DHCP server, or DNS server running on the network.

The presence of a DHCP or DNS server or of Active Directory implies the existence of a server (either Windows 2000 Server or Windows NT Server) on your network. If you have a server, you should use the Network Address Translation (NAT) routing protocol to achieve Internet sharing. NAT is a Windows 2000 Server component that offers more configuration options than ICS (which offers, let's see, none). In addition, NAT supports the use of multiple public IP addresses, whereas ICS can use only one public IP address at a time. (The address can change each time you connect to the Internet, but you can't have more than one simultaneous connection.)

Note You can add a Windows 2000 Server domain controller to a network that already has ICS set up without interfering with ICS. However, in that case, you're probably better off using the additional capabilities of Windows 2000 Server to share an Internet connection.

Setting Up Your Network for a Shared Connection

To use ICS, you should have a network configuration like one of those shown in Figure 25-3. All the computers on the network must be configured to use TCP/IP as their network protocol. However, these computers can use any operating system that supports TCP/IP and DHCP. One of the computers must have a connection to the Internet, either through a network interface card (NIC) connected to a cable modem or DSL modem, or through an analog modem and dial-up connection. It also must be connected to the local network through a separate NIC. We call this the *gateway computer*. This discussion assumes that the gateway computer runs Windows 2000. Windows 98 Second Edition also supports ICS.

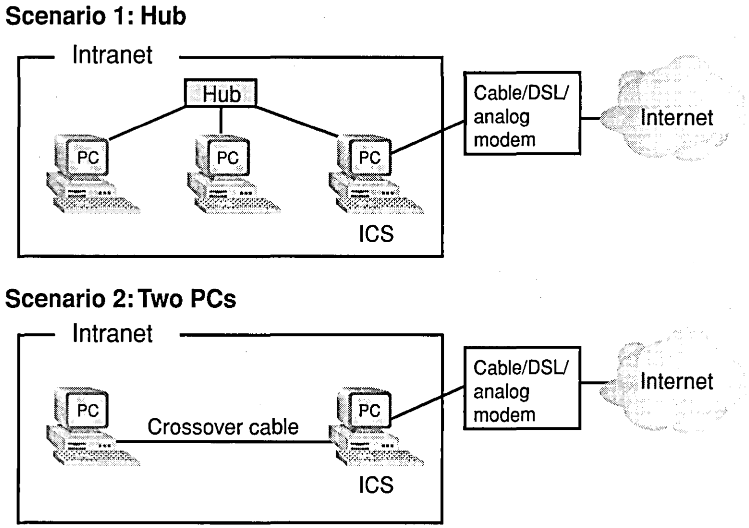


Figure 25-3
The network configuration for Internet Connection Sharing requires two NICs (or, for dial-up connections, one NIC and an analog modem) in the gateway computer.

Note If your computer has more than one NIC installed (for example, if you have one that connects to your LAN and one that connects to a cable modem), rename one (or both) of the connections in the Network And Dial-Up Connections folder so that you can readily differentiate them.

Using a Router Instead of ICS

Another way to configure your network for sharing a connection is to use a router to connect the rest of the network to the Internet, as shown in Figure 25-4. (A *router* is like an intelligent network hub. But instead of passing all packets to the rest of the network, as a hub does, a router keeps LAN traffic on the local subnet and routes nonlocal traffic to the Internet.) Inexpensive cable/DSL routers are available from Linksys (*www.linksys.com*) and other manufacturers. You configure the router using software that comes with it.

With ICS, whenever anyone on the network wants to use the Internet, the gateway computer must be turned on (although no one needs to be logged on). The router setup works well if you don't have a computer that's always on; any computer can access the Internet at any time, without depending on another computer to be running. Because routers send packets only to the intended destination port, they can increase network speed, which can be important with some multimedia and multiplayer gaming applications. Some routers offer additional security and options that aren't available with ICS. Nevertheless, ICS is powerful, easy to configure—and free.

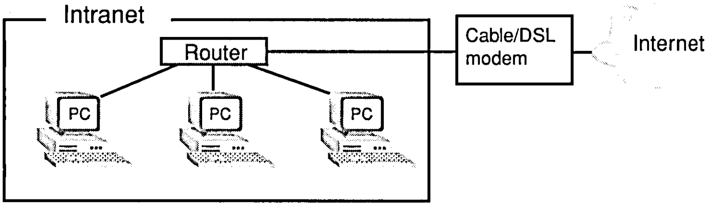


Figure 25-4
A router can provide an alternative method of sharing a high-speed Internet connection.

Configuring and Using ICS

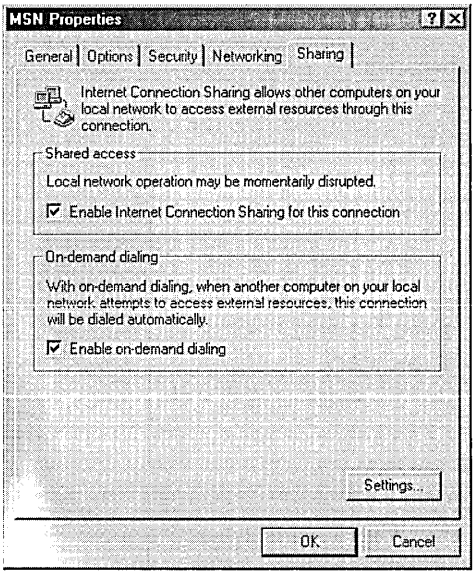
When you enable ICS on your gateway computer, ICS becomes the network's DHCP server and assigns network addresses to all the computers on your network. It assigns the address 192.168.0.1 to the gateway computer and then uses the range 192.168.0.2 to 192.168.0.254 for the rest of your network. The subnet mask for all computers is set to 255.255.255.0, and the default gateway address is set to 192.168.0.1, the address of your gateway computer. (To verify these settings, you can run Ipconfig.exe; *for details, see "Using Tools for Network Troubleshooting," page 406. DHCP servers, addresses, and masks are described in "Introduction to TCP/IP," page 387.)* You cannot change these defaults in ICS.

The secret of ICS's ability to share one IP address among several different computers is the use of ports. *For information about ports, see "Understanding TCP/IP Ports and Security," page 429.* For now, it is enough to think about an IP address as an airport and a port as an individual gate at that airport. When an application on one computer makes a call to an Internet address, it sends a data packet containing both the sending computer's IP address and the destination computer's IP address. Each address has a port number appended to it. That way, when the data packet gets to the destination "airport," it knows which "gate" to use. This combination of IP address and port number is called a *socket*. Likewise, when the destination computer sends back a data packet in response, it knows which "gate" to use at the original sending computer. When you use ICS, the data packets are intercepted on the way out and on the way back in. ICS intercepts the outgoing packet, notes where it came from, selects a currently unused port, appends that to *its own* public IP address, and replaces the sending computer's address with this socket. When the destination computer responds, the data packet is sent to the ICS computer at the assigned port. When ICS sees a data packet at that port, it forwards the packet on to the original sending computer. As a result, the destination computer sees only the address of the computer running ICS, not that of any of the computers running behind it. This hiding of computers behind the gateway provides security for them because no one on the Internet has direct access to them. The gateway computer needs additional protection. *See "Securing Your Internet Connection," page 428.*

Configuring the Gateway Computer

Enabling ICS on the gateway computer is extremely easy:

1. In the Network And Dial-Up Connections folder, right-click the Internet connection you want to share and choose Properties.
2. Click the Sharing tab and select Enable Internet Connection Sharing For This Connection.



Internet Connection Sharing allows other computers on your local network to access external resources through this connection.

Shared access

Local network operation may be momentarily disrupted.

☑ Enable Internet Connection Sharing for this connection

On-demand dialing

With on-demand dialing, when another computer on your local network attempts to access external resources, this connection will be dialed automatically.

☑ Enable on-demand dialing

3. If you are using a dial-up connection, select Enable On-Demand Dialing. (If you clear this check box, users at other computers can access the Internet only when you're already connected.)

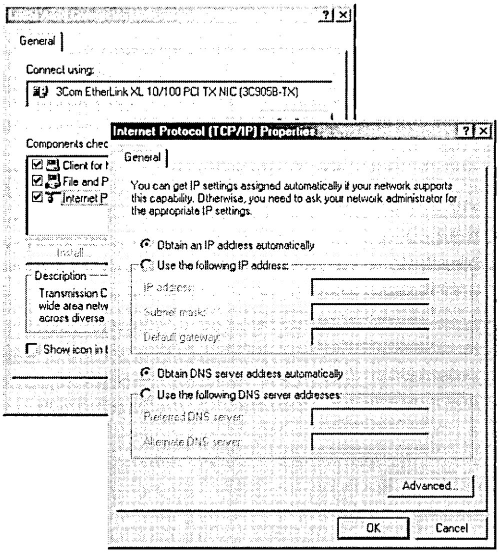
Note To enable sharing, you must be logged on as a member of the Administrators group.

Configuring the Client Computers

Because ICS operates as a DHCP server on your gateway computer, you must configure the other computers on your network to use DHCP to obtain an IP address. (This is the default configuration in Windows 2000.) To confirm the proper configuration of a Windows 2000 client:

1. In the Network And Dial-Up Connections folder, right-click the LAN connection and choose Properties.
2. Select Internet Protocol (TCP/IP) and click Properties.

3. Select Obtain An IP Address Automatically and Obtain DNS Server Address Automatically.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

For more information about TCP/IP configuration, see Chapter 24, "TCP/IP Core Networking Guide."

Note It's important to recognize that you do not need to set up an Internet connection on the client computers. Instead, they connect (indirectly) to the Internet through their LAN connection.

To configure Internet Explorer (and other Internet applications that rely on Internet Explorer's connection settings):

1. Open the Internet Options dialog box and click the Connections tab.
2. Select Never Dial A Connection and then click LAN Settings.
3. In the Local Area Network (LAN) Settings dialog box, clear all the check boxes.

Sharing a VPN Connection

Windows 2000 Professional also allows you to share a virtual private network (VPN) connection in the same way you share an Internet connection. *(For more information about VPNs, see Chapter 28, "Managing Incoming Connections.")* Because a shared VPN connection relies on ICS, the same restrictions apply. (All computers must use TCP /IP and must be configured to obtain an IP address automatically, and the network can't have a DHCP server or a DNS server set up.)

To share a VPN connection, right-click the VPN connection you want to share (in the Network And Dial-Up Connections folder) and choose Properties. Click the

Sharing tab and select Enable Internet Connection Sharing For This Connection. Then, from the For Local Network list, select the network to which you want to grant VPN access. If the VPN connection is active, you must disconnect and then reconnect to enable sharing.

Securing Your Internet Connection

When you connect to the Internet, you put yourself at risk. You can manage this risk if you understand its nature. Internet security is an enormously complicated topic with reams of material written about it. In this chapter, we restrict our focus by assuming that you use your Internet connection for outbound connections only. That is, you use Internet Explorer, Outlook Express, and other Internet applications so that you can connect to other computers on the Internet. You are not hosting a Web site or running an FTP server or in any other way allowing connections to be initiated by outside computers. *We discuss the security issues that arise when you allow others on the Internet to establish connections with your computer in Chapter 28, "Managing Incoming Connections."*

It's important to realize that to use the Internet—even to initiate outbound connections—you need two-way connectivity, which means that the bad guys have a potential avenue to get in whenever your computer is connected to the Internet. Unfortunately, unless you take some steps, a hacker can initiate a connection to your computer and compromise your privacy or damage your computer.

Some argue that the world has two categories of hackers. The Good Hackers ferret out and expose software security problems with benign, or even beneficial, intent. Their motivations tend to be curiosity combined with a desire for programming excellence. The Bad Hackers also ferret out and expose security problems, but with maleficent intent. Their desire is to steal and cause destruction. Whether or not this distinction has any meaning in the real world, hackers are out there, and they are interested in breaking into your computer.

What can hackers do? They can

- Retrieve files from your computer, including financial data and temporary Internet files showing secure information
- Place files on your computer, including viruses and Trojan horses (programs that run on your computer and aid the hacker in accessing your computer) in the form of e-mail attachments, ActiveX components, or Java scripts
- Monitor your Internet activity by observing the sites you visit and intercepting passwords, credit card numbers, and other sensitive information
- Disrupt your computer's functions with attacks called denial-of-service, which can overwhelm your computer and cause it to crash or slow to a screeching halt

Hackers can also use your computer to carry out attacks on other computers. By placing the code they want to use on your computer, they obfuscate their own location and make it difficult to track their attacks.

As you can see, security and privacy are tightly connected. A lack of security poses a threat to your privacy. When hackers gain access through security lapses to your private information, they can use your credit cards, gain access to your bank accounts, even assume your identity. The potential harm is great. Fortunately, the prevention is relatively easy.

Understanding TCP/IP Ports and Security

TCP/IP, on which the Internet is built, uses an addressing scheme comprising IP addresses and ports. We can think of the Internet as a large group of interconnected nodes, where a node might be an individual computer, a router, or a gateway to a private network. Each node has a unique IP address. TCP/IP defines 65536 ports for each IP address. Remember that if we compare an IP address to an airport, a port is like a gate at the airport. Ports are the particular entry and exit points for each IP address. Ports 0 through 1023 are assigned to particular programs or processes. The other ports are loosely assigned or unassigned. (See *www.isi.edu/in-notes/iana/assignments/port-numbers* for more information on port assignments.) For example, by convention, port 20 is used for FTP and port 25 for SMTP. If you want to connect to the FTP server on a remote computer, you send a request to port 20 on that computer. Conversely, at the remote computer, the FTP server monitors port 20 for service requests. And this is the root of the problem.

When you are connected to the Internet, each of your TCP ports can be set to opened or closed. Open ports accept data packets, process them, and send acknowledgments to the originating computer. Closed ports disregard data packets but send a notice to the originating computer that the port is closed. Hackers run scanning programs looking across the Internet for ports at active IP addresses. If they find an open port, they can enter through that port and manipulate the process assigned to it, if any. They can also trick an open port into allowing them access to other parts of your computer. Using open ports, hackers can gain access to your files, deposit files on your computer, and monitor your network activity.

But even if they find a closed ports, hackers can still cause damage in two ways. They can exploit known security holes associated with the port and gain access to your computer. They can also launch a denial-of-service attack against that port. A denial-of-service attack overwhelms your computer, causing it to crash.

Note One important step in keeping your computer secure is to regularly check for and download security patches to your software. These patches fix security holes discovered after the release of a product. Check Microsoft's site at *www.microsoft.com/security* for its latest security bulletins.

Understanding Firewalls

Firewalls are programs that overcome the difficulties described in the previous section. Different firewall programs have slightly different features. But they all isolate computers from the Internet.

The principal firewall activity is *packet filtering*. Packet filtering can be assigned to one or more ports to inspect each packet that is addressed to the port and decide whether it should be allowed through. In most implementations, packet filtering makes its decisions based on one or more of the following:

- The originating IP address
- The originating port
- The destination IP address
- The destination port
- Whether the packet is attempting to initiate a connection or is a continuation of an existing connection

In effect, packet filtering adds a mode that is more secure than closed mode, because a port using packet filtering can disregard any packets sent to it without replying to the originating computer. If a hacker scans for this port and receives no return acknowledgment, the port (and IP address) will appear to not exist and the hacker will move on. This is a great security feature because you don't want hackers spending time trying to open closed ports on your computer.

Packet filtering is selective in two senses. It can be applied to some ports and not others. For example, if you are running a Web server that uses port 80, you can leave that port open and close all others. Packet filtering can also be selective about what it allows to pass through a port it is protecting. You can allow packets from selected computers to connect to selected ports. By doing so, you can create a private "tunnel" through the Internet. *(We discuss tunneling in Chapter 28, "Managing Incoming Connections.")* This also allows you to set up a Web server that only your friends can access (if they have static IP addresses assigned to their computers).

You can also allow in packets that are a continuation of an already established connection. This is what allows you to turn off all your ports and still establish a connection. Otherwise, you would filter out packets sent back to you. Packets contain a bit that tells whether they are initiating a connection or continuing a connection. The filter is typically set to allow continuing packets through but not initiating packets.

Note You can find lots of information about firewalls on the Internet. A good place to start your exploration is *grc.com/su-firewalls.htm* or *ftp://ftp.greatcircle.com/pub/firewalls/FAQ.*

Various firewall programs differ in how you set up packet filtering and what level of control you can exercise. Some come with a set of predefined security levels, meaning sets of packet filtering definitions. Others allow or require you to set up your own definitions.

A feature in newer firewalls is application-level filtering. This type of filtering decides which programs on your computer get access to the Internet. For example, you can allow access to Internet Explorer and Outlook Express but not FTP. This feature is directed primarily at blocking Trojan horses. With application-level filtering, even if a hacker manages to install a Trojan horse on your computer and later to activate it, the firewall prevents it from sending information over the Internet unless it is on the list of privileged applications.

Selecting a Firewall

Many software firewalls and hardware firewalls are available, ranging from free personal firewalls to expensive corporate firewalls. Windows 2000 has some firewall features, as we discuss in the following section. Firewall technology is evolving rapidly—even by Internet time standards—so rather than making specific product recommendations, we offer these guidelines for selecting one:

- Firewalls should implement your security policies. If you are a home user who simply wants to block all access to your computer from the outside, you will require a different firewall than a company hosting a Web server, an FTP server, and a RealServer server. You should define what your security requirements are before you select a firewall.
- You should choose a firewall that does not require more expertise than you have or are willing to obtain. Some firewalls require you to set individual routing rules using arcane instructions. This type of setup gives you total control over how your firewall performs, but if you don't want too much complexity, get a firewall with predefined settings you can select.
- You should choose a firewall that includes some form of application-level filtering. In the current Internet hacking environment, this is a must-have feature.
- Firewalls provide differing levels of monitoring. You should decide how much of your Internet activity you want to monitor, and choose a firewall that provides that capability.

Packet Filtering and Trojan Horses

Trojan horses are small programs that work much like their Greek namesake. Trojan horses can be installed on your computer through an open port. Once installed, they listen to a (usually high-numbered) port until their creator contacts them though that port. After they are contacted and activated, they perform whatever malicious purposes their owner requests, such as sending out files or other information from your computer, monitoring your activities, or launching an attack on another computer using your IP address as cover.

Properly implemented packet filtering foils Trojan horses even if they do get installed. Because you can selectively turn on only the ports you use, the port the Trojan horse wants to use can be turned off, thus making it impossible for its creator to contact and activate it.

Some firewalls include a feature especially designed to prevent the activity of Trojan horses: application-level filtering. With such a firewall, you can specify which programs or processes on your computer are allowed to communicate over the Internet. Because you do not add any Trojan horses to the list of privileged programs, they are not able to communicate with the outside world.

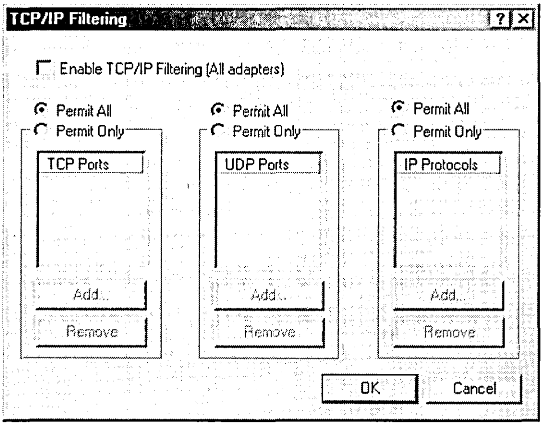
Using Windows 2000 Packet Filtering

Windows 2000 allows you to set up limited packet filtering through the network connection properties. This capability is limited because it filters only incoming packets and does not allow filtering by IP address. *Windows 2000 also has more sophisticated packet filtering capabilities, which we discuss in Chapter 28, "Managing Incoming Connections."*

To configure packet filtering:

1. Open the Properties dialog box for the connection you are setting up.
2. Select Internet Protocol (TCP/IP) and click Properties.
3. Click Advanced and then select the Options tab.
4. Click TCP/IP Filtering and then click Properties. The TCP/IP Filtering dialog box opens, as shown in Figure 25-5.
5. To enable packet filtering, select Enable TCP/IP Filtering (All Adapters).

You have options to set filtering for TCP ports, UDP ports, and IP Protocols. UDP ports are almost the same as TCP ports, except that TCP ports send acknowledgments for all packet transmissions, whereas UDP does not. UDP is used for transmissions such as streaming media, for which a few lost packets don't make a difference. IP protocol is a number (in the range 1 through 255) that identifies the type of IP packet to an upper-layer protocol. Common identifiers are 6 for TCP, 17 for UDP, and 1 for ICMP.



TCP/IP Filtering

☐ Enable TCP/IP Filtering (All adapters)

● Permit All
○ Permit Only
TCP Ports

● Permit All
○ Permit Only
UDP Ports

● Permit All
○ Permit Only
IP Protocols

Figure 25-5
Set packet filtering options in this dialog box.

For each protocol, you can select Permit All or Permit Only. Permit All means not to filter any ports—that is, permit all packets. If you select Permit Only, you then add the port or protocol numbers you want to open. The rest will be closed. Because the packet filtering you set here is only for incoming packets, you need to open only ports that you want other computers to access. For example, if you run a Web server, you need to open port 80 so that anyone wanting to reach your site can do so. You don't need to open port 80 in order to reach another Web site yourself, because connections you establish from the inside are not blocked. Note, however, that this procedure closes ports only in the sense discussed previously. Windows 2000 packet filtering still sends a response to inquiring computers and thus does not supply the added "stealth" mode of most third-party firewalls.

Warning The most important security setting on any connection to the Internet, whether it is a dial-up connection or a network connection, is File And Printer Sharing For Microsoft Networks. Enabling this setting opens the door to your entire computer to nefarious hackers. You should ensure that it is disabled on any Internet (but not LAN) connections.

Closing Ports 137, 138, and 139

TCP ports 137 through 139 are used by NetBIOS, a totally trusting network protocol meant for isolated local networks. File And Print Sharing uses NetBIOS. Therefore, whenever these ports are open to the Internet, everyone on the Internet has File And Print Sharing access to your computer. This is true even if you use password protection, because passwords can be broken. It does not take a hacker much effort to scan your IP address, find the open NetBIOS port, crack your password, and gain access to all your files. Even though NetBIOS is entirely unnecessary for Internet connections, it is enabled by default. Closing this port should be the first thing you do when creating your Internet connection. If you don't want to use TCP/IP filtering as described previously, you can easily use another two-step process for closing these ports. You might as well perform these steps anyway, because they reduce the overhead on your network.

1. Unbind NetBIOS from your TCP/IP protocol. Open the Network And Dial-Up Connections folder. Right-click the icon for your Internet connection and choose Properties. Under Components Checked Are Used By This Connection, clear Client For Microsoft Networks and File And Printer Sharing For Microsoft Networks if these options are listed.
2. Select Internet Protocol (TCP/IP) and click Properties. On the General tab, click Advanced. Click the WINS tab and select Disable NetBIOS Over TCP/IP.

Testing Your Port Security

You can test the security of your Internet connection at the Gibson Research Web site (*https://grc.com/x/ne.dll?bh0bkyd2*). This site performs a scan of your IP address and ports as a hacker might do and reports the status of most commonly used ports. This site also contains a wealth of information on Internet security. (If the preceding link doesn't work for you, go to *grc.com* and then click the link to Shields UP.

Chapter 26

Internet Explorer: Beyond Browsing

In This Chapter

Downloading from the Internet 435
Using Security and Privacy Features 440
Customizing Internet Explorer 446

Microsoft Windows 2000 comes integrated with Microsoft Internet Explorer 5 as the default tool for accessing Web pages from the Internet or a local intranet. Internet Explorer's integration reflects the increased importance of Web activity for most computer users today. Reflecting the range of expertise of Windows users, Internet Explorer can be used with little or no modification by novices, but it also has extensive possibilities for tailoring by expert users. We discuss in this chapter several of these advanced configuration features.

Note In Windows 2000, Internet Explorer is an integral component of the operating system. You cannot remove it using Add/Remove Programs. But if you prefer another browser, you need only install it. If Internet Explorer continues to nag you with its desire to be the default browser after you've installed another, you can quench that desire with a visit to Control Panel | Internet Options | Programs; clear the Internet Explorer Should Check To See Whether It Is The Default check box.

Downloading from the Internet

A common activity of users on the Web is downloading files. These files might be shareware utilities, games, ActiveX components, video clips, or many other types of files.

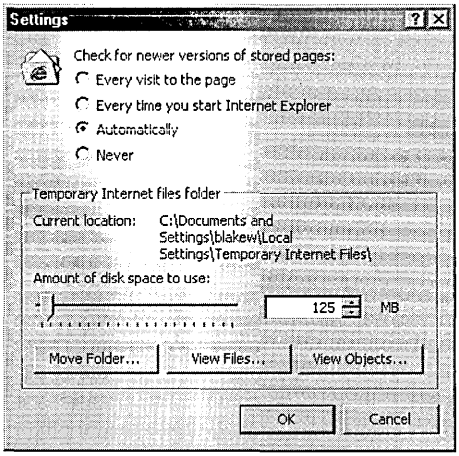
Determining Where Downloaded Files End Up

Internet Explorer maintains two folders for downloaded files. The first, Temporary Internet Files, stores three sets of files:

- HTML files, graphics and sound files, and other files used on the Web pages you view
- Cookies, which some Web sites use to store information about you
- Files you are downloading to another destination, which are stored in this folder until the download is complete

Temporarily storing Web page files increases the speed at which Internet Explorer can display Web pages, because it can use the cached files rather than downloading them again from the Internet.

The Temporary Internet Files folder, which is hidden, is located by default at %UserProfile%\Local Settings\Temporary Internet Files. You can access this folder using Windows Explorer, but a better way is to access it through the Internet Options dialog box. On the General tab, click Settings to display the dialog box shown in Figure 26-1. In the Settings dialog box, you can click View Files to open a Windows Explorer view of the Temporary Internet Files folder. You can perform any ordinary file operation from here.



Settings

Check for newer versions of stored pages:

○ Every visit to the page
○ Every time you start Internet Explorer
● Automatically
○ Never

Temporary Internet files folder

Current location: C:\Documents and Settings\blakew\Local Settings\Temporary Internet Files\

Amount of disk space to use: 125 MB

Figure 26-1
You can manage the Temporary Internet Files folder from the Settings dialog box.

If you want to move the Temporary Internet Files folder—say, to a drive with more free space—you can do that from the Settings dialog box. You need to create the new folder first and then click Move Folder. In the Browse For Folder dialog box, select the new folder and click OK. The move can take a while, and you will be asked to log off to complete the move.

The Settings dialog box gives you four options for using these temporary files. Each option strikes a different balance between the opposing desires for quick display and current information. The options are stated in terms of how often Internet Explorer should check the files in the Temporary Internet Files folder for updates.

- **Every Visit To The Page.** This option causes Internet Explorer to check files every time you access a page. If the temporary files are still current, they are displayed. Otherwise, the new files are downloaded and displayed. This option ensures that the information you see is always current, but it slows your browsing.
- **Every Time You Start Internet Explorer.** This option causes Internet Explorer to check files once per Internet Explorer session. Thus a check is made the first time you visit a page after you open Internet Explorer but not again until you close Internet Explorer and then reopen it. If you have Internet Explorer open over the course of two days and you revisit a page that you visited the previous day, Internet Explorer checks the files again.
- **Automatically.** This option is the same as the Every Time You Start Internet Explorer option except that Internet Explorer tabulates how often pages are actually updated. If a page is not updated frequently, Internet Explorer reduces the frequency with which it checks that page.
- **Never.** This option causes Internet Explorer to never check for newer files and to always display what is in the Temporary Internet Files folder. If you're in the habit of covering your tracks by clearing the Temporary Internet Files folder whenever you quit Internet Explorer (an option you can select in the Security section of the Advanced tab in the Internet Options dialog box), the folder will contain little of value—so you might as well eliminate the overhead of checking it.

In all cases, clicking the Refresh button causes Internet Explorer to check for updated files. Files remain in the Temporary Internet Files folder until the allotted disk space is used, whereupon files are deleted on a first-in, first-out basis. You control the allotment of disk space in the Settings dialog box.

Normally, when you download a file from the Internet, a dialog box asks whether you want to download or open the file. If you choose to download the file, another dialog box asks for a file location. The first dialog box contains the option Always Ask Before Opening This Type Of File. If you clear this option and download the file, you will not receive this prompt for any future downloads of the same file type (that is, files with the same file name extension), and the files will be stored in the Temporary Internet Files folder and opened when the download is complete. If you have cleared this option for a particular file type but want to revert to being prompted for a file location, follow these steps:

1. In Windows Explorer, choose Tools | Folder Options | File Types.

2. From the Registered File Types list, select the file name extension you want to modify and click Advanced.
3. Select Confirm Open After Download.

The second folder for downloads, the Downloaded Program Files folder, stores ActiveX controls. When you accept the download of an ActiveX component (depending on your security settings, Internet Explorer either prompts you for each component or downloads all signed components automatically), it is stored in this folder. Downloaded Program Files is a hidden folder in the %SystemRoot% folder. You can open the Downloaded Program Files folder by clicking View Objects in the Settings dialog box.

Note Your offline Web page files are stored in another hidden folder, %SystemRoot%\Offline Web Pages. You can access this folder in Windows Explorer, but it is usually more convenient to manage your offline Web pages using the Items To Synchronize dialog box. You can reach it from Internet Explorer (Tools | Synchronize) or from the Start menu (Programs | Accessories | Synchronize).

You can remove ActiveX components in two ways. If the component is listed in the Add/Remove Programs dialog box, remove it from there. If it is not listed in Add /Remove Programs, open the Downloaded Program Files folder, right-click the unwanted component, and choose Remove.

Note You can check for an update to an ActiveX control by right-clicking the control's icon in the Downloaded Program Files folder and choosing Update.

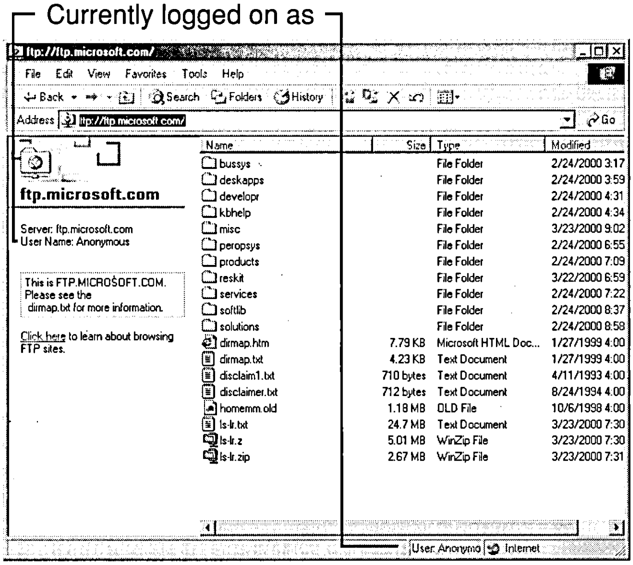
Using FTP Folders

Internet Explorer adds new functionality for viewing file transfer protocol (FTP) sites. FTP folder view allows you to view and traverse FTP sites in much the same way you view and traverse your hard disk or LAN using Windows Explorer, thereby providing consistency in the way you see local and Internet files. If you have Enable Web Content In Folders turned on (in the Folder Options dialog box), you will see additional information about FTP files and folders.

To view a site that allows anonymous logons, simply type the URL in the Address bar of Internet Explorer or Windows Explorer. To connect to an FTP server that requires you to provide your user name and password, you can include your logon information in the Address bar, as in this example:

```
ftp://name:password@ftp.microsoft.com
```

Alternatively, after you arrive at the site, you can open the File menu (or right-click in the window) and choose Login As to provide your logon credentials. Regardless of who you log on as—even if you use anonymous logon—you can tell who you're logged on as by looking at the status bar or, if you're using Web view, by checking the left side of the folder window. See Figure 26-2.


Currently logged on as
ftp://ftp.microsoft.com/
File Edit View Favorites Tools Help
Back Search Folders History
Address ftp://ftp.microsoft.com/
Go
User: Anonymo
Internet

ftp.microsoft.com

Server: ftp.microsoft.com
User Name: Anonymous

This is FTP.MICROSOFT.COM.
Please see the
dirmap.txt for more information.

Click here to learn about browsing FTP sites.

Name	Size	Type	Modified
bussys		File Folder	2/24/2000 3:17
deskapps		File Folder	2/24/2000 3:59
developr		File Folder	2/24/2000 4:31
kbhelp		File Folder	2/24/2000 4:34
misc		File Folder	3/23/2000 9:02
peropsys		File Folder	2/24/2000 6:55
products		File Folder	2/24/2000 7:09
reskit		File Folder	3/22/2000 6:59
services		File Folder	2/24/2000 7:22
softlib		File Folder	2/24/2000 8:37
solutions		File Folder	2/24/2000 8:58
dirmap.htm	7.79 KB	Microsoft HTML Doc...	1/27/1999 4:00
dirmap.txt	4.23 KB	Text Document	1/27/1999 4:00
disclaim1.txt	710 bytes	Text Document	4/11/1993 4:00
disclaimer.txt	712 bytes	Text Document	8/24/1994 4:00
homemm.old	1.18 MB	OLD File	10/6/1998 4:00
ls-lr.txt	24.7 MB	Text Document	3/23/2000 7:30
ls-lr.z	5.01 MB	WinZip File	3/23/2000 7:30
ls-lr.zip	2.67 MB	WinZip File	3/23/2000 7:31

Figure 26-2
Web view shows that this user is logged on as Anonymous.

The FTP folder feature does not support the following functionality:

- Connecting to the Internet using a CERN proxy server or Web proxy server
- Connecting to a Virtual Address Extension (VAX) or Virtual Memory System (VMS) FTP server
- Using Internet Explorer from within a separate program or service
- Copying files from one server to another
- Moving files using drag-and-drop functionality from an FTP server
- Using the Copy command on the Edit menu and shortcut menus for files on an FTP server (although you can copy local files and paste them on an FTP server)

You might also be limited to viewing and downloading files if you are connecting through an FTP proxy.

You can turn off Web-based FTP folders by clearing Enable Folder Views For FTP Sites on the Advanced tab of the Internet Options dialog box. In that case, you must use an FTP gateway or another FTP client to access FTP servers. *For information about the command-line FTP client included with Windows 2000, see Chapter 31, "Using the FTP Clients."*

Using Security and Privacy Features

Security and privacy are among the greatest concerns for most Internet users. Internet Explorer provides numerous options for controlling the type and amount of security and privacy you want to maintain. Access to these options is primarily through the Internet Options dialog box; you can open it by choosing Tools | Internet Options in Internet Explorer or by opening Control Panel | Internet Options.

Using Digital Certificates

Digital certificates make two important security features on the Internet possible: signing and encrypting. *Signing* authenticates the identity of people and organizations on the Internet. If an e-mail message you receive or a program you download is digitally signed, you are assured that the identity claimed by the originating person or organization is genuine. *Encryption* hides information from anyone not authorized to see it.

Digital signature and encryption schemes use three items: public keys, private keys, and a certification authority (CA). You use your private key when you digitally sign a document or program or when you encrypt a message you send to someone else. It's essential to keep your private key secure, because any unauthorized access to it compromises your entire security scheme. People to whom you send signed or encrypted documents use your public key to confirm your identity or decrypt what you have encrypted.

The use of public and private keys, called *asymmetric cryptography,* is an important development in security schemes. In the past, the same key was used to encrypt and decrypt messages, which meant that both the sender and the recipient needed the key. Transmitting the key from sender to recipient was itself a significant security problem. The use of private and public keys removes that problem.

A *certification authority* assigns certificates to individuals and organizations. The CA takes responsibility for verifying the identity of the individual or organization applying for the certificate before granting it. After verifying the requester's identity, the CA assigns that requester a public key and a private key and provides a digital certificate signed with the CA's own private key. The validity of the certificate is therefore only as good as the trust in the CA. Internet Explorer maintains a list of trusted certification authorities and is configured with several CAs' certificates preinstalled. *(We explain how to add or remove trusted CAs in the following section.)* The CA also maintains a database of revoked certificates. You can configure Internet Explorer to check the CA for revoked certificates; *see "Setting Advanced Options," page 455.*

Note Microsoft maintains a Web page that discusses certification authorities at *www.microsoft.com/windows/oe/certpage.htm.*

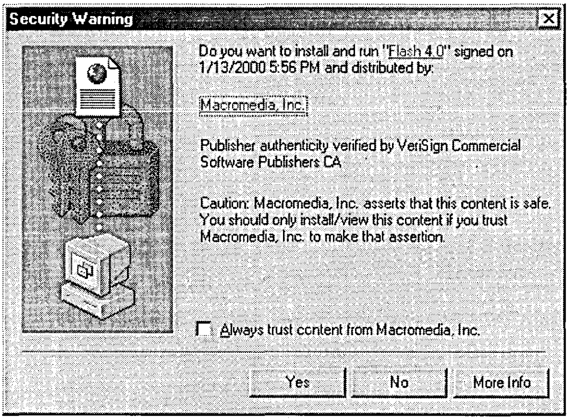
The digital certificate contains three main items: identification information about the sender, the sender's public key, and the CA's validation of the certificate signed with its private key. This certificate is required whenever you send or receive a signed or encrypted document or program. It needs to be sent only once, though, because Internet Explorer stores for future use all certificates that it receives.

Both public and private keys are required for encryption and decryption. For example, when you use your private key to encrypt a message, that message can be decrypted only with your public key. So, if you want to send secure e-mail to others, you must first send them your public key as part of your personal certificate. Then, when you send them a message encrypted with your private key, they can decrypt it with your public key. If they want to send an encrypted message in return, they must encrypt it with their private key, and you must have their public key to decrypt it.

Software distribution over the Internet works much the same way. A software vendor uses a private key to digitally sign a piece of software, which is then made available for download. A certificate containing both the public key and an authorization from a certification authority is attached to the program. When Internet Explorer sees the signature and certificate, it displays a warning and asks whether you want to continue with the download, as shown in Figure 26-3. The warning contains three important notices. The first names the program you are about to install and the date of its signing. The program name might be a link to more information about the program, supplied by the publisher. The second notice is the name of the publisher, which might also be a link to more information. The third notice provides the name of the CA and a statement of the certificate's authenticity. At the bottom is a check box that lets you choose to always trust content from that publisher. If you select this option, that publisher is added to your list of trusted publishers and any future content from that source will be downloaded and installed without notification.

The signing process starts when the software is ready for delivery. At that time, the publisher signs it using its private key. If the program is subsequently tampered with, the signature is invalidated. When Internet Explorer begins downloading the program and sees the signature, it checks the validity of the certificate and presents a warning similar to the one shown in Figure 26-3. Internet Explorer watches for signatures on ActiveX files, cabinet files, Java applets, and executable files.

Note Certificate technology is also used for network credentials. Certificates can be used in conjunction with smart cards to manage logons and access to network resources.



Security Warning

Do you want to install and run "Flash 4.0" signed on 1/13/2000 5:56 PM and distributed by:

Macromedia, Inc.

Publisher authenticity verified by VeriSign Commercial Software Publishers CA

Caution: Macromedia, Inc. asserts that this content is safe. You should only install/view this content if you trust Macromedia, Inc. to make that assertion.

□ Always trust content from Macromedia, Inc.

Figure 26-3
A warning indicates a digitally signed program.

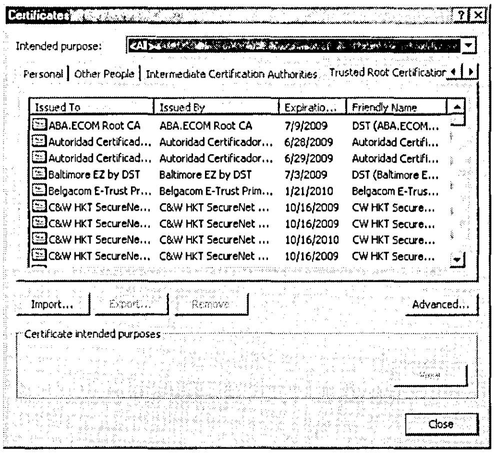
Installing and Removing Trusted Certificates

For Internet Explorer to validate a certificate for a program, the CA's certificate must be stored in Internet Explorer's list of Trusted Root Certification Authorities. If a program is certified by a CA that does not appear in this list, the warning message displayed by Internet Explorer (similar to the one shown in Figure 26-3) indicates that the root certificate has not been enabled as a trusted root and the content cannot be verified. You can still download the file if you choose to. If you click the link attached to the publisher's name, the Certificate dialog box opens. Clicking Install Certificate installs the CA's certificate in Internet Explorer's list of Trusted Root Certification Authorities.

You add or remove trusted certificates by using the Certificates dialog box. Open the Certificates dialog box by clicking Certificates on the Content tab of the Internet Options dialog box. The Certificates dialog box has four tabs, as shown in Figure 26-4.

- **Personal.** This tab contains certificates with an associated private key (typically, your own personal certificates).
- **Other People.** This tab contains certificates with an associated public key. This category contains all certificates that are not in the Personal category and did not come from CAs.
- **Intermediate Certification Authorities.** This tab contains all certificates from CAs, including trusted root certificates.
- **Trusted Root Certification.** This tab contains self-signing certificates. You intrinsically trust content from people and publishers with certificates issued by these CAs.

To remove a certificate, select it and click Remove. You can add certificates when you receive warnings, as described earlier, or by importing them from a file. To use the latter method, simply click Import and follow the wizard. The Certificates dialog box also allows you to export certificates to a file. With the export and import functions, you can move trusted certificates from one computer to another.


Certificates
?
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	DST (ABA.ECOM...
Autoridad Certificad...	Autoridad Certificador...	6/28/2009	Autoridad Certifi...
Autoridad Certificad...	Autoridad Certificador...	6/29/2009	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	7/3/2009	DST (Baltimore E...
Belgacom E-Trust Pr...	Belgacom E-Trust Prim...	1/21/2010	Belgacom E-Trus...
C&W HKT SecureNe...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureNe...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureNe...	C&W HKT SecureNet ...	10/16/2010	CW HKT Secure...
C&W HKT SecureNe...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...

Figure 26-4
The Certificates dialog box lists all certificates you have received.

Adding and Removing Trusted Publishers

As we explained earlier, you can designate publishers as trusted, and you are not notified when you download software from trusted publishers. You add trusted publishers by selecting the Always Trust Content From check box in the Security Warning dialog box. (Refer to Figure 26-3.)

To remove a trusted publisher from your list, click Publishers on the Content tab of the Internet Options dialog box. Select the publisher you want to remove and click Remove.

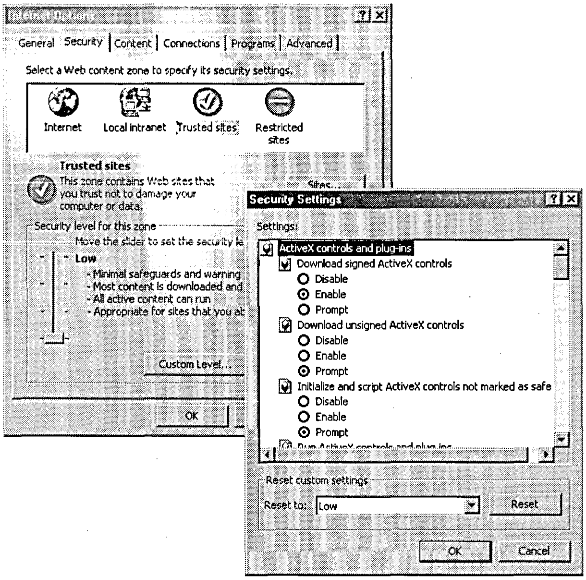
Using Security Zones

The Security tab in the Internet Options dialog box controls the predefined security zones used by Internet Explorer to assist in defining different levels of security for different sites. By default, Internet Explorer uses one of two zones to store sites: Local Intranet and Internet. When you open a Web page, Internet Explorer determines which zone the page is in and applies the respective security settings. You can apply either of two additional zones to sites on an individual basis: Trusted Sites and Restricted Sites. To add or remove a site in either of these zones:

1. On the Security tab of the Internet Options dialog box, select the zone (Trusted Sites or Restricted Sites) to which you want to add a site.
2. Click Sites.
3. Type the URL of the site you want and click Add.

Note Microsoft Internet Explorer 5 Power Tweaks Web Accessories provides an easier way to add sites to these lists. Instead of navigating through dialog boxes and typing URLs, a simple command on the Tools menu adds the current site. *For more information, see "Adding Microsoft Web Accessories," page 460.*

For each zone, you can choose one of four predefined security levels, or you can customize the settings for any zone. The security setting includes such items as what to do with unsigned ActiveX components and whether to accept cookies. To customize the settings for a zone, select the zone, select a security level to use as the basis, and then click Custom Level. In the Settings box, select or clear options to meet your own security preferences. See Figure 26-5.



Select a Web content zone to specify its security settings.

Trusted sites
This zone contains Web sites that you trust not to damage your computer or data.

Security level for this zone
Move the slider to set the security le
Low
- Minimal safeguards and warning
- Most content is downloaded and
- All active content can run
- Appropriate for sites that you at

Settings:

ActiveX controls and plug-ins
Download signed ActiveX controls
○ Disable
● Enable
○ Prompt
Download unsigned ActiveX controls
○ Disable
○ Enable
● Prompt
Initialize and script ActiveX controls not marked as safe
○ Disable
○ Enable
● Prompt

Reset custom settings
Reset to: Low

Figure 26-5
In the Settings box, you set security options for a particular security zone.

Note The Settings box, like similar controls elsewhere in Windows 2000, uses a hierarchical structure much like the Folders bar in Windows Explorer. Although you won't see any plus signs, minus signs, or dotted lines connecting the entries at each level, you *can* collapse and expand the outline simply by double-clicking an entry. You'll find this little-known feature handy when you're trying to wade through an especially long list like this one.

Setting Up Java Custom Security

Internet Explorer has a default configuration for using Java securely. You can customize these settings, but the way of doing so is a bit hidden.

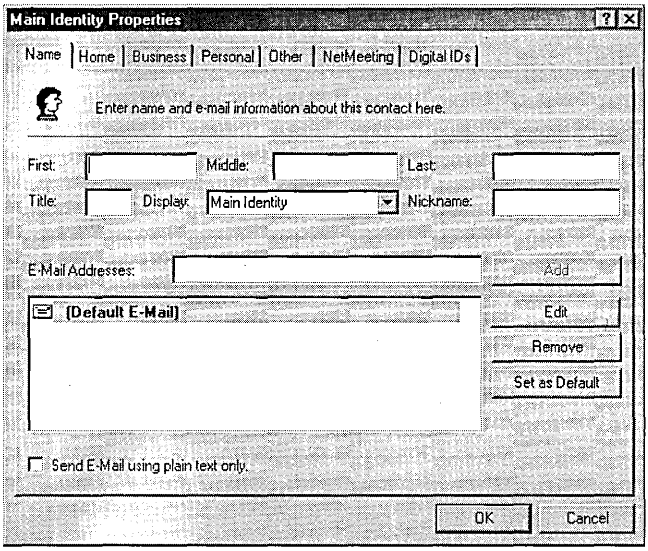
1. On the Security tab of the Internet Options dialog box, select the zone you want to modify and then click Custom Level.
2. Under Microsoft VM\Java Permissions, select Custom. The Java Custom Settings button appears.
3. Click Java Custom Settings.
4. Select the Edit Permissions tab and make the desired changes.

Using Profile Assistant

Internet Explorer contains a utility for storing and selectively sharing your personal information. This information is contained in a user profile, which is kept in a secure, encrypted information store on your computer. Web sites compatible with Profile Assistant can request information from your profile. You then have the option of granting access to information as you choose. The benefit is that you don't have to retype information at each site you visit.

To use Profile Assistant, you must select Enable Profile Assistant on the Advanced tab of the Internet Options dialog box. Then you must fill out your personal profile. On the Content tab of the Internet Options dialog box, click My Profile. If you already have entries in your Address Book, Windows first asks whether you want to use an existing entry for your profile information. If you choose to create a new entry—or if your Address Book is empty—the dialog box shown in Figure 26-6 appears. As you can see, it's an ordinary Address Book record. Fill in the information on each tab as you like and click OK to save it.

When you open a Web page containing forms that are Profile Assistant–enabled, a dialog box appears that shows the fields on the page with corresponding entries in your profile. You can select which fields you want to supply from your profile. A sample Web page and dialog box are shown in Figure 26-7. If you want to use Profile Assistant on your own Web site, visit *msdn.microsoft.com/workshop/management/profile/profile_assistant.asp* for more information.



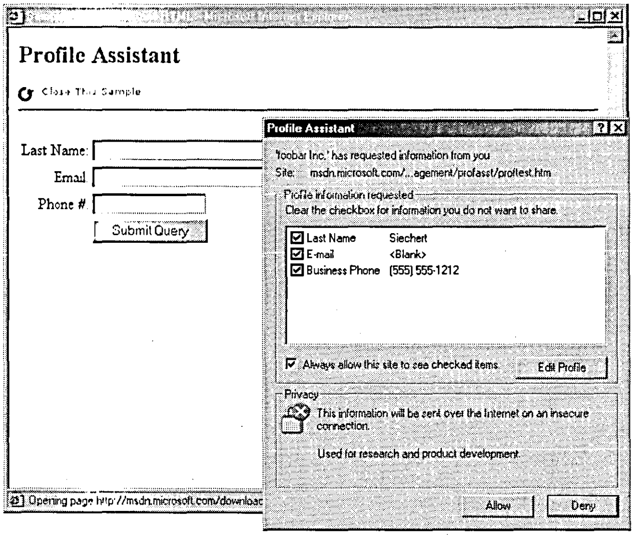
Enter name and e-mail information about this contact here.

Display: Main Identity

[Default E-Mail]

□ Send E-Mail using plain text only.

Figure 26-6
Use Profile Assistant to securely store personal information used by some Web sites.



'foobar Inc.' has requested information from you

Site: msdn.microsoft.com/...agement/profasst/proftest.htm

Clear the checkbox for information you do not want to share.

☑ Last Name Siechert
☑ E-mail <Blank>
☑ Business Phone (555) 555-1212

☑ Always allow this site to see checked items.

This information will be sent over the Internet on an insecure connection.

Used for research and product development.

Opening page http://msdn.microsoft.com/downloac

Figure 26-7
Profile Assistant helps fill out forms on Web pages.

Customizing Internet Explorer

Internet Explorer provides four separate paths for customization: manual, automatic detection, directed configuration, and Group Policy settings. Not all configuration elements are available along all paths, but most are.

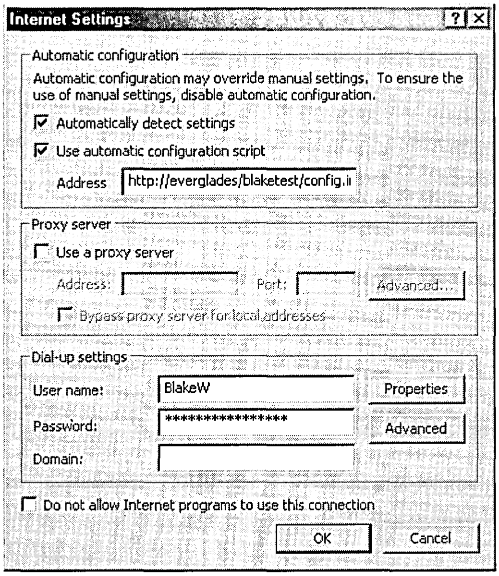
Your site administrator might have created a configuration script for you to use. Configuration scripts can control all aspects of Internet Explorer, from the look of the toolbar to which features you are authorized to change. Unless you are a system administrator for a large network or a developer delivering custom versions of Internet Explorer, you don't need to know much about creating configuration scripts. The tools for creating them are the Internet Explorer Administration Kit (IEAK) and the Internet Explorer Profile Manager, which is included in the IEAK. The IEAK is included on the companion CD.

Automatic detection and directed configuration use these configuration scripts to configure Internet Explorer each time it is started. Automatic detection sends a query to the DHCP or DNS server to find the location of the script. With directed configuration, you supply the location of the script. If your system administrator has configured the network's DHCP or DNS server to supply the script's location, use automatic detection. Otherwise, supply the location of the script.

To enable Internet Explorer to automatically detect settings, open the Internet Options dialog box and click the Connections tab. Click Settings to open the Internet Settings dialog box, as shown in Figure 26-8. Select Automatically Detect Settings. To direct Internet Explorer to the configuration script, select Use Automatic Configuration Script and then enter the location of the script in the following form:

```
http://server/config.ins
```

where *server* is the configuration server name and path.



Internet Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

☑ Use automatic configuration script

Address: http://everglades/blaketest/config.ii

Proxy server

☐ Use a proxy server

Address: Port:

☐ Bypass proxy server for local addresses

Dial-up settings

User name: BlakeW

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

Domain:

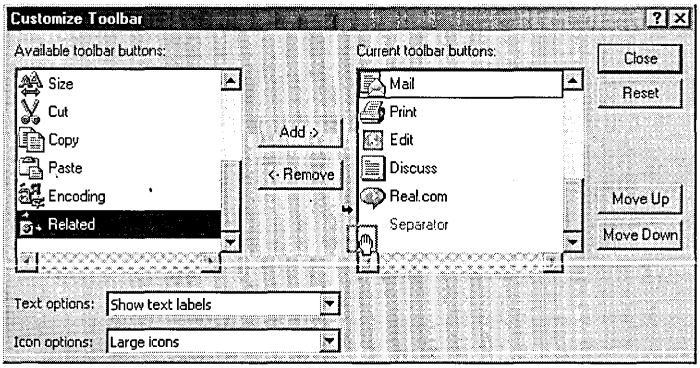
☐ Do not allow Internet programs to use this connection

Figure 26-8
You can select automatic configuration detection and specify an automatic configuration script.

In the following sections, we discuss several features of Internet Explorer that you can customize manually through the browser interface. We also discuss how to set other features for all users of your computer through Group Policy settings.

Customizing the Internet Explorer Toolbar

Internet Explorer allows you to add buttons to the Standard Buttons toolbar or rearrange the existing ones. Right-click the toolbar and choose Customize. The Customize Toolbar dialog box opens, as shown in Figure 26-9. The Current Toolbar Buttons list shows the toolbar buttons that are already displayed, in the order in which they appear. The Available Toolbar Buttons list shows the buttons you can add. The dialog box also contains options for how text is displayed with the toolbar buttons and the size of the button icons.



Text options: Show text labels

Icon options: Large icons

Figure 26-9
You can use a drag-and-drop operation to configure your Internet Explorer.

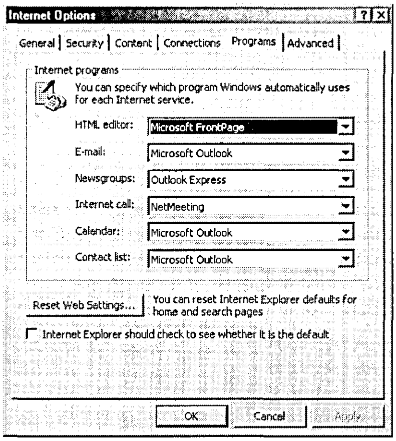
To add a button to the toolbar, click its icon in the Available Toolbar Buttons list and drag it to the Current Toolbar Buttons list. To change the order of buttons on your toolbar, click a button icon in the Current Toolbar Buttons list and either drag it to the desired position or click the Move Up and Move Down buttons until the button is in the proper order.

Internet Explorer and Microsoft Office 2000

Internet Explorer also works together with the Microsoft Office 2000 components. If you have Office 2000 installed, you will notice some differences in Internet Explorer because of the collaboration features of Office 2000. One such item is the Discussion button on the toolbar. Office 2000 allows users to add and share comments on Web pages (or other Office documents) using its online discussion feature. If you click the Discussion button and you have a discussion server on your network, a frame opens in the bottom of the Internet Explorer window, where you can insert comments that are then attached to the current Web page. Other people on your network who also have Office 2000 can view your comments and add their own. A discussion server can be any Web server with Office Server Extensions installed.

Configuring Default Support Programs

Internet Explorer keeps track of six programs related to using the Internet. For example, if you click a mailto link on a Web page, Internet Explorer needs to know which e-mail program to open. If you open the source code for a Web page, Internet Explorer needs to know which editor to use. The programs that Internet Explorer keeps track of are listed in Figure 26-10.



Internet programs

You can specify which program Windows automatically uses for each Internet service.

HTML editor:	Microsoft FrontPage
E-mail:	Microsoft Outlook
Newsgroups:	Outlook Express
Internet call:	NetMeeting
Calendar:	Microsoft Outlook
Contact list:	Microsoft Outlook

Reset Web Settings... You can reset Internet Explorer defaults for home and search pages

□ Internet Explorer should check to see whether it is the default

Figure 26-10
You can configure Internet Explorer support programs on the Programs tab.

These programs are all configured on the Programs tab of the Internet Options dialog box. Each box lists the installed programs in a particular category. For example, if you have installed Microsoft Office and Microsoft FrontPage, you can select Microsoft Word, FrontPage, or Notepad as your default HTML editor.

Note You can also select an HTML editor from the drop-down menu of the Edit button on the toolbar. Making one of these selections opens the source code for the current page in the selected editor.

A new feature of Internet Explorer is the ability to configure Hotmail, a Web-based e-mail system run by Microsoft, as your default e-mail client. With a Hotmail account, you can access your e-mail from any Web browser anywhere in the world. If you use Hotmail, configuring Internet Explorer to use it as its default e-mail program means that whenever you click a mailto link, choose File | Send, or click the Mail button on the toolbar, a new Internet Explorer browser window opens to your Hotmail account.

Configuring Internet Explorer with Group Policy

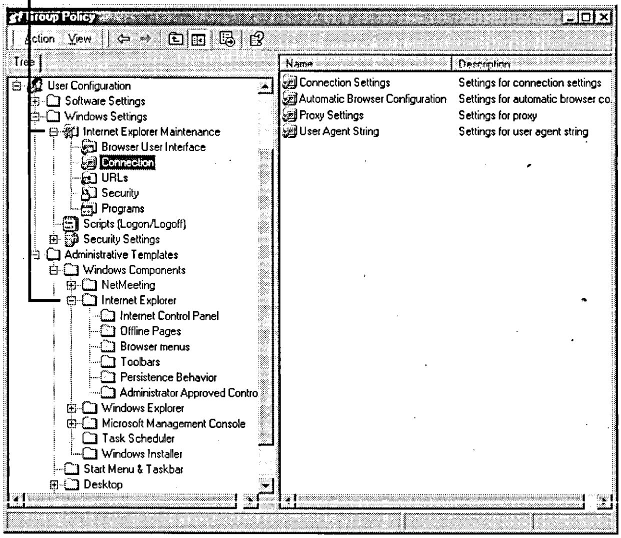
The Group Policy console (Gpedit.msc) provides a way to manage the behavior of users' desktops. The settings in Group Policy apply to all users of the computer on which they are set. Three sets of Group Policy settings deal with Internet Explorer:

- Internet Explorer Maintenance (in Local Computer Policy\User Configuration \Windows Settings) contains policies for configuring Internet Explorer settings.
- Internet Explorer (in Local Computer Policy\User Configuration\Administrative Templates) contains policies for configuring permissions.
- Internet Explorer (in Local Computer Policy\Computer Configuration \Administrative Templates \Windows Components) contains additional policies for Internet Explorer settings.

The Group Policy console is shown in Figure 26-11. *(For detailed information, see Chapter 18, "Using Group Policy.")*

Note You must be logged on as a member of the Administrators group to open the Group Policy console.

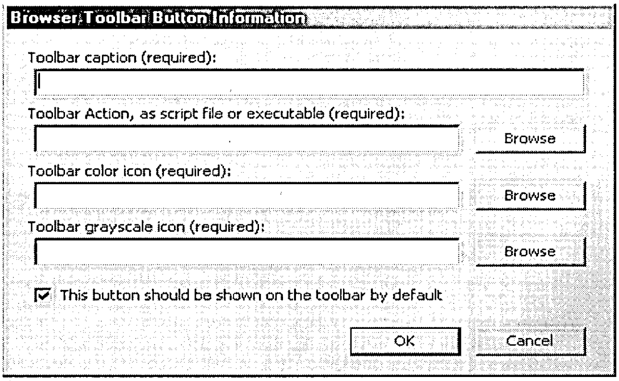
Group Policy settings for Internet Explorer



Name	Description
Connection Settings	Settings for connection settings
Automatic Browser Configuration	Settings for automatic browser co.
Proxy Settings	Settings for proxy
User Agent String	Settings for user agent string

Figure 26-11
The Group Policy console allows you to make Internet Explorer configuration settings for all users of your computer.

The policies under Internet Explorer Maintenance encompass most of the settings you can make directly in Internet Explorer, such as customizing the toolbar and defining default support programs. In some cases, the properties dialog box in Group Policy offers the same options as the Internet Options dialog box, although sometimes Group Policy allows more flexibility. For example, you can add toolbar buttons by using either the Customize Toolbar dialog box (as explained earlier) or Group Policy. When you use Group Policy, however, you must define each aspect of the toolbar button, including its name, icon, and executable file, as shown in Figure 26-12. Doing this requires more knowledge on your part, but it allows you to add buttons that are not found on the list in the Customize Toolbar dialog box.


Browser Toolbar Button Information
Toolbar caption (required):
Toolbar Action, as script file or executable (required):
Browse
Toolbar color icon (required):
Browse
Toolbar grayscale icon (required):
Browse
OK
Cancel

☑ This button should be shown on the toolbar by default

Figure 26-12
You can configure any button for the toolbar using Group Policy.

Note If you use both Group Policy settings and a configuration script, the Group Policy settings will be in effect whenever you open an Internet Explorer window, but the configuration script will override any corresponding Group Policy settings when it runs.

Group Policy settings can also restrict which features of Internet Explorer users are allowed to configure for themselves. For example, under Local Computer Policy \User Configuration\AdministrativeTemplates\Internet Explorer\Internet Control Panel, as shown in Figure 26-13, you can disable any of the tabs in the Internet Options dialog box, thereby preventing anyone who is using your computer from changing security zone settings or any Advanced setting. (To achieve more granular control over the use of security zones and to avoid removing the tab altogether, check the policies in Local Computer Policy\Computer Configuration \Administrative Templates\Windows Components\Internet Explorer.)

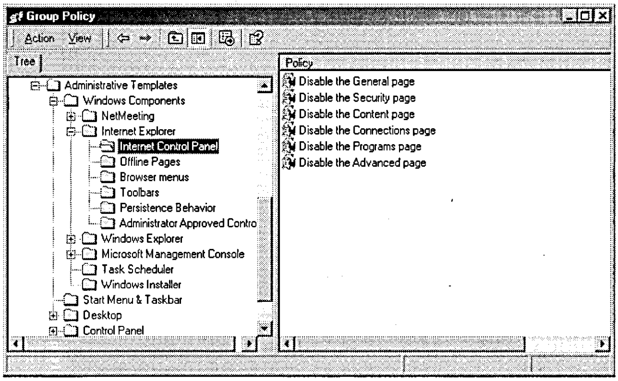


Figure 26-13
Group Policy allows you to restrict user access to Internet Explorer options.

Importing and Exporting Favorites and Cookies

Sometimes Web surfers move from one computer to another or from one browser to another and would like to take their favorites and cookies along with them. Internet Explorer provides a convenient method for doing this with the Import /Export Wizard. The wizard has four functions: Export Favorites, Import Favorites, Export Cookies, and Import Cookies. The export and import functions work with files or other installed browsers.

To use the Import/Export Wizard:

1. Open the wizard by selecting Import And Export from the File menu.
2. Click Next on the first wizard page.
3. Select the action you want to perform and click Next.
4. If you are exporting favorites, the wizard allows you to select a subset of your favorites for exporting. You can select only one folder in your favorites list to export, but the wizard also includes all subfolders of the selected folder. Selecting the highest level folder, Favorites, exports your entire list.
5. Select the source or destination. If you want to import from (or export to) another browser, select Import From (or Export To) An Application and select the browser from the drop-down list. (If no other browsers are installed, this option is not available.) If you export favorites or cookies to another browser, your Internet Explorer favorites totally replace the favorites or cookies of the other browser. If you import favorites from another browser, the imported favorites are added to your existing Internet Explorer favorites list.
6. Click Next and then click Finish.

Exporting favorites and cookies is also a convenient way of backing them up in case you ever have to reinstall Windows. Because the export file is in HTML format, you can also use your favorites backup as your home page. Then, every time you open an Internet Explorer window, all your favorites are displayed.

Using AutoComplete

AutoComplete is a Windows 2000 feature that remembers entries you have used before and suggests them as you type in these places:

- An Address toolbar in Internet Explorer, Windows Explorer, the Windows desktop, or the Windows taskbar
- The Open dialog box from the File menu in Internet Explorer
- Forms on Web pages
- The Run dialog box (which works like the Open dialog box in Internet Explorer)

AutoComplete offers its services in one of two ways. With the default method, when you begin typing in one of the text boxes just described, a drop-down list appears with entries that match the characters you type. As you continue typing, the list of matching entries becomes shorter. To select an item from the list, press the Down Arrow key until that item is highlighted and press Enter. This AutoComplete drop-down list also appears when you click in a form text box and press the Up or Down Arrow key or double-click in a form text box. The list is available only if AutoComplete determines that it might have matches for the form field you are entering.

Internet Explorer also incorporates the inline AutoComplete method used in Internet Explorer 4. When inline AutoComplete is active and you begin typing in one of the text boxes, AutoComplete guesses the next characters based on your previous matching entries and inserts them inline; that is, the text is inserted where you would have typed it. The inserted text is highlighted. If it is incorrect, continue typing and the highlighted text goes away. If it is correct, press Tab to move to the end of the inserted text. At this point, you can continue typing and AutoComplete once again guesses subsequent text. Inline AutoComplete, which does not work with Web page forms, is disabled by default. To enable it, select Use Inline AutoComplete (under Browsing) on the Advanced tab of the Internet Options dialog box.

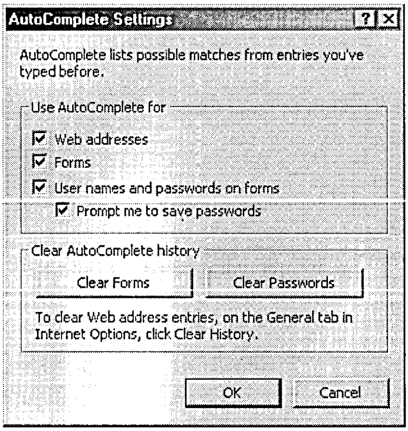
You can enable both forms of AutoComplete at the same time, but doing so is more confusing than helpful.

Note

Internet Explorer has an AutoCorrect feature that corrects common misspelling in the Address bar. Such mistakes as *htp://*, *http:\\*, and *ww.microsoft.com* are automatically fixed after you finish typing and press Enter.

You configure AutoComplete in Internet Explorer with separate options for storing Internet addresses, form entries, and user names and passwords on forms. Internet Explorer handles form entries for user names and passwords separately from other form entries, such as names and addresses.

To configure the Internet Explorer default AutoComplete, click AutoComplete on the Content tab. The AutoComplete Settings dialog box opens, as shown in Figure 26-14. Enable or disable each of the three options by selecting or clearing its respective check box. If you configure AutoComplete for user names and passwords, you can also configure it to prompt you to confirm each time it is about to store a user name/password pair.



AutoComplete lists possible matches from entries you've typed before.

Use AutoComplete for

- ☑ Web addresses
- ☑ Forms
- ☑ User names and passwords on forms
  - ☑ Prompt me to save passwords

Clear AutoComplete history

To clear Web address entries, on the General tab in Internet Options, click Clear History.

Figure 26-14
Open this dialog box from the Content tab in Internet Options.

Using the AutoComplete Settings dialog box, you can also clear all the stored form entries or all the stored password entries by clicking Clear Form or Clear Passwords. You can delete individual entries from any list when the drop-down list is displayed by clicking the entry you want to remove and pressing Delete.

Note The data that AutoComplete uses to generate matches is stored in encrypted files. Web sites have access only to the data that is actually entered on forms, not the data that is stored in these files.

Selecting Language Encoding

Encoding refers to the character set used to display a language. The United States uses the Western European character set, which contains the letters and symbols for English, French, Spanish, and Italian. To view a Web page that's encoded in another character set, you need to select that character set.

To do so, choose Encoding from the View menu and then select from among the installed character sets. To see a list of all the character sets available in Internet Explorer, choose View | Encoding | More. If you choose an uninstalled character set, the install-on-demand feature prompts you to install it.

Setting Advanced Options

The Advanced tab in the Internet Options dialog box provides a number of options for customizing Internet Explorer. Table 26-1 describes these options. Note that most of the "Don't show this dialog box again" settings are controlled by options on the Advanced tab.

Table 26-1. Options on the Advanced Tab

Option	Description
Accessibility	
Always expand ALT text for images	Expands a picture box if necessary to display all the alternate text for an image. (If the Show Pictures option in the Multimedia section is cleared, Internet Explorer displays alternate text—usually a caption or a description of a picture—in the space allocated for the picture.)
Move system caret with focus/selection changes	Specifies that the system caret always follows the selection. This affects some screen magnifiers and screen readers, which focus on the area around the system caret.
Browsing	
Always send URLs as UTF-8	Specifies that Internet Explorer use the UTF-8 character format for URLs. UTF-8 is an expanded format allowing for translation of characters in any language.
Automatically check for Internet Explorer updates	Directs Internet Explorer to automatically check for updates approximately every 30 days, notify you if one is available, and ask whether you want to download it. The default URL and refresh rate can be changed using a configuration file created by the IEAK Profile Manager.
Close unused folders in History and Favorites	Reduces clutter in the History and Favorites bars by closing the open folder when you select another folder.
Disable script debugging pages.	Turns off debugging warnings for errors on Web

(continued)

Table 26-1. Options on the Advanced Tab *(continued)*

Option	Description
Browsing *(continued)*	
Disable a notification about every script error	Prevents error message dialog boxes from being displayed when a page has a script error. A warning is displayed in the toolbar. Double-clicking this warning opens the error message dialog box.
Enable folder view for FTP sites	Allows Internet Explorer to display FTP sites using the Windows Explorer layout. If you are connecting through an FTP proxy, you might be limited to viewing and downloading files if this option is selected. *See "Using FTP Folders," page 438.*
Enable Install On Demand	Directs Internet Explorer to automatically download and install the Web components needed to display a page properly. See *msdn.microsoft.com/workshop/author/behaviors/reference/methods/installable.asp* for a list of components that do not install on demand in Windows 2000.
Enable offline items to be synchronized on a schedule	Allows offline Web content to be synchronized on a schedule. If this option is cleared, scheduled Web page synchronization tasks are ignored, and the following icon is displayed in the taskbar notification area when a scheduled synchronization has been skipped:
Enable page hit counting	Allows Web sites to create a log of which pages you view on the sites, even when you work offline. This log is stored on your computer and uploaded whenever you visit the sites online.
Enable page transitions	Allows Web sites to use multimedia transitions from one page to another.
Enable Personalized Favorites Menu	Specifies that only recently viewed favorites appear on the Favorites menu. To display the "hidden" items, click the arrow at the bottom of the menu, or simply wait a few seconds. This setting controls only the Favorites menus in Internet Explorer and Windows Explorer; the Use Personalized Menus option in the Taskbar And Start Menu Properties dialog box controls the Favorites menu (and other submenus) on the Start menu.
Notify when downloads complete	Displays a message announcing the completion of a complete file download.

(continued)

Table 26-1. Options on the Advanced Tab *(continued)*

Option	Description
Browsing *(continued)*	
Reuse windows for launching shortcuts	Directs Internet Explorer to use an existing window when you take one of the following actions: • Double-click an Internet shortcut from within Windows Explorer • Open a URL by clicking Start | Run • Use a desktop toolbar, such as the Address or Links bar If this option is cleared, a new instance of Internet Explorer opens when you take one of these actions.
Show friendly HTTP error messages	Displays a message with a description of the problem and suggestions for resolution when a Web page cannot be located or displayed. If this option is cleared, the standard HTTP message is displayed.
Show friendly URLs	Determines the appearance of addresses in the status bar when you point to a link. A "friendly" address includes only the part of a URL following the last slash (/).
Show Go button in Address bar	Displays the Go button at the right end of the Address bar. Clicking the Go button has the same effect as pressing Enter while the Address bar is active.
Show Internet Explorer on the desktop	Displays the Internet Explorer icon on the desktop. If you want to delete the icon, clear this check box.
Underline links	Specifies whether you want text links to be underlined always, never, or only when you hover the mouse pointer over the link.
Use inline AutoComplete	Enables Internet Explorer 4–style AutoComplete in which entries are completed as you type.
Use smooth scrolling	Disables the accelerated scroll mode when you click and hold the scroll buttons. You might want to clear this option if you use Accessibility features and experience problems with them.
HTTP 1.1 settings	
Use HTTP 1.1	Directs Internet Explorer to attempt to use the enhanced features of the latest version of HTTP when connecting to Web sites. Many sites still use HTTP 1.0; if you have trouble connecting, try clearing this check box.

(continued)

Table 26-1. Options on the Advanced Tab *(continued)*

Option	Description
HTTP 1.1 settings *(continued)*	
Use HTTP 1.1 through proxy connections	Directs Internet Explorer to attempt to use HTTP 1.1 even when using a proxy connection.
Microsoft VM	
Java console enabled (requires restart)	Enables the Java console for testing Java programs and applets. Open the Java console from the View menu.
Java logging enabled	Directs Internet Explorer to create a log of all Java program activity. This log is useful for security and troubleshooting.
JIT compiler for virtual machine enabled (requires restart)	Enables the Just-in-Time compiler to translate Java bytecode to native machine code. A link is created between the bytecode and compiled machine code. If this option is cleared, Java applications always run in the Internet Explorer Java interpreter.
Multimedia	
Always show Internet Explorer (5.0 or later) Radio toolbar	Enables the Radio toolbar when Internet Explorer is started. You can display the Radio toolbar for a single session by right-clicking the toolbar and choosing Radio.
Play animations	Directs Internet Explorer to play animations when pages are displayed. When this option is cleared, you can still play an individual animation by right-clicking the animation's icon and then choosing Show Picture.
Play sounds	Directs Internet Explorer to play music and audio clips, which can be slow. Clear this option to display pages more quickly or if you don't have a sound card.
Play videos	Directs Internet Explorer to play video clips, which can be slow. Clear this option to display pages more quickly.
Show image download placeholders	Directs Internet Explorer to draw a placeholder for images while they are downloading. This causes the page to display in its correct layout even before the images complete downloading.
Show pictures	Directs Internet Explorer to download and display all images, which can be slow. Clear this option to display pages more quickly. If this option is cleared, Internet Explorer displays any alternate text accompanying the images.

(continued)

Table 26-1. Options on the Advanced Tab *(continued)*

Option	Description
Multimedia *(continued)*	
Smart image dithering	Specifies the use of additional processing time to smooth images.
Printing	
Print background colors and images	Includes background images when you print the page.
Search from the Address Bar	
When searching	The following four options determine what happens when you perform a search from the Address bar. Configure the Address bar search by clicking Customize at the top of the Search bar and then clicking Autosearch Settings.
Display results, and go to the most likely site	Displays the Search bar with search results and displays the page most closely matching your request.
Do not search from the Address bar	Prevents searching from the Address bar.
Just display the results in the main window	Displays search results in the main window, not on the Search bar.
Just go to the most likely site	Displays the page most closely matching your request. Other search results are not displayed.
Security	
Check for publisher's certificate revocation	Directs Internet Explorer to check a software publisher's certification authority to see whether the program's certificate has been revoked before the certificate is accepted. *See "Understanding Digital Certificates," page 440.*
Check for server certificate revocation (requires restart)	Directs Internet Explorer to check a site's certification authority to see whether the site's certificate has been revoked before it is accepted.
Do not save encrypted pages to disk	Prevents pages from a secure or encrypted site from being stored on your hard disk.
Empty Temporary Internet Files folder when browser is closed	Specifies that the Temporary Internet Files folder is emptied when you close the program.
Enable Profile Assistant	Directs Internet Explorer to respond to Web sites' requests for Profile Assistant information. (Internet Explorer always asks your permission before sending any information to a new site.) *See "Using Profile Assistant," page 445.*

(continued)

Table 26-1. Options on the Advanced Tab *(continued)*

Option	Description
Security *(continued)*	
Use Fortezza	Enables the Fortezza cryptographic service provider (CSP) plug-in. To use the Fortezza CSP plug-in, users must have the necessary Fortezza hardware and CSP installed.
Use PCT 1.0	Allows you to send and receive secure information using PCT (Private Communications Technology), a Microsoft-proprietary protocol that's more secure than SSL 2.0.
Use SSL 2.0	Allows you to send and receive secure information using SSL (Secure Sockets Layer) 2.0, the standard protocol for secure transmissions.
Use SSL 3.0	Allows you to send and receive secure information using SSL 3.0, a newer protocol for secure transmissions that is not yet supported by many Web sites.
Use TLS 1.0	Allows you to send and receive secured information through TLS (Transport Layer Security), an open security standard similar to SSL 3.0. Note that some Web sites might not support this protocol.
Warn about invalid site certificates	Displays a warning if the address in a certificate is not valid.
Warn if changing between secure and not secure mode	Displays a warning when you go from a secure site to an unsecure site.
Warn if forms submittal is being redirected	Displays a warning if you submit information via a Web-based form and the information is addressed to a Web site other than the one where you enter the information.

Adding Microsoft Web Accessories

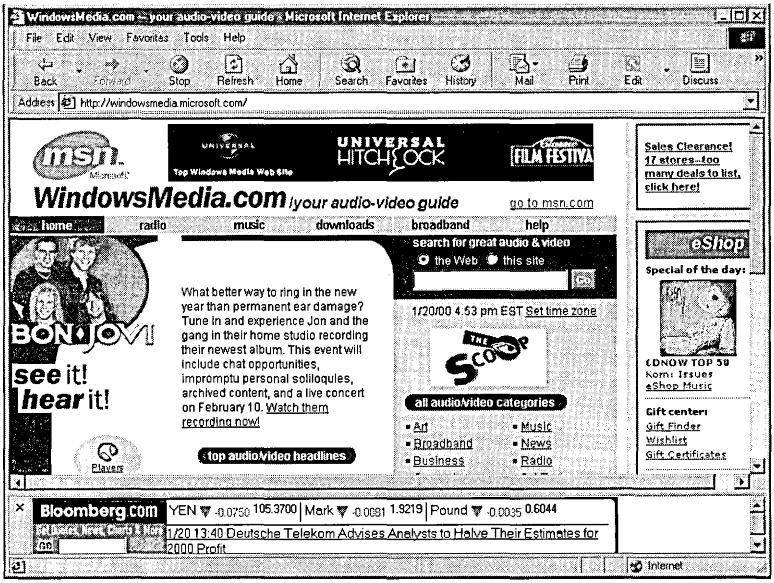
Internet Explorer expands the extensibility introduced in Internet Explorer 4 as PowerToys. You can find add-ins at the Microsoft Web Accessories Web page, which offers additional Explorer bars (discussed in the next section) and Internet Explorer extensions (including one called Web Accessories). The Microsoft Web Accessories Web page (*www.microsoft.com/windows/ie/WebAccess*) includes the following extensions provided by Microsoft:

- **Internet Explorer 5 Web Accessories.** A selection of useful utilities for Internet Explorer 5 including quick search, zoom in/zoom out, list links, and text highlight.
- **Microsoft Internet Explorer 5 Power Tweaks Web Accessories.** A set of utilities including an Online/Offline toolbar button, Tools menu commands for adding sites to security zones, and a copy command for URLs on a Web page.
- **Microsoft Web Developer Accessories.** Two tools for examining the code behind a Web page.

To install a Web accessory, download its installation file and then run it. You will need to close all Internet Explorer windows to complete the installation. To remove a Web accessory, use Control Panel | Add/Remove Programs.

Using Other Explorer Bars

Internet Explorer uses the Explorer bar technology as a means of extending its capabilities through additional Explorer bars provided by Microsoft and third parties. These additional Explorer bars provide information such as news headlines or stock quotes. Microsoft maintains a list of some third-party Explorer bars on its Web Accessories page (*www.microsoft.com/windows/ie/WebAccess*). Figure 26-15 shows an Internet Explorer window with the Bloomberg Explorer bar (at the bottom of the window) displaying stock quotes and news from the Bloomberg Web site. Real.com adds its own Explorer bar when you install one of its products. Expect to see many more companies offering their own Explorer bars as the usefulness of these bars becomes better recognized.



What better way to ring in the new year than permanent ear damage? Tune in and experience Jon and the gang in their home studio recording their newest album. This event will include chat opportunities, impromptu personal soliloquies, archived content, and a live concert on February 10. Watch them recording now!

1/20/00 4:53 pm EST Set time zone

YEN ▼ -0.0750 105.3700 | Mark ▼ -0.0081 1.9219 | Pound ▼ -0.0035 0.6044

1/20 13:40 Deutsche Telekom Advises Analysts to Halve Their Estimates for 2000 Profit

Figure 26-15
Additional Explorer bars enhance Internet Explorer functionality.

Note According to Microsoft documentation, you should be able to install Web accessories and new Explorer bars by choosing Windows Update from the Tools menu in Internet Explorer. However, this command opens the Windows Update page, which does not provide information on Internet Explorer extensions. You will be better off going directly to the Web Accessories page at *www.microsoft.com/windows/ie/WebAccess* or downloading from an accessory creator's Web site.

To use a new Explorer bar, simply download the bar and run the setup executable. Close all Internet Explorer windows and then restart Internet Explorer to complete the installation. After it has been installed, your new Explorer bar is available from the View | Explorer Bar command, as shown in Figure 26-16. You can also add a button for the new Explorer bar to the Standard Buttons toolbar. *For more information, see "Customizing the Internet Explorer Toolbar," page 448.* To uninstall an Explorer bar you no longer want, use Control Panel | Add/Remove Programs.

Chapter 27

Managing a Web Server

In This Chapter

Installing Internet Information Services 464

Using IIS 465

Managing Security on Your Site 472

Redirecting Requests to the Site 482

Using Content Ratings 482

Running an FTP Server 482

Using Your Web Site for Collaboration (WebDAV) 483

Setting Up IIS for Internet Printing 483

Microsoft Windows 2000 Professional supplies you with ample tools for hosting Web and FTP sites. The primary tool is Internet Information Services (IIS) 5. IIS 5 provides a Web server, a File Transfer Protocol (FTP) server, and a Simple Mail Transfer Protocol (SMTP) virtual server. You might already be familiar with IIS; IIS 4 is a part of Microsoft Windows NT Server, and a scaled-down version of IIS, Personal Web Server (PWS), is included with Windows 98. IIS 5 (the version supplied with Windows 2000) contains FrontPage Server Extensions, which allow your Web server to make use of the added Web site capabilities offered by Microsoft FrontPage.

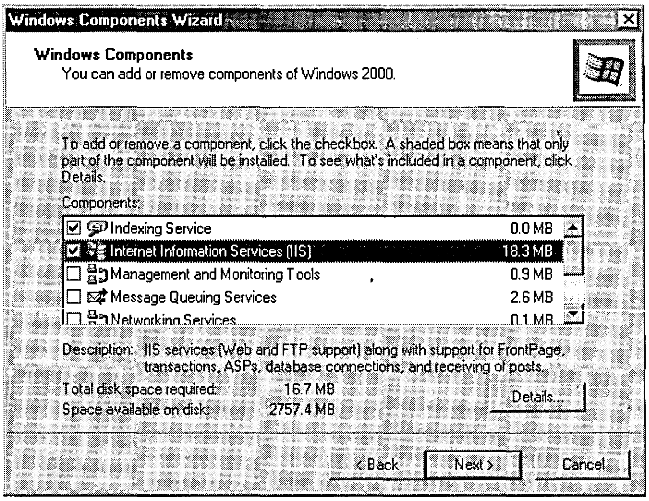
Windows 2000 also provides extensive security capabilities for Internet servers through user accounts, NTFS, and Group Policy settings.

Note IIS 5 in Windows 2000 Professional is limited to 10 simultaneous connections. This limitation can be even more severe than it seems because a single browser window might require multiple connections to the Web server. Although the connection limit precludes using Windows 2000 Professional as a Web server for a heavily used public Internet site, IIS in Windows 2000 Professional can be very useful in your organization. First, if you're a Web developer, IIS provides a Web server that you can use for testing your creations before uploading them to a larger server. Second, organizations of any size can use IIS to manage an *intranet*, a network that works much like the public Internet. (You browse an intranet with a Web browser, which displays HTML pages. The main difference is that an intranet is not accessible to the outside world.) And if you really do have a low-traffic site—perhaps the only visitors are your grandparents, who want to see the new baby photos—you can use IIS to host an Internet site. To go beyond the 10-connection limit, you must use Microsoft Windows 2000 Server.

Installing Internet Information Services

IIS is not installed by default unless you installed Windows 2000 Professional as an upgrade and PWS was installed on your previous system. To install IIS:

1. In Control Panel, open Add/Remove Programs.
2. Click Add/Remove Windows Components.
3. In the Windows Components Wizard, select Internet Information Services (IIS), as shown in Figure 27-1. Click Next to finish the installation.



Windows Components Wizard

Windows Components
You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Indexing Service	0.0 MB
☑	Internet Information Services (IIS)	18.3 MB
□	Management and Monitoring Tools	0.9 MB
□	Message Queuing Services	2.6 MB
□	Networking Services	0.1 MB

Description: IIS services (Web and FTP support) along with support for FrontPage, transactions, ASPs, database connections, and receiving of posts.

Total disk space required: 16.7 MB
Space available on disk: 2757.4 MB

Figure 27-1
Use the Windows Components Wizard to install IIS.

Note If the volume on which you install IIS is not formatted using NTFS, you will not be able to restrict access to your Web pages to authors and administrators. Anyone can create and edit Web files on your Web server.

When you install IIS, the Internet Information Services snap-in is registered on your system and added to the Computer Management console (under Services And Applications). The FrontPage Server Extensions are also installed, although you must complete their configuration before you can use them on a Web. *See "Configuring FrontPage Server Extensions," page 468.*

Using IIS

IIS manages the folders that make up the sites served by your Web server. All the tools necessary to run IIS are available within the Internet Information Services snap-in.

Viewing the IIS Documentation
The IIS installation places the IIS documentation on your Web site (actually, in %SystemRoot%\Help\Iishelp, with a virtual directory on your Web site) so that you can access it with any Internet browser. Open *localhost/iishelp* to view the documentation.

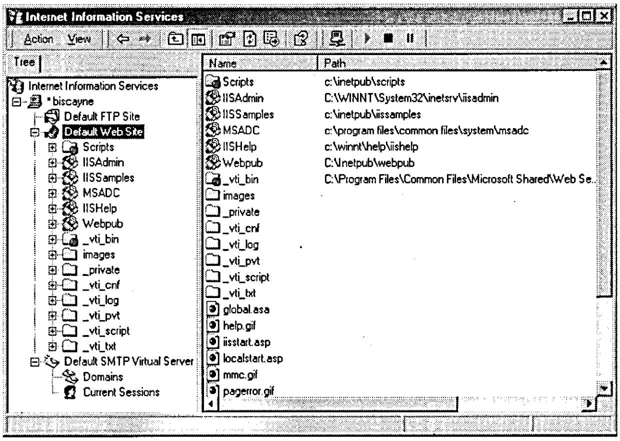
Using the Internet Information Services Snap-In

You control IIS using the Internet Information Services snap-in for Microsoft Management Console (MMC). You can avoid the clutter of the Computer Management console and open the Internet Information Services console in its own window by choosing Start | Settings | Control Panel | Administrative Tools | Internet Services Manager. See Figure 27-2. *For information about MMC, see Chapter 4, "Using and Customizing Microsoft Management Console."*

The Internet Information Services console operates on your local computer by default but allows connections to other computers, assuming that appropriate permissions are set. Each computer shown has entries for the default Web site, default FTP site, and default SMTP virtual server, the three components offered by IIS in Windows 2000 Professional.

Home Directories and Virtual Directories

Much of IIS has to do with managing directories. (*Directory* is the traditional name for what is now usually called a *folder*. As you'll see throughout Windows 2000, some



Name	Path
Scripts	c:\inetpub\scripts
IISAdmin	C:\WINNT\System32\inetsrv\iisadmin
IISSamples	c:\inetpub\iissamples
MSADC	c:\program files\common files\system\msadc
IISHelp	c:\winnt\help\iishelp
Webpub	C:\Inetpub\webpub
_vti_bin	C:\Program Files\Common Files\Microsoft Shared\Web Se...
images	
_private	
_vti_cnf	
_vti_log	
_vti_pvt	
_vti_script	
_vti_txt	
global.asa	
help.gif	
iisstart.asp	
localstart.asp	
mmc.gif	
pagerror.gif	

Figure 27-2
You can manage IIS from the Internet Information Services console.

old terms linger—and in IIS, *directory* is the most-used term.) Directories are used in IIS for three tasks:

- Organizing Web site (and FTP site) files (as described in this section)
- Applying security and permissions *(see "Managing Security on Your Site," page 472)*
- Configuring FrontPage extensions *(see "Configuring FrontPage Server Extensions," page 468)*

You need to keep in mind three kinds of directories: server home directories, site home directories, and virtual directories. Your Web server has a home directory, sometimes called the *root directory,* which serves as the starting point for everything else you serve. By default, the server's home directory is C:\Inetpub\Wwwroot. You can change this directory by opening the properties of the Default Web Site and clicking the Home Directory tab.

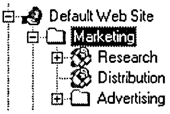
Each Web site served by IIS also has a home directory. Typically, when you create a Web site to be served on your computer, you organize its files using a folder hierarchy. The highest-level folder will be the home directory for that Web site.

You can store each Web site's home directory under your server's root folder—but you don't have to. Home directories can reside anywhere on your computer or anywhere else on your intranet. If you store these home directories somewhere other than the server's root directory, however, you need to create a virtual directory under the root directory that points to the folder containing the Web site. There is a slight security advantage to using virtual directories; their use hides the physical location of your files.

For example, say that you work in the marketing department of your company and have been asked to create and maintain a marketing Web site. The IT people at your company are sometimes hard to deal with, so you decide to host the Web site on your computer at your desk (a computer that is running Windows 2000 Professional). As you design your site, you realize that it needs three main components: Research, Advertising, and Distribution. This is fine, except that the people who handle all the distribution issues work in another building and want to control that part of the marketing Web site themselves. Fortunately, IIS running on your computer can handle what you need to do. However, IIS running in Windows 2000 Professional is limited to 10 simultaneous connections. Thus, this example is relevant only if the site is lightly used.

When you add a Web or a subweb using the Internet Information Services snap-in, you must create its root folder first. So your initial step in setting up your marketing site is to use Windows Explorer to create a Marketing folder in the server home directory. Then you can create a subfolder under Marketing called Advertising. You decide to keep all Web files for the Research segment of your Web site in C:\Research, where all your other research files are stored. The distribution people have created a shared folder on their computer named Distribution. Now the folders are ready; you need to let IIS know what is going on.

IIS automatically detects the folders you create in the server home directory. If you have the Internet Information Services snap-in open when you create the folders, you need to refresh Default Web Site. In our example scenario, you would see the Marketing folder under Default Web Site. When you open the Marketing folder, you would see the Advertising folder. You create virtual directories for the other two folders. Select the Marketing folder and choose Action | New | Virtual Directory. The Virtual Directory Creation Wizard starts. Follow the wizard to select the Research and Distribution folders. For the shared Distribution folder on the networked computer, you need to supply a user name and password for accessing that folder. After you've created these virtual folders, your Internet Information Services snap-in will look something like this:



Even though the physical folders are distributed around your network, IIS makes the URLs uniform. Table 27-1 shows the relationship between the location of your files and the corresponding URLs, assuming that

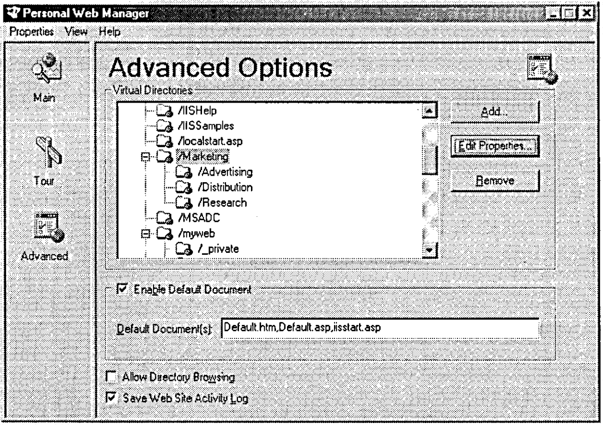
- Your computer's name is Frodo
- The distribution department computer's name is Mecury
- Your server home directory is C:\Inetpub\Wwwroot

Table 27-1. Example URLs

Physical Location	URL
C:\Inetpub\Wwwroot\Marketing	http://Frodo/Marketing
C:\Research	http://Frodo/Marketing/Research
C:\Inetpub\Wwwroot\ Marketing\Advertising	http://Frodo/Marketing/Advertising
\\Mecury\Distribution	http://Frodo/Marketing/Distribution

Using Personal Web Manager

When you install IIS 5 on a computer running Windows 2000, Microsoft Personal Web Manager is also installed. Personal Web Manager is the user interface associated with Personal Web Server in Windows 98. In Windows 2000, it offers a limited, but more user-friendly, control mechanism for IIS 5. To open Personal Web Manager, click Start | Settings | Control Panel | Administrative Tools | Personal Web Manager. The Advanced Options page of Personal Web Manager is similar to the Internet Information Services snap-in. On the Advanced Options page, you can create new virtual directories and set certain permissions. You cannot configure secure connections or authentication modes other than Anonymous. Personal Web Manager is useful for novice users, but advanced users will find it limiting.



Advanced Options

Virtual Directories

```
/IISHelp
/IISSamples
/localstart.asp
/Marketing
    /Advertising
    /Distribution
    /Research
/MSADC
/myweb
    /_private
```

☑ Enable Default Document

Default Document(s): Default.htm,Default.asp,iisstart.asp

☐ Allow Directory Browsing

☑ Save Web Site Activity Log

Configuring FrontPage Server Extensions

FrontPage is Microsoft's Web site authoring and management program, which is available either as part of Microsoft Office 2000 or separately. FrontPage includes a number of "extensions" that extend the basic HTML capabilities for Web site functionality, Web site authoring, and Web site administration. These extended capabilities include the following:

- **Web site functionality.** Interactive discussion groups, hit counters, search forms
- **Web site authoring.** Automatic maintenance of hyperlinks, generation and maintenance of navigation bars, and automatic page formatting
- **Web site administration.** Permission control, Web site publishing

Note The Windows user interface sometimes calls these extensions FrontPage Server Extensions and at other times calls them Windows Server Extensions. They are, however, the same extensions.

The FrontPage Server Extensions provide the server-side support for these FrontPage capabilities. In order to take advantage of the extensions you use when creating a site with FrontPage, the server hosting the site must run the server extensions. FrontPage Server Extensions are installed by default when you install IIS, but you must run the Configure Server Extensions Wizard to complete the installation.

To run the wizard, select Default Web Site in the Internet Information Services console and then choose Action | All Tasks | Configure Server Extensions. If you have installed IIS on an NTFS volume, you are given the opportunity to set up some Windows security groups to be used by IIS for controlling access to Web pages. By default, three groups are used: *hostname* Admins, *hostname* Authors, and *hostname* Browsers. The wizard also allows you to select a group or user to administer the server. The final wizard page sets up the Webmaster e-mail identity. Completing the wizard completes the installation of the FrontPage Server Extensions.

Note Detailed documentation for FrontPage Server Extensions can be found in the FrontPage Server Extensions Resource Kit (SERK). You can download the FrontPage SERK from *officeupdate.microsoft.com/2000/downloadDetails/Fp2kserk.htm* or view it online at *officeupdate.microsoft.com/frontpage/wpp/serk.*

After you complete the wizard, you should add users to the new groups you have created. Open the Computer Management console and select System Tools\Local Users And Groups\Groups. Double-click the group in the details pane and then click Add. Select users from the list, or select a domain controller from the Look In list to add domain users. *For information about the Local Users And Groups snap-in, see "Local Users And Groups MMC Snap-In," page 487.*

But wait, there's more. You need to apply the extensions to individual Web sites. Whenever you create a new Web site on your server that needs FrontPage Server Extensions, you must configure the extensions for that site. The steps are essentially the same as configuring the extensions for the server. In the Internet Information Services snap-in, select the home directory icon for the site where you want to enable server extensions, and then select Action | All Tasks | Configure Server Extensions.

The New Subweb Wizard appears. The only question you must answer in this wizard is whether you want to use the same administrator as the parent Web uses. You'll want to set up a different administrator if someone else will administer the site and you don't want that person to have administrator access to the rest of the Web server. If you select Use A Different Administrator For This Web, you are also asked to allow the wizard to create a new Windows group to use for the Web. Consenting creates *webname* Admins, *webname* Authors, and *webname* Browsers groups. If you manage this Web site separately (for example, the Distribution subweb in our previous example), it is a good idea to create these separate groups.

Although you can handle all the configuration of FrontPage Server Extensions through the Internet Information Services snap-in, IIS includes three other extension administration tools: the FrontPage Server Extensions snap-in; Fpsrvadm.exe and Fpremadmexe command-line utilities; and FrontPage Server Extensions HTML Administration Forms.

You can reach the FrontPage Server Extensions snap-in by going to Start | Settings | Control Panel | Administrative Tools | Server Extensions Administrator. This snap-in, which you can use in any management console, has essentially the same functionality relative to the server extensions as the Internet Information Services snap-in, except that it is arranged slightly differently. (In yet another example of inconsistency, the snap-in is called FrontPage Server Extensions in some contexts and Microsoft Server Extensions in others. The two names refer to the same snap-in.)

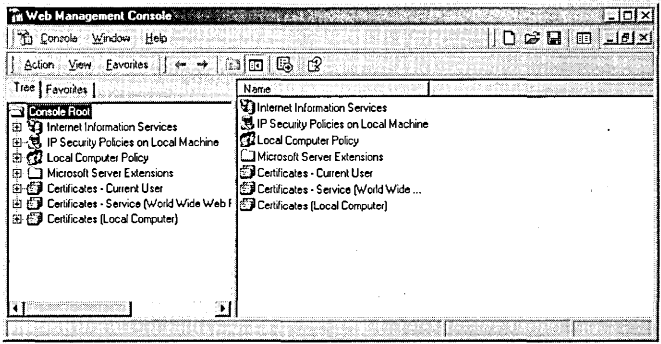
The FrontPage Server Extensions installation includes two command-line utilities for administering extensions. Fpsrvadm.exe offers a complete set of FrontPage Server Extensions operations and runs on the server computer. Fpremadm.exe is similar to Fpsrvadm, but it administers extensions running on a remote computer. You will find these utilities in %CommonProgramFiles%\Microsoft Shared\Web Server Extensions\40\Bin.

The FrontPage Server Extensions HTML Administration Forms are HTML pages that can be used to remotely install and administer the FrontPage Server Extensions from a Web browser on any computer connected to the Internet. These forms are copied to your Web server's hard drive as a part of the FrontPage Server Extensions setup. To use these forms on your Web server from any computer connected to the Internet, you must create a virtual directory with proper authentication and access control that points to %CommonProgramFiles%\Microsoft Shared\Web Server Extensions\40 \Admisapi. It is important that you set NTFS permissions for the folder and access and authentication permissions for the Web site. Remove all access to this folder for all user accounts except those authorized to manage your server remotely.

Note You can remove FrontPage Server Extensions from a Web site that is currently configured to use them. In the Internet Information Services snap-in, right-click the home directory icon for the site you want to convert. Select All Tasks | Convert Server Extensions Web To Directory.

Creating a Web Management Console

MMC technology allows you to create a single management console that groups similar activities. Several MMC snap-ins would be useful in a single console for managing the various aspects of your Web server. The illustration that follows shows a console with snap-ins for Internet Information Services, IPSec, Local Computer Policy, Microsoft Server Extensions, and the three levels of certificate management. *For information about creating a console like this one, see Chapter 4, "Using and Customizing Microsoft Management Console."*


Web Management Console
Console Window Help
Action View Favorites
Tree Favorites
Console Root
Internet Information Services
IP Security Policies on Local Machine
Local Computer Policy
Microsoft Server Extensions
Certificates - Current User
Certificates - Service (World Wide Web F
Certificates (Local Computer)
Name
Internet Information Services
IP Security Policies on Local Machine
Local Computer Policy
Microsoft Server Extensions
Certificates - Current User
Certificates - Service (World Wide ...
Certificates (Local Computer)

You can also create a separate console for one Web or subweb on your server. If someone other than the server administrator needs Administrator access to one Web site but not to the whole Web server, you should create a console for just that Web or subweb. The easiest way to do this is from a console with the Internet Information Services snap-in: Navigate to the Web for which you want a separate console, right-click its icon, and select New Window From Here. Then choose Save As from the Console menu to save this new view as a new console. You can also change the new console's name by choosing Options from the Console menu.

Changing the Home Page

IIS uses C:\Inetpub\Wwwroot as the default home directory. You can change that location if you wish. In the Internet Information Services snap-in, right-click Default Web Site and choose Properties. Click the Home Directory tab and click Browse next to the Local Path text box. Navigate to the folder that you want to use as the home directory.

Managing Security on Your Site

In the following sections, we describe four elements of IIS security:

- **Authentication.** Controlling who gains access to your site
- **Access Control.** Controlling which resources (files) users are allowed to access
- **Encryption.** Securing the data link between your server and the client
- **Auditing.** Monitoring server activity to detect potential vulnerabilities or past infractions

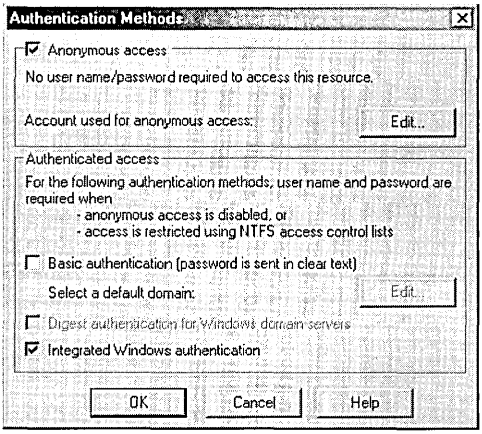
Authentication

Authentication is the process of ensuring the identity of users of your Web site. It is analogous to the process of logging on to your computer or domain. IIS authentication works hand-in-hand with Windows authentication and NTFS file security. You can enable and configure four methods of authentication, each of which can be modified by requiring secure links, client certificates, or both. *For details, see "Encryption," page 474.*

- **Anonymous authentication.** Anyone can access the files on your Web server without supplying a user name and password. If you are setting up a public Web server, this is the authentication method you should use.
- **Basic authentication.** Only someone with a user name and password can access your Web site. The user name and password are sent as plain text over the network and could be intercepted.
- **Digest authentication.** Only someone with a user name and password can access your Web site. The user name and password are sent across the network as a hash value that is not feasible to decipher. Digest authentication is available only on domains with a Windows 2000 domain controller using Active Directory and does not work with Microsoft Internet Explorer 4.
- **Integrated Windows authentication.** Only someone with a user name and password can access your Web site. Hashing technology is used to identify your user without actually sending the password over the network Integrated Windows authentication works only with the Internet Explorer browser and does not work through proxy servers.

For all but the first method, you must have appropriate accounts set up on your computer or your network's domain controller. Anonymous authentication uses an existing user account. It is also a good idea to create a Windows user group with permissions tailored to your Web users. You also have access to the security features of NTFS (if your sites' home directories are on NTFS partitions.) *For information on securing files and folders, see Chapter 32, "Using the NTFS File System."*

You enable one or more of the four authentication methods in the properties dialog box for the site's home directory. On the Directory Security tab, click Edit in the Anonymous Access And Authentication Control box. The Authentication Methods dialog box opens, containing options for each of the authentication methods. (See Figure 27-3.) You can select any or all of the available options. Digest authentication is available only if the domain controller on your network is running Windows 2000 Server. If you select Anonymous Access and one or more authenticated methods, the authenticated methods are used only if anonymous access fails or if access to files and directories is restricted by NTFS permissions. IIS attempts to use digest authentication and integrated Windows authentication before falling back to basic authentication.



☑ Anonymous access

No user name/password required to access this resource.

Account used for anonymous access:

Authenticated access

For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Basic authentication (password is sent in clear text)

Select a default domain:

☐ Digest authentication for Windows domain servers

☑ Integrated Windows authentication

Figure 27-3
You can select the methods of authenticating users of your Web site.

All access to your Web site is controlled by user accounts. Even anonymous authentication uses an account for all user access. When IIS is installed on your computer, an account named IUSR_*computername* is automatically created. Anonymous authentication uses this account for all users of your Web site unless you reconfigure it. To change the account used by anonymous authentication, click Edit in the Anonymous Access section of the Authentication Methods dialog box.

You should develop at least an informal account policy for the Web sites you serve. If you require an authentication method, users need to have accounts established. You can create one account per Web site or one account per user. Using Group Policy settings and NTFS, you can create specialized permissions as appropriate for your server.

Access Control

After a user has established a connection with your Web server, he or she still needs access permission to files and folders on your server. This access is controlled by

NTFS permissions. You can set NTFS permissions for individual folders or files by user or by group. *For more information, see Chapter 32, "Using the NTFS File System."*

Within the Internet Information Services snap-in, you can set permission by using the Permissions Wizard. This wizard provides three options for setting permissions on folders:

- Inherit the permissions of the parent folder
- Apply a set of permissions appropriate for a public Web site
- Apply a set of permissions appropriate for a secure Web site

The primary difference between the public and secure permissions is that anonymous logins are allowed on public sites. Otherwise, the same read and execute permissions are set. To run the wizard, select a folder in the Internet Information Services snap-in and choose Action | All Tasks | Permissions Wizard.

Encryption

A communication link between a Web browser and a Web server is secured by the use of encryption. IIS 5 uses Secure Sockets Layer (SSL) as the encryption protocol on secure links.

Secure communication and certificates are not very complicated, but the available information about these subjects is sparse, making them seem mystical. A further confusion is that certificates are used for two interrelated purposes. IIS uses certificates to support both authentication and secure communication links. *For an introduction to certificates, see "Using Digital Certificates," page 440.*

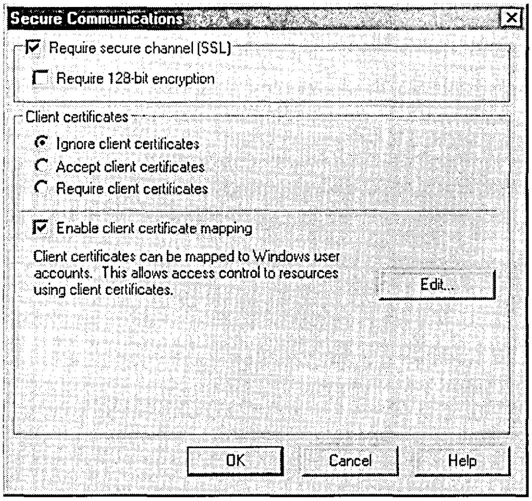
The discussion in Chapter 26 concerns certificates from the Web browser's point of view. Windows 2000 provides a user interface for managing certificates on your computer. *(For more information, see Chapter 35, "Managing Security Certificates.")* This section, however, discusses certificates as they concern running a Web server.

Certificates come in three flavors:

- **Server certificates** are used to identify servers to Web browsers and to supply the key for SSL encryption. Whenever a user connects to a page on your server using the HTTPS protcol (as opposed to HTTP), the server first identifies itself with its server certificate. After the browser accepts the certificate, an encrypted SSL connection is established using the server's private key at the server and public key at the browser. Note that two activities happen, each with different components of the server certificate. The certificate's identification information is used to identify the server to the client, and then the certificate's keys are used to create the encrypted SSL connection.

- **Client certificates** are used to identify Web browsers to servers. A secure site can require browsers to identify themselves with a client certificate as part of the authentication step.
- **Certification Authority (CA) certificates** provide the trust value for server and client certificates. Internet Explorer keeps a list of known and trusted CAs. When a user browses to a secure Web page, the Web server's server certificate is sent to the browser. The browser checks the CA that issued the server certificate. If the CA is in the list of trusted CAs, the certificate is accepted automatically. If the CA is not listed, a dialog box is displayed, giving the user the option of accepting or rejecting the certificate.

Most of the configuration settings for certificate use with Web servers are handled by the Secure Communications dialog box, shown in Figure 27-4. Open this dialog box for any object (file or folder) in the Internet Information Services snap-in by right-clicking the object's icon and choosing Properties. Select the Directory Security or File Security tab and then click Edit in the Secure Communications dialog box. If the Edit button is dimmed, you need to obtain and install a server certificate as we describe later in this chapter. *(See the sidebar "Obtaining a Server Certificate," page 481.)*



Secure Communications

☑ Require secure channel (SSL)

□ Require 128-bit encryption

Client certificates

● Ignore client certificates

○ Accept client certificates

○ Require client certificates

☑ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

Figure 27-4
You can manage the use of server and client certificates in creating secure communication links.

The Secure Communications dialog box contains two sets of controls. The first set controls whether the communication link for the selected object is required to be secure (SSL). The second set controls the use of client certificates in user authentication.

You enable an SSL connection by selecting Require Secure Channel (SSL) at the top of the Secure Communications dialog box. Making this selection requires that all connections to that resource (file if the object is a file, or all the files in the folder if the object is a folder) use SSL. This selection has three results. First, the browser must request a link to the resource using the HTTPS protocol. Second, the server must send its certificate to the browser for acceptance. Third, the server uses its private key to establish an encrypted link, which the browser decrypts with the server's public key.

Note SSL uses 40-bit encryption by default. You can require SSL to use the significantly more secure 128-bit encryption by selecting Require 128-Bit Encryption in the Secure Communications dialog box. For most uses, 40-bit encryption is sufficient. Some financial institutions use 128-bit encryption for certain transactions. Owing to export limitations that were only recently lifted, 128-bit encryption is not generally used outside the United States and Canada.

HTTP vs HTTPS

The format for a URL is *protocol://domainname/resource*. The domain name is the server hosting the resource. *(For information about domain names, see "Domain Name System," page 493.)* The resource is an optional part of the URL that identifies a particular file on the server that you want to access. The protocol indicates the set of communication standards used between the client and server computers. Examples of protocols are FTP, HTTP, HTTPS, and Telnet.

The protocol part of the URL performs an important task: it controls which port at the server is addressed. Each protocol addresses a different port and, in that way, the server knows which protocol to use in establishing a connection with the client. Thus when clients address a resource on your server using *https://*, they are addressing a different port than when they use *http://*. If you use packet filtering to control security on your computer, you need to open both ports 80 (HTTP) and 443 (HTTPS) to enable secure communication.

Using SSL considerably slows down a connection because of the encryption /decryption process. For this reason, you should restrict its use to only the resources that need it.

Note You can require SSL connections for a Web site by selecting Require Secure Channel (SSL) in the Secure Communications dialog box. In this case, users must enter the HTTPS URL format in their browser in order to connect to any page on the secure Web site. If, however, an SSL connection is not required, users still have the option of creating an SSL connection by using the HTTPs URL format when connecting to a Web site. This method works if the Web server has a server certificate installed, even if an SSL connection is not required.

You can set up a Web site to both use basic authentication and require an SSL communication link, as discussed previously. If you do so, an SSL link is made before authentication is performed. The user name and password are therefore transmitted encrypted. However, all user interaction with the Web site will use SSL and hence will run more slowly.

You can also configure a Web site for basic authentication without requiring an SSL link, and users can request an SSL link if they want to protect their password. The user has the option of addressing the Web site with either the HTTP or HTTPS URL format. If the HTTPS format is used and the Web server has a server certificate installed, an SSL link will be established. After an SSL link is established, all pages on the Web site will use the secure link. However, if the link was created by request, the user can manually change a URL from HTTPS to HTTP after authentication is complete, and the SSL link will be dropped.

The second section of the Secure Communications dialog box controls whether users are required to identify themselves with their own client certificates. These options modify the authentication methods discussed previously.

Client certificates can be used in place of user names and passwords in any of the authentication schemes requiring them. This is accomplished by mapping client certificates to Windows user accounts. If certificate mapping is used, when the client's certificate is received by the server, it is checked against the mapping and, if a corresponding user account exists, the user is logged on using that account.

Two ways of mapping certificates are available: one-to-one and many-to-one. In one-to-one mapping, each user's certificate is mapped to an account. The server must have an exact copy of each user's certificate to create the mappings.

In many-to-one mapping, client certificates are mapped by rules that relate a set of certificate parameters to a user account. In this circumstance, copies of the certificate are not needed. However, this means that many-to-one mapping is not as secure as one-to-one mapping.

To use certificate mapping, select Enable Client Certificate Mapping in the Secure Communications dialog box and then click Edit. The Account Mappings dialog box opens. To create a one-to-one mapping, click the 1-to-1 tab and then click Add. Select a certificate to use and the user account to which it should be mapped. To create a many-to-one mapping, click the Many-to-1 tab, click Add, and follow the wizard to select certificate fields to use in the mapping rules.

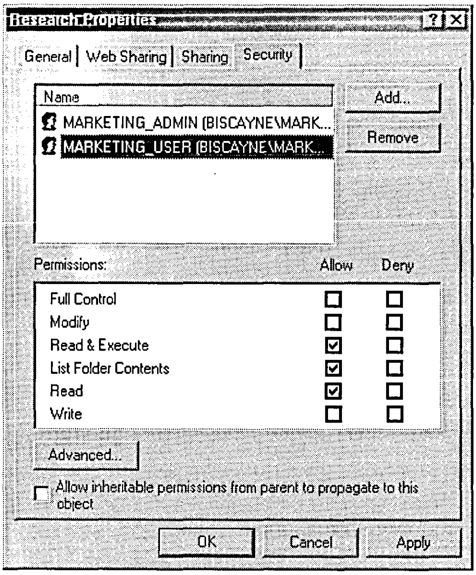
You might need to export client certificates to files and copy the files to your server in preparation for using them in one-to-one mappings. The exact steps used to export a certificate depend on the browser used, but you should not include private keys in the exported file, and the exported file should be in Base64 Encoded X.509 (.cer) format.

The logistics behind a one-to-one certificate mapping system can be quite extensive. Using Enterprise Certificate Authority Services on a Windows 2000 domain controller can simplify the management of individual client certificates.

Note Microsoft maintains a Web page about certification authorities at *www.microsoft.com/windows/oe/certpage.htm.* You can also request a client certificate from Microsoft at *sectestca2.rte.microsoft.com/certsrv.*

Let's return to the example of a marketing Web site, introduced earlier in this chapter. To expand the example, let's say that you keep proprietary information on this site and you can allow only the marketing department and selected other people within your company to view certain areas of the site. Because of the sensitive nature of some of this information, your boss is breathing down your neck to ensure that only authorized employees can access it. You have all the options we discussed previously for authentication and secure communications, so you are not afraid.

You begin by creating three new user accounts on your computer: MARKETING _USER, MARKETING_ADMIN, and DISTRIBUTION_ADMIN. The first will be used for all authorized users of the marketing site. The second two will be for administrators of the whole site and of just the distribution site, respectively. You go to each folder and grant basic access permissions for MARKETING_USER and Full Control for the administrators. (DISTRIBUTION_ADMIN gets permission only for the Distribution folder and subfolders.) See Figure 27-5.



Name
MARKETING_ADMIN (BISCAYNE\MARK...
MARKETING_USER (BISCAYNE\MARK...

Permissions:	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□

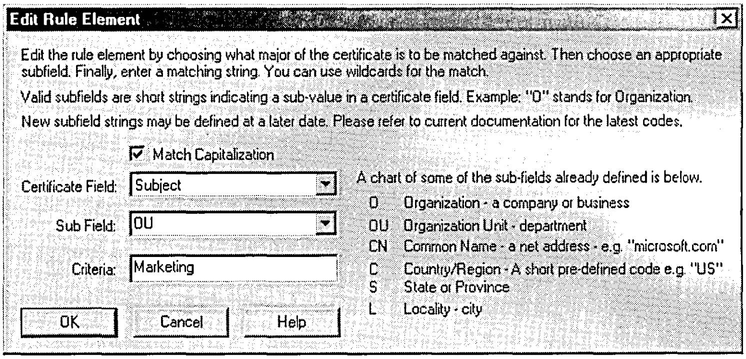
□ Allow inheritable permissions from parent to propagate to this object

Figure 27-5
Set NTFS permissions to limit access to your Web folders.

Because you want to be especially careful with the Administrator accounts, you use one-to-one mapping for them. You collect a copy of the client certificate for each person who is authorized to act as administrator either for the entire marketing site or for the Distribution subweb only. Map those certificates to the MARKETING _ADMIN or DISTRIBUTION_ADMIN account as appropriate.

Using the Internet Information Services snap-in, you can open the properties dialog box for the marketing site. In the Authentication Methods dialog box, clear all but Integrated Windows Authentication. In the Secure Communications dialog box, select Require Secure Channel (SSL), Require Client Certificates, and Enable Client Certificate mapping. Click Edit to begin defining mappings.

You know that one thing the IT people at your company did right was to issue everyone a client certificate that included his or her department name in the Organizational Unit (OU) subfield of the certificate's Subject field. So you create a many-to-one mapping using a rule (shown in Figure 27-6) that maps any certificate with Marketing in the OU subfield to the MARKETING_USER account. For any other people in your company to whom you want to grant access, simply create a one-to-one mapping using their certificates. Now you can tell your boss to relax.



Edit the rule element by choosing what major of the certificate is to be matched against. Then choose an appropriate subfield. Finally, enter a matching string. You can use wildcards for the match.

Valid subfields are short strings indicating a sub-value in a certificate field. Example: "O" stands for Organization.

New subfield strings may be defined at a later date. Please refer to current documentation for the latest codes.

☑ Match Capitalization

Certificate Field: Subject

Sub Field: OU

Criteria: Marketing

A chart of some of the sub-fields already defined is below.

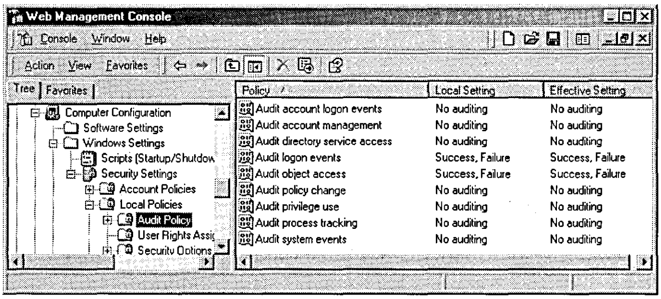
O	Organization - a company or business
OU	Organization Unit - department
CN	Common Name - a net address - e.g. "microsoft.com"
C	Country/Region - A short pre-defined code e.g. "US"
S	State or Province
L	Locality - city

Figure 27-6
You can create many-to-one rules to map classes of users to individual accounts.

Auditing

Two avenues of monitoring activity on your Web server are available: NTFS auditing, and IIS event logging.

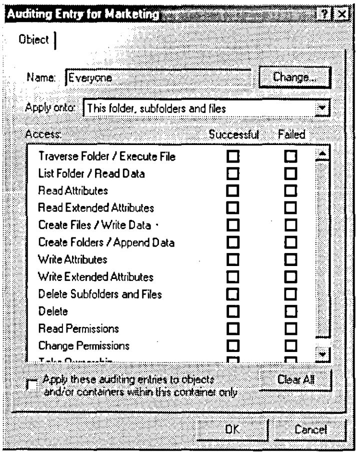
To use NFS auditing, you must first enable auditing in Local Security Policy. To do that, open the Local Security Policy snap-in. (It's in the Web Management console described earlier in this chapter; if you didn't create such a console, go to Start | Settings | Control Panel | Administrative Tools | Local Security Policy or run Secpol.msc.) Then navigate to Security Settings\Local Policies\Audit Policy. Figure 27-7 shows the audit options. To enable a policy, right-click the policy's icon and choose Security. You can enable policies to log successful events, unsuccessful events, or both. For example, you can log both successful and unsuccessful logon attempts. *For more information, see "Enabling Auditing," page 576.*



Policy	Local Setting	Effective Setting
Audit account logon events	No auditing	No auditing
Audit account management	No auditing	No auditing
Audit directory service access	No auditing	No auditing
Audit logon events	Success, Failure	Success, Failure
Audit object access	Success, Failure	Success, Failure
Audit policy change	No auditing	No auditing
Audit privilege use	No auditing	No auditing
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	No auditing

Figure 27-7
Select audit policies for your Web server from the Local Security Policy snap-in.

Then, for each object you want to audit, you specify which users or groups and which events should be recorded in the Security log. In a Windows Explorer window, navigate to the folder you want to audit. Right-click the folder icon and choose Properties. Click Advanced and then click the Auditing tab. Click Add and then select the user or group you want to audit with respect to the selected folder. If you want to audit all activity involving this folder, regardless of the user, select Everyone. The Auditing Entry dialog box opens, in which you can select the activities you want to audit. (See Figure 27-8.)



Name: Everyone

Apply onto: This folder, subfolders and files

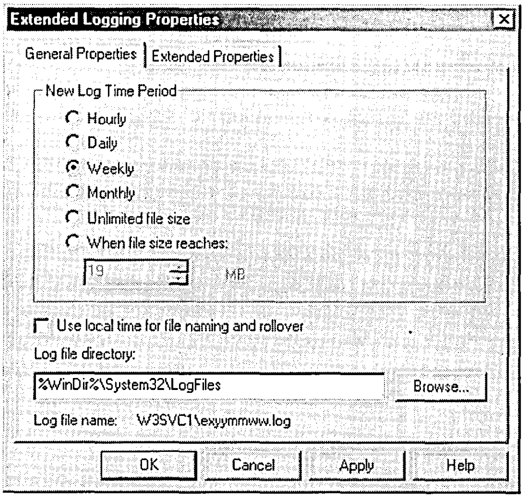
Access:	Successful	Failed
Traverse Folder / Execute File	□	□
List Folder / Read Data	□	□
Read Attributes	□	□
Read Extended Attributes	□	□
Create Files / Write Data	□	□
Create Folders / Append Data	□	□
Write Attributes	□	□
Write Extended Attributes	□	□
Delete Subfolders and Files	□	□
Delete	□	□
Read Permissions	□	□
Change Permissions	□	□

□ Apply these auditing entries to objects and/or containers within this container only

Figure 27-8
In the Auditing Entry dialog box, you can select audit policies for folders using Windows NTFS auditing.

To view the logs, open Event Viewer (Start | Settings | Contorl Panel | Administrative Tools | Event Viewer) and select Security Log. IIS logging records more of the activity on your Web site than either of the other two auditing methods. For example, if you want to monitor the IP addresses of visitors to your site, you need to use IIS logging. You turn logging on or off for the whole site. You then choose to log activity for individual sites. You also have an option of three log-file formats.

To turn on logging for the site, in the Internet Information Services snap-in, right-click the icon for the Web site and choose Properties. On the Web Site tab, select Enable Logging. Select the log format you want and click Properties. The Extended Logging Properties dialog box opens, as shown in Figure 27-9. Select the frequency with which you want to start new log files and specify the folder where you want log files to be stored. If you use W3C Extended Log format, an Extended Properties tab lets you select which data to include in each log entry. See the online IIS documentation for more information about log-file formats.



Extended Logging Properties

General Properties | Extended Properties

New Log Time Period

○ Hourly
○ Daily
● Weekly
○ Monthly
○ Unlimited file size
○ When file size reaches:

19 MB

□ Use local time for file naming and rollover

Log file directory: %WinDir%\System32\LogFiles

Log file name: W3SVC1\exyymmww.log

Figure 27-9
Use this dialog box to configure how often log files are started and where they are stored.

Obtaining a Server Certificate

The process for obtaining a server certificate involves creating a certificate request (in the form of a request file), submitting the request to a Certification Authority, obtaining the approved certificate, and installing the certificate on your computer. The Web Server Certificate Wizard handles almost all this process.

The Web Server Certificate Wizard generates a request for a server certificate and installs the certificate once it is granted. If you are connected to a domain server running Enterprise Certificate Services, the wizard submits your request online. The wizard also detects an out-of-date or about-to-expire certificate.

You can start the Web Server Certificate Wizard through the Internet Information Services snap-in. Open the Properties dialog box for the Web site and select the Directory Security tab. Click Server Certificate and the wizard begins. The options presented by the wizard depend on whether you already have a server certificate installed or have an outstanding request.

Redirecting Requests to the Site

You can cause the Web server to *redirect*, that is, serve a different page than the one indicated by the URL. You might want to do this, for example, if you discontinue some section of a Web site, but users still attempt to view these pages. A redirect can serve a page informing the browser of the change, or the redirect can serve a current page. To redirect from an object (folder or file), open the properties dialog box for the object. Click the Directory tab and select A Redirection To A URL. Then enter the redirect URL in the text box. If you select The Exact URL Entered Above, the server will serve the exact file. If you select A Directory Below This One, the server will append the resource name to the directory you enter in the text box and serve that file. Use this latter option if the file is the same but in a different location.

Using Content Ratings

The Platform for Internet Content Selection (PICS) specification defines metalabels included in HTML headers that are used to describe the content of Web pages. IIS provides a means of applying Recreational Software Advisory Council (RSAC) ratings to your Web site or subweb. In the properties dialog box for the site you want rated, select the HTTP Headers tab and click Edit Ratings. On the Ratings Service tab, select Ratings Questionnaire. Doing so opens the RSAC Web site in a browser window. Follow the instructions there to complete the RSAC questionnaire. After completing the questionnaire and registering with RSAC, you will be given the appropriate ratings for your site. Then click the Ratings tab, select Enable Ratings For This Resource, and enter the ratings for each of the four categories. After this is complete, all pages from your site will be sent with the appropriate header information. If the user's browser is able to interpret these headers, the browser can be set to accept or reject your page, depending on its rating.

Running an FTP Server

Setting up and running an FTP server is very similar to operating a Web server. When you install IIS, a default FTP site is created automatically. The authentication and access topics discussed earlier in this chapter apply to FTP servers as well. Like Web sites, FTP sites are organized around folders and use NTFS permissions to control access. In general, however, you have fewer options for FTP configuration than for Web configuration.

FTP uses either anonymous or basic authentication. The authentication method is set for the entire FTP site; you cannot set a different method for subdirectories. You also have no option for creating a secure link. On the Security Accounts tab of the Default FTP Site Properties dialog box, either select or clear Allow Anonymous Connections. If you select anonymous authentication, you can select which user account is used by all users who log in anonymously. You can also select Allow Only Anonymous

Connections if you want to prevent anyone gaining access to your computer or network by logging on with a recognized user name.

Use NTFS permissions to set user permissions on FTP folders and files.

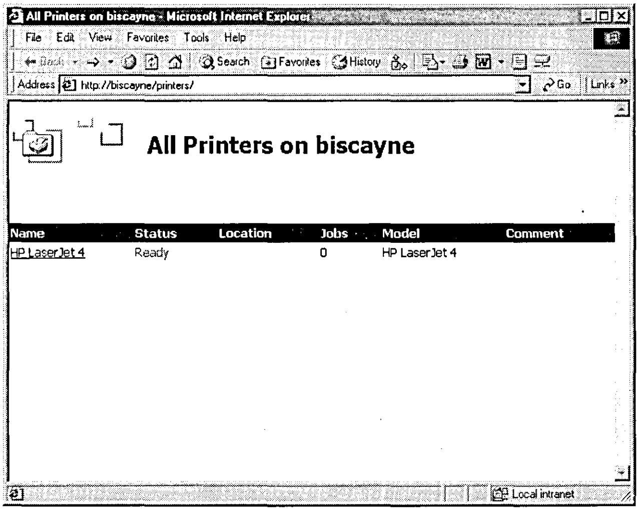
Using Your Web Site for Collaboration (WebDAV)

Web Distributed Authoring and Versioning (WebDAV) allows users to set up shared folders served by IIS. Users with proper permissions can publish files to, open and edit files in, and lock and check out files in WebDAV folders. Windows 2000 and Internet Explorer 5 support WebDAV. Microsoft Office 2000 supports additional collaboration features with WebDAV.

To create a WebDAV folder, set up a virtual directory under Default Web Site in IIS. The physical directory can be anywhere on your intranet. Give the directory Read, Write, and Browsing permissions. Then, any Windows 2000 users on your intranet can create a Web folder shortcut to the WebDAV folder in their My Network Places folder.

Setting Up IIS for Internet Printing

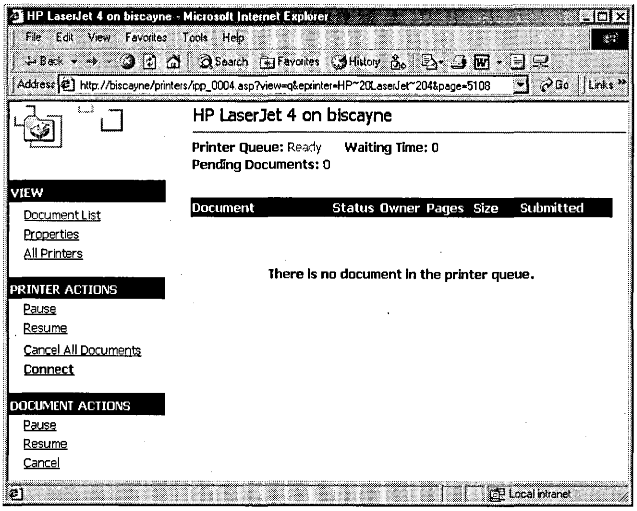
IIS also enables Internet Printing Protocol (IPP). Whenever you share a printer and you are running IIS, the shared printer becomes available over the Internet. Users to whom you've given permission can view and manage printers in a Web browser in much the same way that they can using the Printers folder for local and network printers. In an Internet Explorer window, open http://*hostname*/printers for a list of shared printers on *hostname*. *Hostname* can be a computer name (for an intranet), a domain name, or an IP address. Select one of the printers to open a page with printer status and control options. See Figures 27-10 and 27-11.



All Printers on biscayne

Name	Status	Location	Jobs	Model	Comment
HP LaserJet 4	Ready		0	HP LaserJet 4	

Figure 27-10
By running IIS, you can share printers throughout your intranet or over the Internet.


HP LaserJet 4 on biscayne - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links
Local intranet

http://biscayne/printers/ipp_0004.asp?view=q&eprinter=HP~20LaserJet~204&page=5108

HP LaserJet 4 on biscayne

Printer Queue: Ready **Waiting Time:** 0
Pending Documents: 0

VIEW
- Document List
- Properties
- All Printers

PRINTER ACTIONS
- Pause
- Resume
- Cancel All Documents
- Connect

DOCUMENT ACTIONS
- Pause
- Resume
- Cancel

Document	Status	Owner	Pages	Size	Submitted

There is no document in the printer queue.

Figure 27-11
IPP offers capabilities similar to those available in the Printers folder—but with a familiar Web-style interface.

Chapter 28

Managing Incoming Connections

In This Chapter

Creating Incoming Connections 486

Understanding Tunnels and Virtual Private Networks 489

Using IPSec 490

A computer running Microsoft Windows 2000 Professional can allow access from remote computers using three methods: dial-up connection, direct (for example, serial or parallel lines) connection, and virtual private network (VPN). In this chapter, we discuss creating these types of connections and the advanced security capabilities of IPSec.

For information about other means of allowing remote computers to connect to your computer (Web and FTP), see Chapter 27, "Managing a Web Server." For information about connections for dialing out from your computer, see Chapter 22, "Making Network Connections."

Dial-up connections use a telephone lines and some type of modem—for example, an analog modems, ISDN modems, or X.25 modems. You can create a direct parallel connection to another computer using Parallel Technologies Direct Parallel Connection cables. (Contact Parallel Technologies at *www.lpt.com.*) Virtual private networks allow you to use a network (for example, a corporate LAN or the Internet) as the medium for connecting your computer with other computers in another local network, no matter how physically distant the computers are.

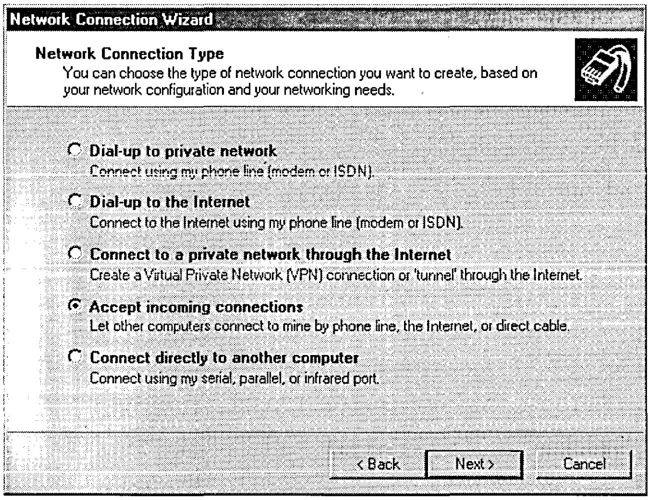
When you allow access to your computer through incoming connections, you need to be concerned with the security issues these connections create. We discuss the Windows 2000 implementation of a security scheme called IPSec in this chapter.

Creating Incoming Connections

In Windows 2000 Professional, you create one incoming connection to handle all the variety of incoming connections you need to allow. As your requirements change, you can modify the properties of this connection.

To create the incoming connection, perform the following steps:

1. Open the Network Connection Wizard by clicking Start | Settings | Network And Dial-Up Connections | Make New Connections. Click Next on the first wizard page.
2. Select Accept Incoming Connections and click Next.



Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ **Dial-up to private network**
Connect using my phone line (modem or ISDN).

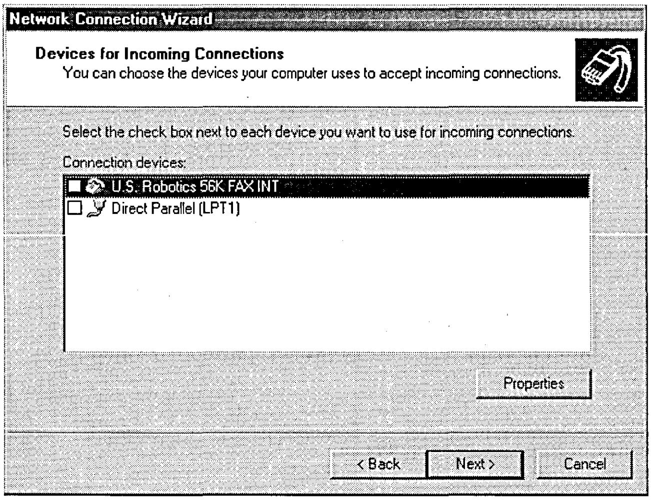
○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

○ **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

● **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

3. Select one or more devices for which you want to allow incoming connections. (VPNs do not use a connection device.)



Devices for Incoming Connections
You can choose the devices your computer uses to accept incoming connections.

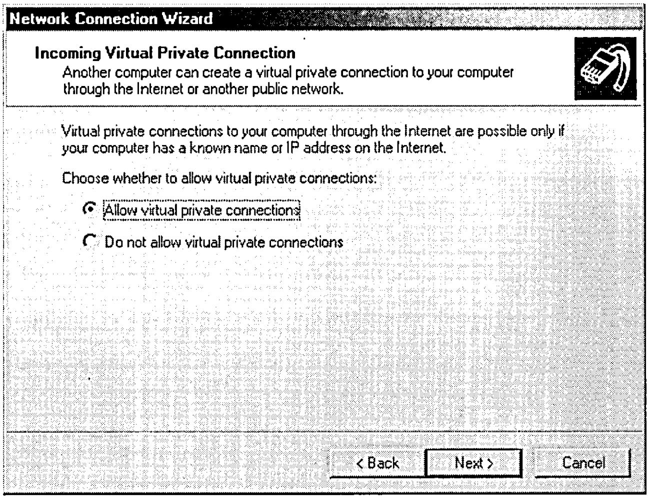
Select the check box next to each device you want to use for incoming connections.

Connection devices:

□ U.S. Robotics 56K FAX INT
□ Direct Parallel (LPT1)

? □ NIC (LAN)

4. Make a selection, either allowing or not allowing virtual private connections, and click Next.



Network Connection Wizard

Incoming Virtual Private Connection

Another computer can create a virtual private connection to your computer through the Internet or another public network.

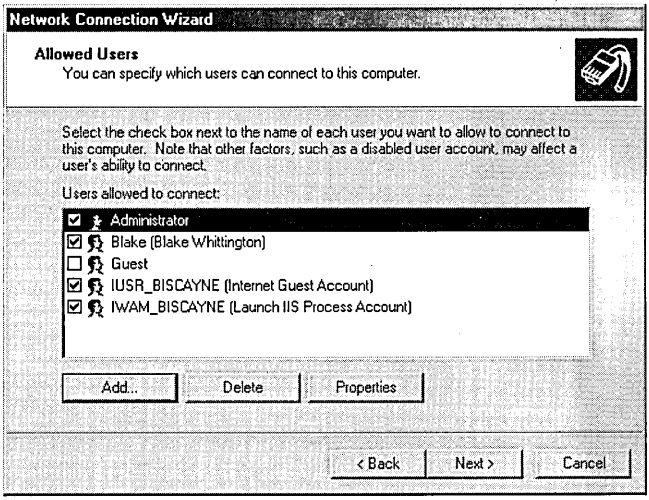
Virtual private connections to your computer through the Internet are possible only if your computer has a known name or IP address on the Internet.

Choose whether to allow virtual private connections:

● Allow virtual private connections

○ Do not allow virtual private connections

5. From the list of users, select all users who have permission to connect using this connection.



Network Connection Wizard

Allowed Users

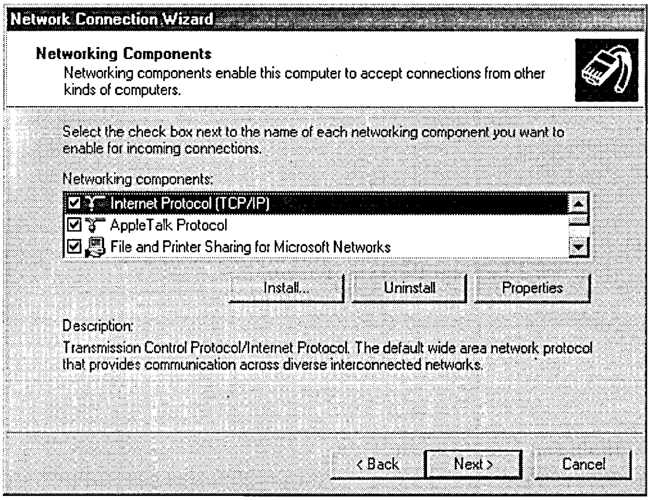
You can specify which users can connect to this computer.

Select the check box next to the name of each user you want to allow to connect to this computer. Note that other factors, such as a disabled user account, may affect a user's ability to connect.

Users allowed to connect:

☑ Administrator
☑ Blake (Blake Whittington)
□ Guest
☑ IUSR_BISCAYNE (Internet Guest Account)
☑ IWAM_BISCAYNE (Launch IIS Process Account)

6. Select which protocols are to be allowed on this connection. By default, all installed protocols are selected. Clear the check box for any you don't need. Install any protocols you need that are not displayed. Click Next and then click Finish.


Network Connection Wizard

Networking Components

Networking components enable this computer to accept connections from other kinds of computers.

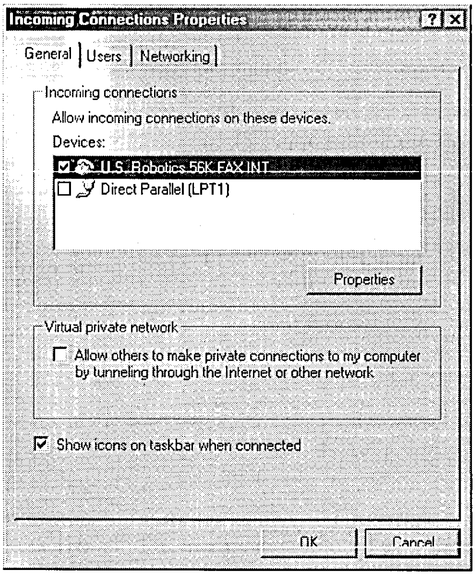
Select the check box next to the name of each networking component you want to enable for incoming connections.

Networking components:

- ☑ Internet Protocol (TCP/IP)
- ☑ AppleTalk Protocol
- ☑ File and Printer Sharing for Microsoft Networks

Description:
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Your connection now shows up in the Network And Dial-Up Connections folder with the name Incoming Connections. Right-click the icon for Incoming Connections and choose Properties. The Incoming Connections Properties dialog box (see Figure 28-1) appears, showing you all the configuration selections you made and allowing you to change them.



Incoming connections

Allow incoming connections on these devices.

Devices:

- ☑ U.S. Robotics 56K FAX INT
- ☐ Direct Parallel (LPT1)

Virtual private network

☐ Allow others to make private connections to my computer by tunneling through the Internet or other network

☑ Show icons on taskbar when connected

Figure 28-1
You can configure properties for all your incoming connections.

Understanding Tunnels and Virtual Private Networks

The Internet is the greatest thing since sliced bread. Not only does it let you order groceries over it and download music from it, but it also comes with miles and miles of cables, hundreds of routers, and tons of other equipment necessary for making internetworks work—not to mention the associated transmission protocols. Someone had the great idea of using all that infrastructure for connecting separate private networks. In the olden days, if you had offices in New York and Chicago and you wanted to connect their computer networks, you had to pay the phone company to use its cables and set up special protocols at each end. But if two computers (or two networks) are each connected to the Internet, a physical connection between them already exists, with a transmission protocol already set up. The only question is how to make use of these assets.

That's where tunneling comes in. You want to enable network data to reach computers on the other side of an intervening network just as if the sending and receiving computers were on the same local network. Tunneling protocols dig underneath the protocol of the intervening network to create the illusion of a direct path between the two separated networks.

This is accomplished by encrypting each IP packet or frame (depending on the protocol) and wrapping it inside another packet or frame with new header information for traveling through the intervening network. That is, when a network frame (if we're talking about a frame-based protocol) created on one of the computers is destined for a computer on the other side of the tunnel, the entire frame is encrypted and a new header that routes the encrypted frame through the intervening network is attached. When the new frame gets to the other side, the new header is stripped off, and the original frame is decrypted and routed forward just as though it had never left the original local network. When you put all these pieces together, you end up with a virtual private network. Tunneling protocols are the core of VPNs.

The intervening network does not have to be the Internet. Offices might have special networks separated from the primary corporate network for privacy reasons. The private network can be connected to the corporate network through a VPN server. The VPN server allows any authorized computer on the corporate network to connect to the private network. In this case, the corporate network is the intervening network through which the tunnel is created.

Three tunneling protocols are in wide use today:

- **Point-to-Point Tunneling Protocol (PPTP).** PPTP allows IP, IPX, or NetBEUI frames to be encrypted and then wrapped in an IP header to be sent across an intervening network.
- **Layer 2 Tunneling Protocol (L2TP).** L2TP allows IP, IPX, or NetBEUI frames to be encrypted and then sent over any IP, X.25, Frame Relay, or ATM intervening network. L2TP is new in Windows 2000.

- **IP Security (IPSec) Tunnel Mode.** IPSec Tunnel Mode allows IP packets to be encrypted and then encapsulated in an IP header to be sent across an intervening network. IPSec is new in Windows 2000.

Windows 2000 uses PPTP or L2TP for tunnel connections. Only Microsoft Windows 2000 Server can act as a VPN server using L2TP. Windows 2000 Professional can, however, connect to a VPN server using L2TP. Windows 2000 uses IPSec to enhance the security of all network interactions.

Internet Security Sites

The following is a short list of the many Web sites devoted to network security. The companion CD includes a number of additional links.

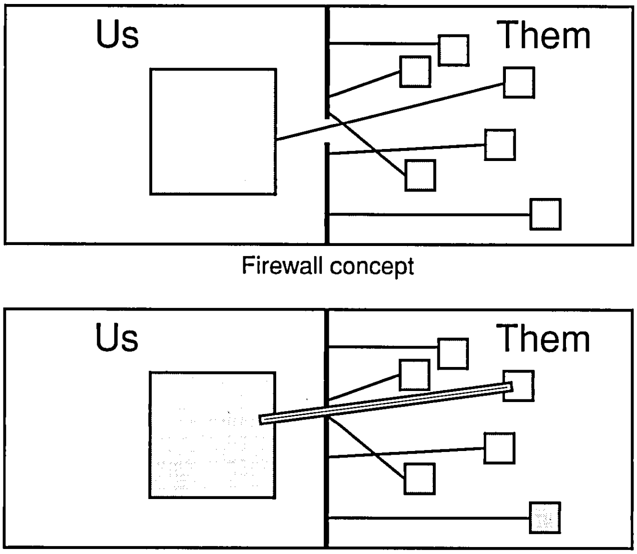
- *www.microsoft.com/security*
- *www.microsoft.com/technet/security/dosrv.asp*
- *grc.com/su-reading.htm*
- *www.cert.org*
- *www.denialinfo.com*
- *csrc.nist.gov*
- *www.netsec-intl.com*

Using IPSec

The previous section introduced IPSec as a tunneling protocol. Actually, IPSec is a broader security mechanism meant to overcome many of the security limitations of IP (Internet Protocol). Because all network activity in Windows 2000 uses IP by default, IPSec provides an important service for all network connections, incoming as well as outgoing. We discuss IPSec in this chapter because it is often associated with VPNs. But IPSec can be used for any network connection.

In Chapter 25, "Making Internet Connections," we discuss Internet security using packet filtering. IPSec, however, works with a different concept. Packet filtering forms a shield that determines which IP packets to allow in and out of your computer. It is like a wall around your computer with one small door. Any packets from any external computer that meet the requirements are allowed in. All the security happens at the wall.

IPSec negotiates a security association between two computers and is sometimes called *end-to-end security*. The security takes place on each computer through the negotiated link. Although packet filtering is a part of IPSec, IPSec encompasses other security protocols, and the packet filtering that IPSec uses has more flexibility than the filtering discussed in Chapter 25. Figure 28-2 depicts the difference between these two concepts.



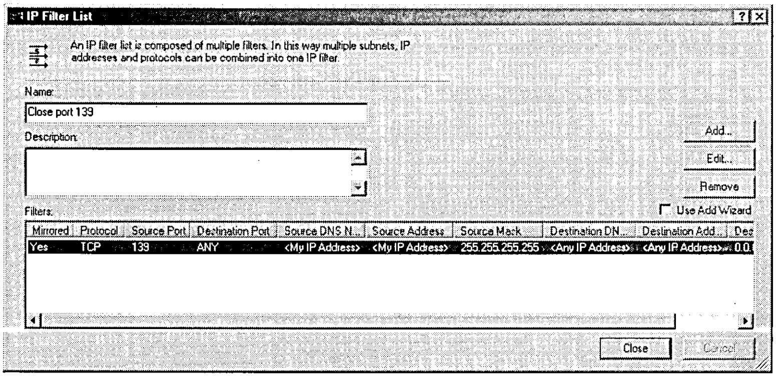
Firewall concept

IPSec concept

Figure 28-2
IPSec is conceptually different from packet filtering.

IPSec comprises a suite of protocols (including packet filtering). A combination of configuration settings for all the associated protocols is called a *rule*, or a *filter rule*. An IPSec policy is a collection of one or more rules. You can enable only one IPSec policy at a time, but the policy might have several rules. Each rule is made up of five components:

- **Filter List.** Consists of one or more packet filtering definitions for filtering on protocol, source address/port/mask, and destination address/port/mask. Filter lists are named and stored for use in multiple rules. You can configure only one filter list per rule. A sample filter for closing port 139 is shown here. Although this example shows only one filter in the list, you can have as many filters as needed.



An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name:
Close port 139

Description:

Filters:

□ Use Add Wizard

Mirrored	Protocol	Source Port	Destination Port	Source DNS N...	Source Address	Source Mask	Destination DN...	Destination Add...	Des
Yes	TCP	139	ANY	<My IP Address>	<My IP Address>	255.255.255.255	<Any IP Address>	<Any IP Address>	0.0.

- **Filter Action.** Provides direction on what the filter does with connections matching the filter criteria: permit, block, or negotiate a secure connection.
- **Authentication Methods.** Offers a selection of user authentication method: Kerberos, certificate, or code/key. Kerberos V5 protocol uses Windows user accounts defined on your domain. Therefore, if the computers you are connecting are not on the same domain, you must use one of the other authentication methods. You can require that the computer attempting a connection have a server certificate from a selected certification authority (CA). You select the CA from your Trusted CA list by clicking Browse. You can also use an alphanumeric key. If you use a preset key, both computers must have exactly the same key configured.
- **Tunnel Setting.** Determines whether a connection can use a virtual private network. If you want the rule to allow a VPN connection, you configure the IP address of the requesting computer. Note that you can configure only one tunneling connection per rule. To allow multiple computers to request a VPN connection, you must create a rule for each computer and select each rule for the active policy.
- **Connection.** Determines which connections this rule should be applied to: all, dial-up, or network.

Creating an IPSec Policy

IPSec policies are managed through the Security Settings extension of the Group Policy snap-in. You can launch Local Security Settings, a console with just that extension, by going to Start | Settings | Control Panel | Administrative Tools | Local Security Policy or by typing *secpol.msc* at a command prompt; you can also find the extension as part of Group Policy (Gpedit.msc). Alternatively, you can install the IPSec Security Policy Management snap-in at the root level of any console.

Regardless of how you display IPSec in Microsoft Management Console (MMC), to work with IPSec policies, you select IP Security Policies On Local Machine. (If you're using the Group Policy console, go to Local Computer Policy\Computer Configuration \Windows Settings\Security Settings\IP Security Policies On Local Machine.)

The user interface for creating IPSec policies can be a bit confusing. It provides property dialog boxes for the policy, each rule, each filter list, and each action. You must use one wizard but might use as many as four wizards. Use the IP Security Policy Wizard to create the shell of your new policy. From there, you can add rules to the policy and then add filter lists and filter actions to the rules—either by running wizards or by editing their respective properties dialog boxes directly. The following sections explain each of these procedures.

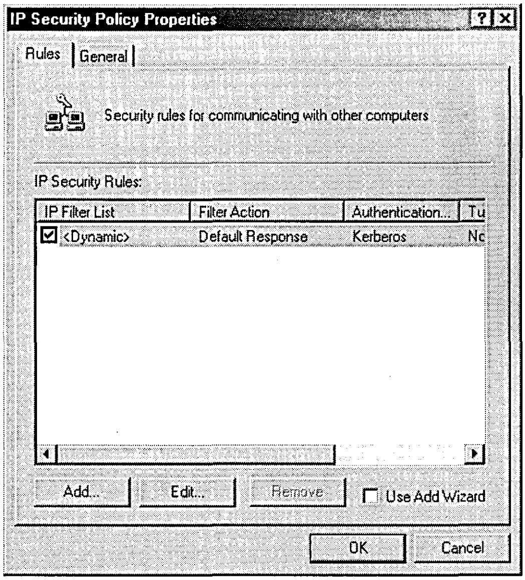
Create the Policy Shell

1. From the Action menu, choose Create IP Security Policy. The IP Security Policy Wizard appears. Click Next.
2. Enter a name for the policy and a description if desired. Click Next.
3. The default response filter action enforces Kerberos authentication and a custom security scheme and is used when no other filter rule applies. If you want to include this default rule in your policy, leave Activate The Default Response Rule selected. Otherwise, clear the check box. Click Next.
4. If you chose to use the default rule, the wizard asks you for an authentication method to use for that rule. Make a selection and click Next.

Add Filter Rules to the Policy

At this point, you have created the shell of your policy. You now need to fill out the filter rules.

1. Make sure that Edit Properties is selected and click Finish. The properties dialog box for your new policy appears. If you selected the default response rule, it is selected in the IP Security Rules list. Now you can add the primary rule(s) for this policy.



Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ <Dynamic>	Default Response	Kerberos	Nc

□ Use Add Wizard

2. Make sure that Use Add Wizard is selected and click Add. The Security Rule Wizard appears. Click Next. (If you feel confident, clear Use Add Wizard. When you click Next, the New Rule Properties dialog box appears. Fill out each tab according to the steps that follow.)

3. If this rule is to allow a VPN connection, select The Tunnel Endpoint Is Specified By This IP Address and enter the IP address of the computer that will be requesting the connection. Otherwise, leave This Rule Does Not Specify A Tunnel selected. (In the properties dialog box, these options are on the Tunnel Setting tab.) Click Next.

Note

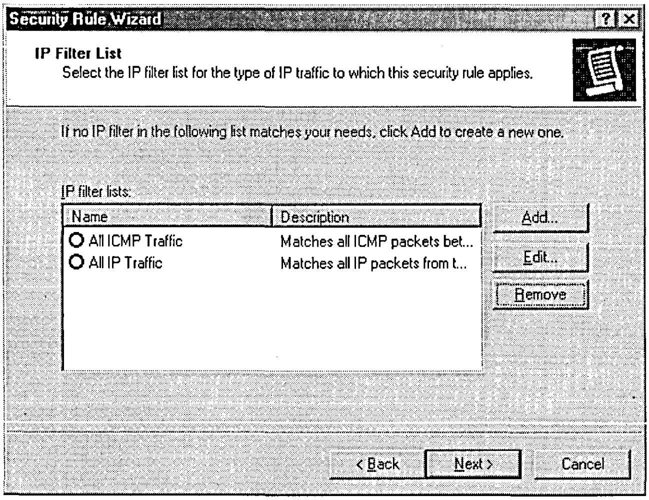
You need to create a rule for each computer that might be requesting a VPN connection.

4. Select the network connections to which you want to apply this policy (Connection Type tab). Remote Access refers to dial-up connections. Click Next.

5. Select the authentication method for this rule (Authentication Methods tab). Click Next.

Add Filter Lists to the Filter Rule

Now you need to select or define the filter list you want to use for this policy. If you're using Security Rule Wizard, the list of predefined filters is displayed, as shown here. You'll find comparable settings on the IP Filter List tab of the properties dialog box.



IP Filter List

Select the IP filter list for the type of IP traffic to which this security rule applies.

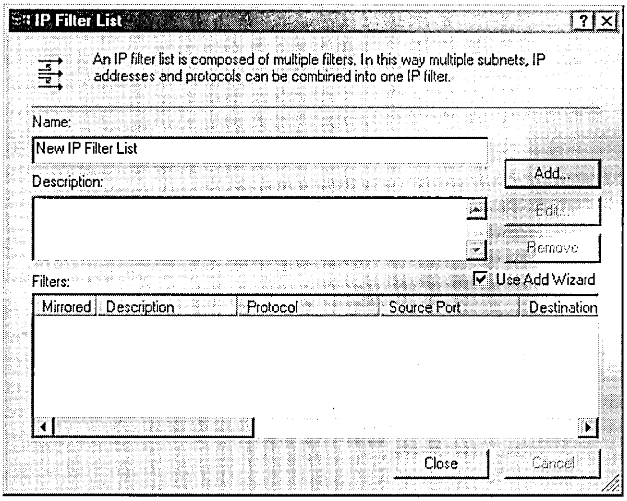
If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...

1. If the filter list you want to use is already defined, select it from the list and skip to the next section, "Finish Configuring the Rule." Otherwise, click Add to define a new filter list.
2. When you click Add, the IP Filter List dialog box appears. This is a shell for new filter lists. Enter a name and description for this filter list.
3. With Use Add Wizard selected, click Add to add a filter to this list. (If you feel confident, clear Use Add Wizard. When you click Add, the Filter Properties dialog box appears. Fill out each tab according to the following steps.)

Note Filter lists are saved by name and can be used in multiple rules.



IP Filter List

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: New IP Filter List

Description:

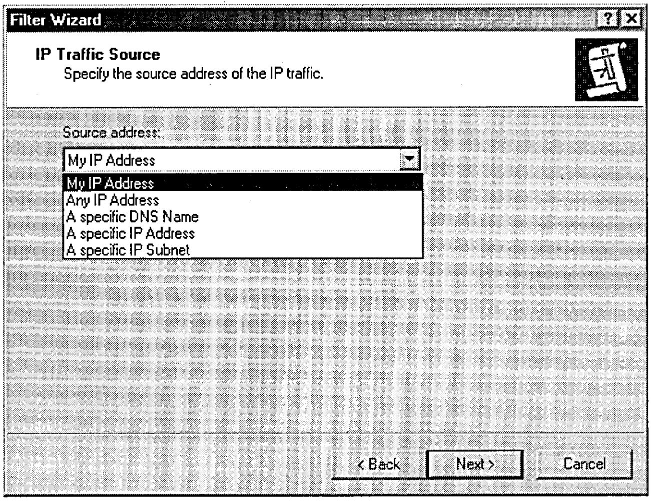
Filters:

☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

4. The IP Filter Wizard appears. Click Next.
5. From the drop-down list, select the source address of the packets. (In the Filter Properties dialog box, the list is on the Addressing tab.) Click Next.

Note If you are creating a filter for a VPN connection, select A Specific IP Address for the source and My IP Address for the destination. Enter the IP address of the computer requesting the VPN connection as the source IP address.



Filter Wizard

IP Traffic Source

Specify the source address of the IP traffic.

Source address: My IP Address

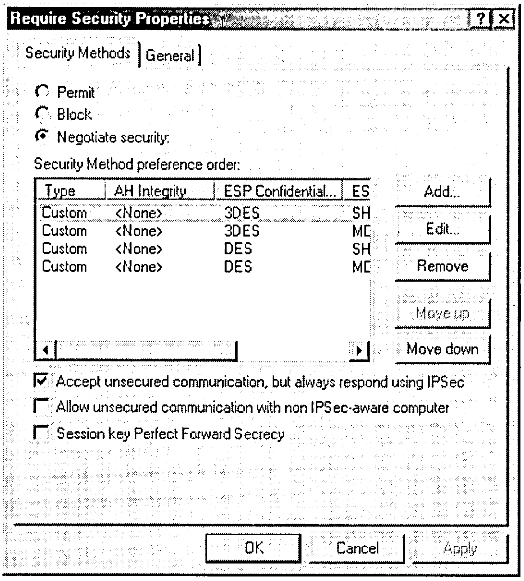
6. From the drop-down list, select the destination address of the packets. (In the Filter Properties dialog box, use the Addressing tab.) The options are the same as for the source. Click Next.
7. Select the protocol. (In the Filter Properties dialog box, use the Protocol tab.) Common selections are Any, IP, TCP, UDP, and ICMP. Click Next. Depending on your selection, you might need to select the port numbers to filter.
8. Click Finish to return to the IP Filter List dialog box. If you want to add another filter, click Add and repeat the preceding process.

Note Filters are not applied in the order in which they are listed. Filters are generally applied from most specific to least specific. This ordering is not guaranteed during system startup, so some anomalous behavior can occur at that time.

9. When you finish adding filters to the filter list, click Close to return to the Security Rule Wizard. (If you've skipped the wizards, you return to the New Rule Properties dialog box.) Select the filter list you just created. Click Next.

Finish Configuring the Rule

1. Select an action to perform on packets matching the filter. (In the New Rule Properties dialog box, the list is on the Filter Action tab.) Pick one of the default actions or click Add to run the Filter Action Wizard and create a new action. Select one of the default actions and then click Edit to see its properties dialog box. The Require Security Properties dialog box is shown here. Click Next and then click Finish.



○ Permit
○ Block
● Negotiate security:

Security Method preference order:

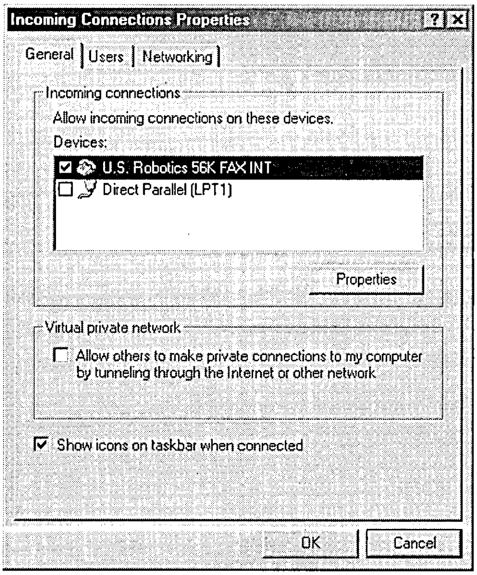
Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	3DES	SH
Custom	<None>	3DES	MC
Custom	<None>	DES	SH
Custom	<None>	DES	MC

☑ Accept unsecured communication, but always respond using IPSec
☐ Allow unsecured communication with non IPSec-aware computer
☐ Session key Perfect Forward Secrecy

On the wizard page, click Next and then click Finish.

Note Filter actions are saved by name and can be used in multiple rules.

2. Click OK. That rule is now defined. If you want to add another rule, click Add and repeat the process. As you add each rule, it is added to the IP Security Rules list in the properties dialog box for the policy. When you have added all the rules you want for your policy, click Close.



Incoming connections
Allow incoming connections on these devices.
Devices:
☑ U.S. Robotics 56K FAX INT
☐ Direct Parallel (LPT1)

Virtual private network
☐ Allow others to make private connections to my computer by tunneling through the Internet or other network

☑ Show icons on taskbar when connected

Enabling an IPSec Policy

In the Local Security Settings console, right-click the policy that you want to enable and choose Assign (the IPSec word for enable). That policy is now enabled. If any other policy had been assigned, it becomes unassigned.

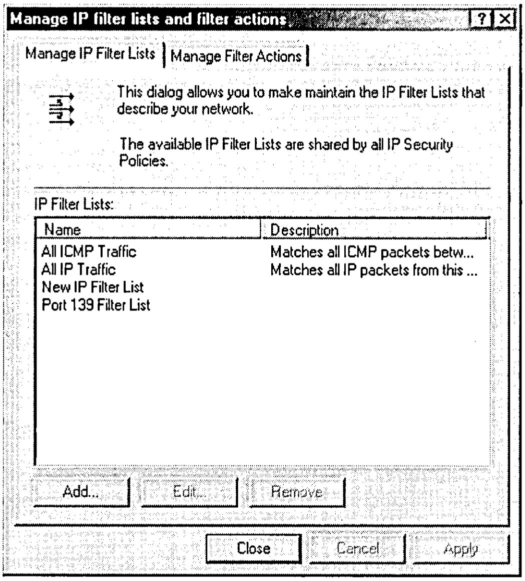
You also have another way to enable IPSec policies. In the Network And Dial-Up Connections folder, select any connection and open its properties dialog box. Select the tab containing the components (the General tab or the Networking tab, depending on the type of connection). Select Internet Protocol (TCP/IP) and click Properties | Advanced | Options | IP Security | Properties. Select Use This IP Security Policy and then select the policy you want from the drop-down list.

Modifying an IPSec Policy

As discussed earlier, IPSec policies have rules made up of filter lists, filter actions, authentication methods, tunnel settings, and connection types. Filter lists, filter actions, and policies are entities with names and associated configuration settings. Therefore, you can edit filter lists and filter actions on their own or through the policies that contain them.

In the IP Security On Local Machine folder in the Local Security Settings console, choose Manage IP Filter Lists And Filter Actions from the Action menu. The Manage IP Filter Lists And Filter Actions dialog box appears, as shown in Figure 28-3. Select the filter list or filter action you want to modify and click Edit. The respective properties dialog box opens, and you can edit the configuration settings. These changes will be reflected in each policy that uses the respective filter list or filter action.

To modify an IPSec policy, select the policy in the Local Security Settings console and then choose Properties from the Action menu. The policy properties dialog box appears, similar to the one shown in Figure 28-4. Select the rule you want to edit and click Edit to display the Edit Rule Properties dialog box. This is the same dialog box you see if you don't use the wizard to create new rules. Each tab in this dialog box contains the setting for one of the five elements of an IPSec rule.



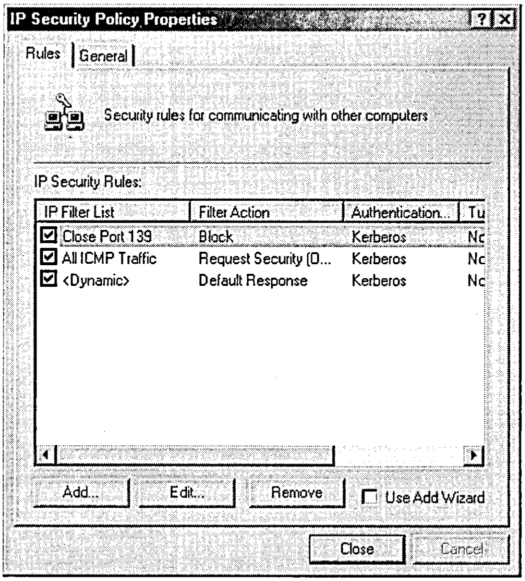
This dialog allows you to make maintain the IP Filter Lists that describe your network.

The available IP Filter Lists are shared by all IP Security Policies.

IP Filter Lists:

Name	Description
All ICMP Traffic	Matches all ICMP packets betw...
All IP Traffic	Matches all IP packets from this ...
New IP Filter List	
Port 139 Filter List	

Figure 28-3
You can edit filter lists and filter actions directly.



Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ Close Port 139	Block	Kerberos	Nc
☑ All ICMP Traffic	Request Security (O...	Kerberos	Nc
☑ <Dynamic>	Default Response	Kerberos	Nc

Figure 28-4
You can modify an IPSec policy from its properties dialog box.

Troubleshooting IPSec

Several tools are useful for troubleshooting connections that use IPSec:

- **Ping.** The Ping command can help to determine whether the network between two computers is functioning. In a Command Prompt window of one computer, type *ping IP*, where *IP* is the IP address of the other computer.
- **Event Logs.** The System or Security event logs have entries for failed connections, often with helpful descriptions. If connections fail, check these logs.
- **Policy Integrity Check.** Sometimes links in policies can break. To check for problems in the policy, select IP Security Policies On Local Computer in the Local Security Settings console and choose Action | All Tasks | Check Policy Integrity. All policies will be checked.
- **IPSec Monitor.** The IPSec Monitor tool displays information for each active security association. IPSec Monitor can also provide statistics about security associations, key usage, bytes sent and received, and other items. To start IPSec Monitor, type *ipsecmon* at a command prompt.

In some cases, restarting the Policy Agent might be necessary; to do that, restart the computer. You can reinstall the IPSec components by removing and reinstalling TCP/IP.

Enabling IPSec Through a Firewall

If you want to use IPSec for network connections that must connect through a firewall, proxy server, security gateway, or router, certain filters must be in place to allow IPSec data through.

The following filters must be enabled for both input and output traffic:

- IP Protocol ID 50: for IPSec Encapsulating Security protocol traffic
- IP Protocol ID 51: for IPSec Authentication Header traffic
- UDP port 500: for inbound Internet Key Exchange negotiation traffic

Chapter 29

Communicating Over the Internet

In This Chapter

Using NetMeeting 502
Using Internet Instant Messaging 512

The Internet provides unparalleled opportunities for communication. The World Wide Web and e-mail are becoming as ubiquitous as telephones and televisions. Internet Chat Request (ICQ) and instant messaging are also increasingly clogging Internet bandwidth. The Internet now delivers audio (music clips, voice communications, and so on) and video (such as movie clips and Webcam feeds). Online video conferencing is emerging as a powerful tool that makes use of the Internet's existing infrastructure and ever-expanding bandwidth. Microsoft Windows 2000 allows you to take full advantage of these developing technologies.

Microsoft NetMeeting is a fully developed network conferencing tool, complete with chat, audio, video, and whiteboard capabilities. In addition, NetMeeting allows you to share applications and remotely control the desktop of another computer—and it comes installed with Windows 2000. Because you're an expert, we assume that you've deduced the basics of NetMeeting. In this chapter, we explore some topics that are not covered in our more introductory book, *Running Microsoft Windows 2000 Professional* (Microsoft Press, 2000).

Another useful technology for using the Internet to communicate with friends and colleagues is Internet messaging. Microsoft offers an Internet messaging service called MSN Messenger Service. Although it doesn't come with Windows 2000, MSN Messenger Service is available as a free download from Microsoft. MSN Messenger Service allows you to chat with friends over the Internet whenever you are both logged on to the service. MSN Messenger Service is also tightly integrated with NetMeeting, as we explain in this chapter.

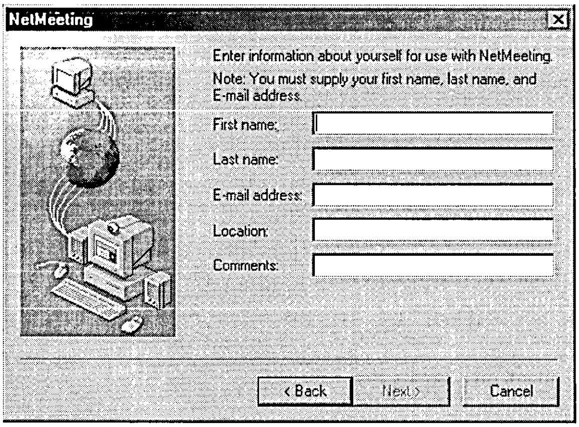
If you need something between text-based chatting and full conferencing, Microsoft Phone Dialer, another component of Windows 2000, lets you use the Internet to place phone calls. Phone Dialer also allows video, turning it into the picture telephone of early science fiction stories. Because Phone Dialer is less capable than NetMeeting in most respects, we don't cover it in this book. (At the risk of including too many plugs, you'll find Phone Dialer well documented in our other Windows 2000 book, mentioned previously.)

Using NetMeeting

NetMeeting is easy to use, with its basic functions intuitively accessible from the main window. The following sections provide some background information that will help you get the most out of NetMeeting.

Setting Up NetMeeting

NetMeeting is installed by default on Windows 2000. (You'll find its Start menu entry buried at Programs | Accessories | Communications | NetMeeting.) The first time you start NetMeeting, you are led through a setup wizard. You can cancel the wizard, but then you must enter the information in the Options dialog box before you can log on to a directory service. The setup wizard asks for information about you, your location, and what directory service, if any, you want to log on to. See Figure 29-1. *(For information about directory services, see the following section, "Finding People and Being Found.")* The setup wizard also summons the Audio Tuning Wizard to assist you in adjusting your speakers and microphone, if you have these installed.


NetMeeting

Enter information about yourself for use with NetMeeting.

Note: You must supply your first name, last name, and E-mail address.

First name:

Last name:

E-mail address:

Location:

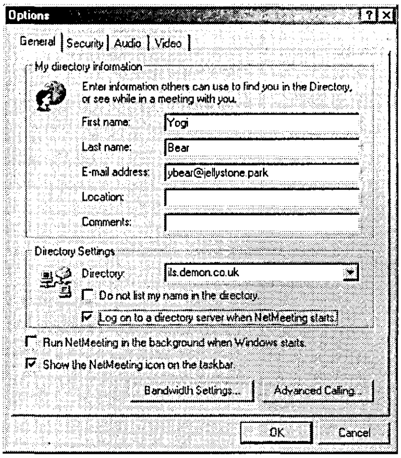
Comments:

Figure 29-1
To help set up NetMeeting, you need to enter information about yourself in a setup wizard.

Note It is not unheard of for people to enter phony names and e-mail addresses. Using a bogus e-mail address prevents your receiving unsolicited e-mail, and NetMeeting doesn't care whether the information is correct. However, people who search for you by e-mail address need to know what address you are using.

The setup wizard asks for the speed of your Internet connection. This is important because NetMeeting determines the optimal compression scheme and codec selections based on this setting. A *codec,* an abbreviation for *coder/decoder,* is the software-implemented algorithm for converting audio and video to digital form for transmission and back to audio and video again at the receiving end. If you change your Internet connection, be sure to update this setting by clicking Bandwidth Settings on the General tab of the Options dialog box.

All the items you enter in the setup wizard are available in the Options dialog box (shown in Figure 29-2), which you open by choosing Tools | Options. To change your directory service, type the name of the new service in the Directory text box on the General tab. All the services you have used in the past and the Microsoft Internet Directory are listed in the drop-down list. To rerun the Audio Tuning Wizard, click the Audio tab and then click Tuning Wizard.



Enter information others can use to find you in the Directory, or see while in a meeting with you.

First name: Yogi

Last name: Bear

E-mail address: ybear@jellystone.park

Location:

Comments:

Directory: ils.demon.co.uk

□ Do not list my name in the directory.

☑ Log on to a directory server when NetMeeting starts.

□ Run NetMeeting in the background when Windows starts.

☑ Show the NetMeeting icon on the taskbar.

Figure 29-2
Use the Options dialog box to set or change your identifying and directory service information.

Finding People and Being Found

To connect with another NetMeeting user, you need to know two pieces of information: whether the other party is available and the other party's IP address. You might already know the IP address of the person you want to contact and when that person is available. In that case, you can call the IP address directly (without using a directory), and your call can be completed. In most cases, though, you won't know one or both of these pieces of information. If your contact connects to the Internet through a modem, the IP address is likely to be different each time the contact logs on. All these considerations are applicable to other people trying to connect with you.

Note To determine your own IP address (so that you can provide it to others, for example), type *ipconfig* in a Command Prompt window. Alternatively, in NetMeeting choose Help | About Windows NetMeeting.

When you click the Find Someone In A Directory button or select Directory from the Call menu in NetMeeting, a directory window opens with options for locating the person you want to contact. The Select A Directory drop-down list offers places to look for people you've recorded (Windows Address Book, History, and Speed Dial) or from one or more directory services. Windows Address Book is the address list used by Microsoft Outlook Express. If you've added NetMeeting information for a contact in the Address Book, that contact will show up when you select Windows Address Book in the Find Someone window. The History list shows users you've contacted before. You can also add users to your Speed Dial list by right-clicking an entry in a directory list and choosing Add To SpeedDial List.

Directory services handle the collection and distribution of contact and IP address information for users logged on to their service. NetMeeting works with two kinds of directory services: Internet Locator Service (ILS) and the Microsoft Internet Directory. When you log on to a directory service, you are announcing to the world that you are available, and your IP address is published (though not displayed) in the directory. If you provided additional information during setup (location or comment, for example), the directory service might also publish that information.

NetMeeting does not allow simultaneous directory service connections; you can log on to only one at a time. Therefore, people looking for you must know which one you are using. You can, however, search for people on as many directory services as you like (unless you are using the Microsoft Internet Directory).

Using ILS Directories

An ILS is simply a listing of users of NetMeeting (and similar programs) who have logged on to that ILS. When users log on to an ILS, their identifying information (name, e-mail address, location, and comment) is entered in the ILS listing along with their IP address. If they have audio (speakers/microphone) or video (camera) equipment installed on their computer, that information is also noted in their ILS listing. To connect with someone listed in an ILS directory, look for that individual's listing in the directory and start a call using the listing.

You can find an extensive list of ILS servers at *www.netmeet.net/bestservers.asp*. If you want to find someone who is logged on to an ILS, you need to know the name of the ILS or you'll be out of luck. You must let your friends and business colleagues know which ILS you use so they can find you. And you should know the ILS they use. You can search for users on any ILS—not just the one you are logged on to.

Note Many ILS hosting services offer additional services for registered users such as specialized listing groups and audio/video greetings. Visit the Web sites of a few to see what they offer.

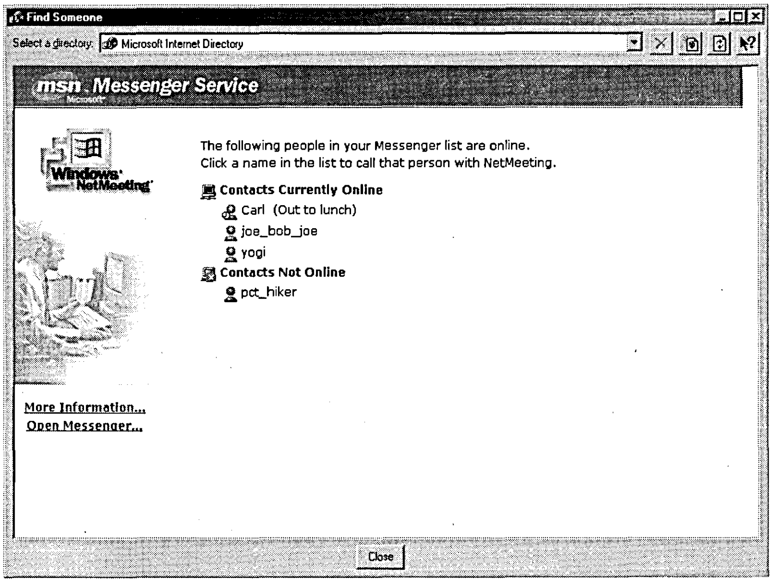
You can limit what is published about you when you log on to a directory service. You can also request that your entry not be displayed in the directory. To do this, open the Options dialog box and select Do Not List My Name In The Directory on the General tab. NetMeeting, however, does not require full or accurate information. For example, you must enter something in the E-mail Address field, but it could be all Xs or 9s or anything else. In the name fields, you can enter just your initials. Many (possibly even most) users enter fictitious information. This is another way to limit what is published about you.

Note Microsoft no longer hosts any ILS sites. Microsoft is focusing on the Microsoft Internet Directory using MSN Messaging Service. NetMeeting still supports ILS servers run by other parties.

Using Microsoft Internet Directory

The second type of directory service is the Microsoft Internet Directory. In the past, the Microsoft Internet Directory was an HTML front end to a Microsoft-hosted ILS (actually several ILSs). That is no longer the case. As of December 15, 1999, the Microsoft Internet Directory is based on the MSN Messenger Service directory. Like an ordinary ILS, it maintains a list of users logged on with identifying information and IP addresses. *For more information about MSN Messenger Service, see "Using Internet Instant Messaging," page 512.*

In order to use the Microsoft Internet Directory, you must have MSN Messenger Service installed and have a Microsoft Passport. Both are free. (You already have a Passport if you have a Hotmail account or an MSN account. Otherwise, you can obtain one with a visit to *www.passport.com.*) The Microsoft Internet Directory works somewhat differently than an ILS. The directory uses your MSN Messenger Service contact list, which you create and update within MSN Messenger Service. The Microsoft Internet Directory listing in NetMeeting shows only users in your contact list. (See Figure 29-3.) To use the Microsoft Internet Directory for connecting to other NetMeeting users, your NetMeeting session must be logged on to the Microsoft Internet Directory. This is different from using an ILS, because you do not have to be logged on to an ILS to view its directory. MSN Messenger Service does not have to be running unless you want to make changes to your contact list.



The following people in your Messenger list are online.
Click a name in the list to call that person with NetMeeting.

Contacts Currently Online
- Carl (Out to lunch)
- joe_bob_joe
- yogi

Contacts Not Online
- pct_hiker

More Information...
Open Messenger...

Figure 29-3
The Microsoft Internet Directory displays your MSN Messenger Service contact list.

Microsoft Internet Directory offers some important privacy advantages over ILS directories. Your name isn't broadcast to everyone who logs on to the directory; only those users who have added you to their list of MSN Messenger Service contacts can see your name and availability. This not only guards your own privacy but also shields you from the all-too-explicit listings that clutter many ILS directories.

Note

Although you get to specify your name as you want it to appear on others' screens (Microsoft Internet Directory uses the setting from MSN Messenger Service, not the one from NetMeeting), users can still see your e-mail address, which appears as a ScreenTip when they pause the mouse pointer over your name in the directory. If you don't want your NetMeeting correspondents to be able to pester you with e-mail, use passport.com as your Passport provider instead of hotmail.com or msn.com. The ScreenTip that appears displays an "address" (for example, *carl@passport.com*) that isn't actually linked to an e-mail account.

Using Advanced Calling Options

NetMeeting's compliance with Internet telephony standards enables you to take advantage of additional network communication facilities, namely gateways and gatekeepers. A *gateway* is a computer on your network that provides an interface to telephones and traditional video conferencing equipment. In NetMeeting, you communicate computer to computer. By going through a gateway, you can use NetMeeting to connect directly to someone's telephone or to a videoconference using standard telephone connections.

A *gatekeeper* is a computer on your network that controls the connections made across the gateway. A gatekeeper can be thought of as a combination router and proxy server for network telephony connections. It controls the number of connections and the bandwidth allotment for each call. It also manages network addresses for incoming calls.

If you have a gatekeeper account or use a gateway, open the Options dialog box and click Advanced Calling. In the Advanced Calling Options dialog box, enter the account information and respective IP address.

Considerations for Using Remote Desktop Sharing

The Remote Desktop Sharing feature of NetMeeting allows a person on one computer to operate another computer. This feature is especially useful in a help desk scenario where the help support personnel can operate the computer of the person needing help and, presumably, solve the problem directly. It can also be used by an individual who needs to run an office computer to operate a computer at home.

Two complications associated with Remote Desktop Sharing can limit its usefulness.

First, you must know the IP address of the computer you want to control. (If the computer is on your local network, you need to know only its network name.) If that computer is on a dial-up connection to the Internet, it will have a different address each time a connection is made. If you are the help desk person trying to take control of a user's computer, you must explain to the user how to figure out his or her IP address.

Note You can find your own IP address by choosing Help | About Windows NetMeeting. If you have separate connections to your local area network and to the Internet, you'll see an IP address for each one. (If you're not sure which is your IP address on the Internet, run Ipconfig.exe, which displays the adapter name along with each IP address.)

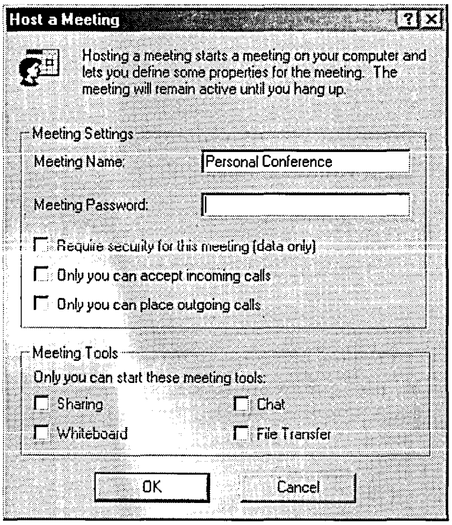
Second, the computer to be controlled must be connected to the Internet while waiting for someone to run Remote Desktop Sharing to control it. If you want to control your computer at home, you must leave it running and connected to the Internet. This can be a problem if you use a dial-up connection and your ISP disconnects you after a certain amount of idle time.

Implementing NetMeeting Security

NetMeeting provides security for three areas of program use:

- Password protection for hosted meetings and Remote Desktop Sharing
- Authentication of callers and meeting participants
- Encryption of chat, whiteboard, shared program, and file transfer data

When you host a meeting (by selecting Host Meeting from the Call menu), you can require a password for all participants by entering a password in the Meeting Password text box in the Host A Meeting dialog box, as shown in Figure 29-4. You need to let all the other meeting participants know the password so they can join.



Hosting a meeting starts a meeting on your computer and lets you define some properties for the meeting. The meeting will remain active until you hang up.

Meeting Settings

Meeting Name: Personal Conference

Meeting Password:

□ Require security for this meeting (data only)

□ Only you can accept incoming calls

□ Only you can place outgoing calls

Meeting Tools

Only you can start these meeting tools:

□ Sharing □ Chat

□ Whiteboard □ File Transfer

Figure 29-4
You can make a meeting secure by requiring a password.

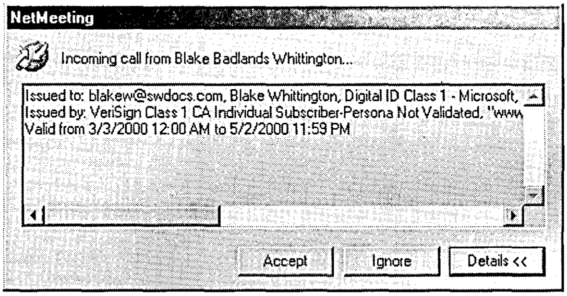
Controlling the Meetings You Host

By default, if you host a meeting and someone joins that meeting, that person can invite anyone else to join the meeting. If the meeting is password-protected, anyone who has the password can give it to anyone else. You might want to exercise more control over who joins your meeting. The Host A Meeting dialog box includes two options that give you such control. If you select Only You Can Accept Incoming Calls, a dialog box asks you to either accept or ignore users who try to join your meeting. If you select Only You Can Place Outgoing Calls, no one else will be able to invite new attendees.

You can also restrict which NetMeeting tools are used in your meeting. At the bottom of the Host A Meeting dialog box are check boxes giving you exclusive control over starting program sharing, chat, the whiteboard, and file transfer.

For Remote Desktop Sharing, calling a computer that's running Windows 2000 requires authentication with the password of that computer's Administrator account. This cannot be changed.

User authentication uses personal certificates to verify the identity of users. The NetMeeting documentation is a bit confusing when it comes to authentication. NetMeeting has no capacity for requiring authentication of connecting users (either in a normal call or a meeting) other than manually rejecting connections from anyone who does not supply a certificate. Users can offer a certificate as authentication of their identity. When a certificate is offered, the accept/ignore dialog box also has a Details button that, when clicked, displays the contents of the certificate. You can then decide to accept or ignore the connection, based on the contents of the certificate. See Figure 29-5. This is different than using certificates in IPSec, where authentication happens behind the scenes. *For information about the use of certificates for authentication, see "Managing Security on Your Site," page 472.*



Incoming call from Blake Badlands Whittington...

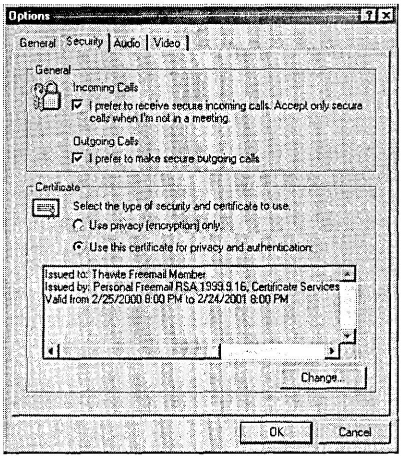
Issued to: blakew@swdocs.com, Blake Whittington, Digital ID Class 1 - Microsoft,
Issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated, "www
Valid from 3/3/2000 12:00 AM to 5/2/2000 11:59 PM

Figure 29-5
If a requesting connection supplies a certificate for authentication, you can view the contents of the certificate by clicking Details.

To supply a certificate when you call another NetMeeting user, select Use This Certificate For Privacy And Authentication on the Security tab of the Options dialog box, as shown in Figure 29-6. Then, from the list of personal certificates, select the one you want to use. This certificate will be used for both authentication and encryption.

Note that NetMeeting generates a certificate during setup that is used by default unless another one is selected. The NetMeeting certificate provides only an encryption key; it does not provide user authentication.

You can also secure a connection by encrypting its data. Securing connections is handled separately for incoming and outgoing calls—and hosting meetings is handled separately yet. On the Security tab of the Options dialog box (shown in Figure 29-6), select the check box under Incoming Calls to accept only secure calls. If you make this selection and someone calls you without securing the call, NetMeeting automatically rejects the call. The caller receives a message stating that you accept only secure calls. If someone calls you on a secure call, you see a message box similar to that shown in Figure 29-5 stating that a certificate is being used for privacy only. You can then accept or ignore the call.



General

Incoming Calls

☑ I prefer to receive secure incoming calls. Accept only secure calls when I'm not in a meeting.

Outgoing Calls

☑ I prefer to make secure outgoing calls

Certificate

Select the type of security and certificate to use.

○ Use privacy (encryption) only.

● Use this certificate for privacy and authentication:

Issued to: Thawte Freemail Member
Issued by: Personal Freemail RSA 1999.9.16, Certificate Services
Valid from 2/25/2000 8:00 PM to 2/24/2001 8:00 PM

Figure 29-6
You can require encryption on incoming or outgoing calls and supply a certificate for authentication.

The other side of the coin is securing the call you make to someone else. Select the box under Outgoing Calls to encrypt the calls you make to others. If you select this option and then make a call, the notice dialog box that appears on the screen of the person you call will have a Details option showing that the call you are making is using a certificate for privacy only. This occurs regardless of whether the party you are calling requires secure incoming calls.

These two selections apply only to calls between two users. If you want to use encryption to secure a meeting that you are hosting, select Require Security For This Meeting (Data Only) in the Host A Meeting dialog box. Then only users who have elected to use security on outgoing calls can join your meeting.

Audio and video are not securable. If you elect to use secure connections, you can't use the audio or video features. Chat, whiteboard, and program sharing all work on secured connections.

Using Policies and the Resource Kit Wizard

NetMeeting has a number of policies that control the way the program works. For example, the Set Call Security Options policy sets the level of security for incoming and outgoing calls automatically for all users of the computer. The NetMeeting policies can be found in two categories within Group Policy, which you can start by running Gpedit.msc. Computer Configuration\Administrative Templates \Windows Components\NetMeeting contains a policy that restricts Remote Desktop Sharing. The remaining policies are in User Configuration\AdministrativeTemplates

\Windows Components\NetMeeting. *For more information, see Chapter 18, "Using Group Policy."*

You can also set policies using the NetMeeting Resource Kit Wizard. The NetMeeting Resource Kit is included on this book's companion CD. (Alternatively, you can download it from *www.microsoft.com/windows/netmeeting/corp/reskit/NM3RK.exe.*) The Resource Kit provides two useful components: the NetMeeting Resource Kit documentation and the NetMeeting Resource Kit Wizard. The documentation is an extensive explanation of NetMeeting. The wizard allows you to create a distributable version of NetMeeting with preconfigured policy settings.

Note While NetMeeting is running, you cannot change the computer's display resolution or color depth. To change these settings, close NetMeeting first.

If NetMeeting is running when you start a program that attempts to change the display resolution or color depth (such as DirectX-based games), the program might not start because NetMeeting locks the display resolution and color depth. To fix the problem, close NetMeeting before starting other programs.

Integrating NetMeeting with Your Web Pages

You can add NetMeeting components to your Web pages in two ways: callto hyperlinks or ActiveX controls.

A callto hyperlink works in much the same way as a mailto hyperlink, which calls the user's default e-mail program. Callto hyperlinks instead call NetMeeting. Using one of the formats shown in Table 29-1 in the HTML of your Web page starts NetMeeting if it is not already running and places a call to the indicated party.

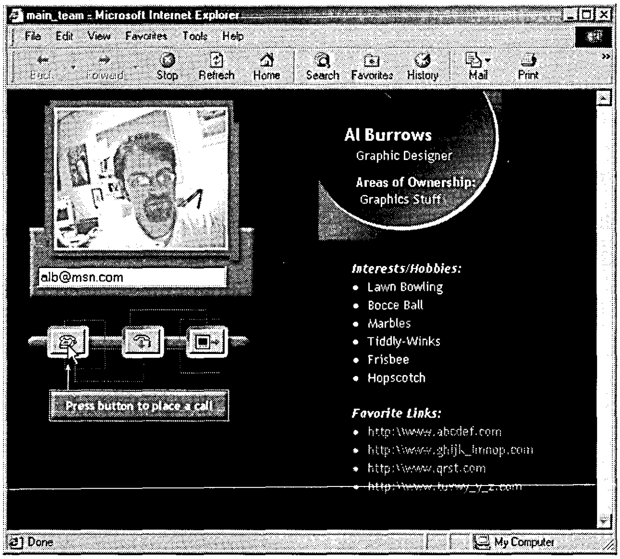
Table 29-1. Callto Formats

Callto Format	Example
callto:*server name/e-mail address*	callto:ils.ilshost.com/someone@microsoft.com
callto:*DNS name*	callto:machine2.test.com
callto:*IP address*	callto:10.0.0.124
callto:*e-mail address*	callto:someone@microsoft.com

You can also use the NetMeeting ActiveX component in your Web pages. In this case, the NetMeeting user interface resides on your Web page. To use the NetMeeting ActiveX component, you need to add the following code to your Web page:

```
<object ID="NetMeeting" CLASSID="CLSID:3E9BAF2D-7A79-11d2-9334-0000F875AE17"></object>
```

The sample page in Figure 29-7 uses the ActiveX component and some JavaScript to create a great-looking calling page.


main_team - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Done
My Computer

alb@msn.com

Press button to place a call

Al Burrows
Graphic Designer

Areas of Ownership:
Graphics Stuff

Interests/Hobbies:

- Lawn Bowling
- Bocce Ball
- Marbles
- Tiddly-Winks
- Frisbee
- Hopscotch

Favorite Links:

- http:\\www.abcdef.com
- http:\\www.ghijk_lmnop.com
- http:\\www.qrst.com
- http:\\www.tuvwy_y_z.com

Figure 29-7
Use scripting and the NetMeeting ActiveX component to embed NetMeeting features in your Web pages.

The NetMeeting Software Developers Kit (SDK) contains samples, include libraries, and documentation for writing C++ code using the NetMeeting ActiveX component and using the component in JavaScript and VBScript. Download the SDK from *www.microsoft.com/windows/netmeeting/authors/sdk/nm3sdk.exe.*

Most of the samples in the SDK are C++ code that needs to be built before it is run. Two of the samples (Teampage and ViewModes) are HTML and can be run without Visual C++. The Teampage sample uses JavaScript and VBScript calls to the NetMeeting components. Figure 29-7 shows the Teampage sample.

Using Internet Instant Messaging

Instant messaging, a text-based chat service, is yet another great benefit of the Internet. Friends use it to chat free (aside from Internet connection charges) with friends overseas. Family members keep in touch more regularly. Just seeing that a long-distance friend is logged on and only a click away gives one warm fuzzies.

You can download Microsoft's instant messaging software, MSN Messenger Service, free from Windows Update (*windowsupdate.microsoft.com*) or directly from *messenger.msn.com.* To use it, you need to register for a Microsoft Passport. A Passport is a user ID you can use at participating Web sites. Your existing Hotmail account or MSN account serves as a Passport. (Hotmail—*www.hotmail.com*—is a Web-based e-mail system run by

Microsoft. With a Hotmail account, you can access your e-mail from any Web browser anywhere in the world. MSN—*www.msn.com*—is a Microsoft-owned Internet service provider.) Your passport name becomes your MSN Messenger Service user name (and, by extension, your NetMeeting name when you log on to the Microsoft Internet Directory). As you can see, Microsoft's strategy is to integrate a variety of online communication capabilities. When you install MSN Messenger Service, you are given several opportunities to register for a Microsoft Passport.

Note The Web sites for the Microsoft Internet Directory and for MSN Messenger Service are not consistent in their stated requirements. The Microsoft Internet Directory site says that you need a Hotmail account. You really need a Microsoft Passport. A Hotmail account counts as a Passport.

MSN Messenger Service is constructed around your contact list, which is a list you construct of other MSN Messenger Service users you want to keep in touch with. The MSN Messenger Service window displays all your contacts who are currently logged on to MSN Messenger Service (either through MSN Messenger Service or NetMeeting) and those who are not. See Figure 29-8.

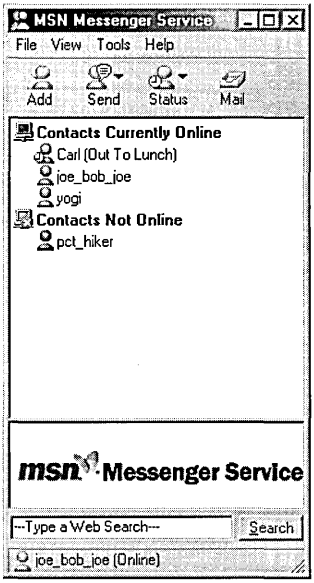


Figure 29-8
The MSN Messenger Service window is an unobtrusive addition to your desktop, but it allows you to be in immediate contact with family and friends.

From the main window, you can initiate a text-based chat session with any of your online contacts. You can also send e-mail to any contact, online or not. In keeping with Microsoft's plan of integrating services, you can invite a contact to a NetMeeting meeting. All these options are available by right-clicking a contact's name.

Chapter 30

Using Telnet

In This Chapter

Using the Telnet Clients 516
Running a Telnet Server 521

Telnet refers to both an Internet protocol and the programs that implement the protocol. The protocol was developed in the early days of network research and development as a means of executing commands on one computer from another computer over a network. In those days, personal computers were still a long way off. Most computing was done on mainframes or minicomputers where multiple users connected to the same computer using terminals (essentially a monitor and a keyboard). Terminals connected to a bank of serial ports on the computer, allowing users to interact with the computer using a command-line interface much like the Command Prompt window in Microsoft Windows 2000. The Telnet protocol allowed someone connected by terminal to one computer to emulate a terminal connection to another computer through a network connecting the two computers. Thus, a telnet client is called a *terminal-emulation program.*

Telnet is text-based in two ways:

- Telnet uses a command-line interface. It does not use a graphical user interface with icons you can drag and drop. You type commands and that's it. Some telnet programs for Windows operating systems come with some graphical trappings, but those tend to be peripheral.

- The Telnet protocol does not include any file-transfer capability. All that is transferred are textual commands and the responses to those commands.

Over the years, Telnet has been used widely by libraries making their catalogs available online and bulletin boards distributing information over the Internet. The use of Telnet today has been largely superseded by HTTP and the Web. Most of the information once available only through Telnet is now available on Web sites.

Telnet is still used by system administrators for remote administrative tasks and for special applications, however. It is also the only way to access some data archives that have never been updated for Web access.

Because a telnet client is a terminal-emulation program, it has a couple of configuration items peculiar to the use of terminals on mainframes and minicomputers. On those systems, different models of terminals handled some issues differently. For example, a user who wanted to delete the character he or she had just typed used the Backspace key on some terminals and the Delete key on others. Also, different computers expected different actions when the user pressed the Return key (now called the Enter key). Some systems expected a carriage return character, and some expected both a carriage return and line feed character. The choice of these options depended on the terminal and the configuration of the host computer. A computer kept configuration files that listed all the terminal types it needed to know about. These files were generally named *termcap* and the entries called *termtypes*. Part of the logon process was identifying the terminal type so that these configuration items would be properly set. Telnet has options for selecting a termtype to emulate as well as whether to send both a carriage return and line feed when you press Enter.

Using the Telnet Clients

Windows 2000 includes two telnet clients:

- **Command-line client.** The command-line telnet client (Telnet.exe) runs in a Command Prompt window and has no graphical interface additions. It is the same basic telnet client used years ago.
- **HyperTerminal.** HyperTerminal (Hypertrm.exe) is a terminal-emulation program that also includes a telnet client.

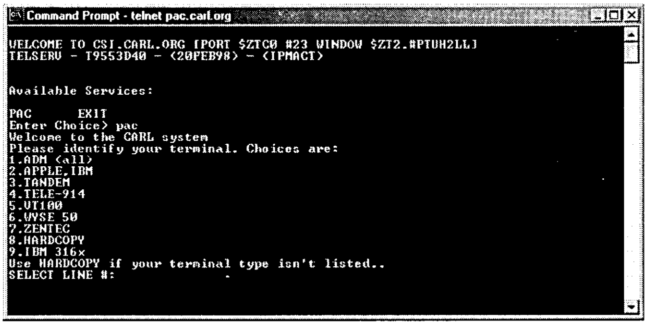
Note Windows 98 includes a telnet client (also called Telnet.exe) that provides a graphical user interface for basic telnet functions. (It uses menus and dialog boxes in much the same way that Notepad uses them to provide a GUI-based plain-text editor.) If Windows 98 is installed on your computer, you can use its telnet client in Windows 2000.

You can start a telnet client by clicking a Telnet link (in an Internet Explorer window) or by entering a Telnet address (including the *telnet://* protocol identifier) in any address bar. Windows then calls its default telnet client, which is determined by the (Default) value in the HKLM\Software\Classes\Telnet\Shell\Open\Command registry key. On a system that has Windows 2000 Professional newly installed, this value is set to *rundll32.exe url.dll,TelnetProtocolHandler %l*—which opens the command-line telnet program. However, the first time you open HyperTerminal, the value is changed to *C:\Program Files\ Windows NT\hypertrm.exe /t %1* and HyperTerminal becomes the default client. HyperTerminal makes the change only once. If you change the default back to the command-line client, you cannot change again to HyperTerminal simply by opening HyperTerminal. You must then manually change the registry value.

Of course, you can also start either telnet client directly. The easiest way to start the command-line client is to type *telnet* at a command prompt. To start HyperTerminal, click Start | Programs | Accessories | Communications | HyperTerminal.

Using the Command-Line Telnet Client

The command-line telnet client has two modes, local and remote. Before you make a connection, telnet is in local mode; after a connection is made, telnet is in remote mode. Telnet's internal commands are available in local mode. The commands of the computer to which you are connected are available in remote mode. In many cases, when you log on to a telnet server you enter a special program on that server, such as a library catalog or a bulletin board. Figure 30-1 shows an example session on the Colorado Association of Research Librarians (CARL) site.



```
VELCOME TO CSI.CARL.ORG [PORT $ZTC0 #23 WINDOW $ZT2.#PTUH2LL]
TELSERU - T9553D40 - (20FEB98) - (IPMACT)


Available Services:

PAC      EXIT
Enter Choice> pac
Welcome to the CARL system
Please identify your terminal. Choices are:
1.ADM (all)
2.APPLE,IBM
3.TANDEM
4.TELE-914
5.VT100
6.WYSE 50
7.ZENTEC
8.HARDCOPY
9.IBM 316x
Use HARDCOPY if your terminal type isn't listed..
SELECT LINE #:
```

Figure 30-1
Many telnet sessions begin with a request to identify your terminal type.

Start the telnet client from a command prompt. The syntax for the command-line telnet client is

```
telnet [address [port]]
```

If you supply an address, telnet automatically attempts to open a connection and, if successful, enters remote mode. Telnet normally connects on port 23, but some servers require a connection on another port. Unless you are notified of this requirement, you do not need to supply a port number. If you do not supply an address, telnet enters local mode, from which the commands listed in Table 30-1 are available. If you are in remote mode and want to execute a local command, you must precede the local command with the escape sequence (Ctrl+]). Press Enter to return to the remote session.

Table 30-1. Telnet Local Commands

Command	Action
close	Closes the current connection.
display	Displays telnet environment parameters. (See Table 30-2 for a list.)
open *host [port]*	Connects to a site. *Host* can be a host name or an IP address.
quit	Exits the telnet client.
set *param*	Turns on a telnet environment parameter. (See Table 30-2 for a list.)
status	Displays connection status information.
unset *param*	Turns off a telnet environment parameter. (See Table 30-2 for a list.)
? or help	Displays help information.

The command-line telnet client has four environment parameters that you can set. To turn on a parameter, use the set command; to turn off a parameter, use the unset command. The TERM parameter stores the terminal-emulation type. Use the set command and one of the terminal types listed in Table 30-2.

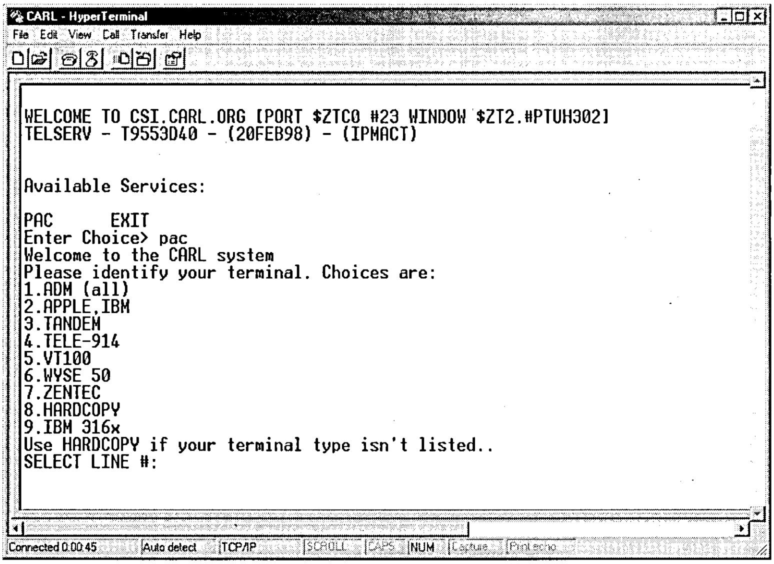
Table 30-2. Telnet Environment Parameters

Parameter	Description
NTLM	Turns on or off (set or unset) Windows NT LAN Manager (NTLM) authentication, which allows you to use your Windows 2000 user account to log on to a Windows 2000–based telnet server. When NTLM is off, your user name and password for logging on to a telnet site are sent as plain text. *For details, see "Running a Telnet Server," page 521.*
LOCAL_ECHO	Turns on or off (set or unset) LOCAL_ECHO. You should turn on LOCAL_ECHO if your keystrokes don't appear in the telnet display; this means that the server is not echoing the information you type back to your "terminal." If each character you type appears twice, turn off LOCAL_ECHO.
TERM *x*	Sets the terminal-emulation type (where *x* is ANSI, VT100, VT52, or VTNT). Select a terminal type that's supported by the telnet server you're connecting with; the default type is ANSI.
CRLF	Turns on or off (set or unset) sending both carriage return (CR) and line feed (LF).

The same command-editing and command-history features that you can use in a Command Prompt session are available in the command-line telnet client. *For information about these features, see "Editing the Command Line," page 180.* You can also use Doskey macros—predefined sequences of commands that you can recall by typing an abbreviation—within Telnet.exe, allowing you to quickly and easily enter commands and logon information that you use frequently. *For details, see "Using Doskey Macros in Programs," page 606.*

Using the HyperTerminal Telnet Client

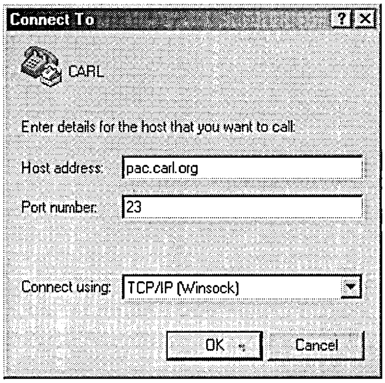
HyperTerminal is a utility that allows you to connect to other computers using dial-up or network connections. It is more general-purpose than the command-line telnet client and adds the convenience of the Windows graphical user interface. HyperTerminal allows you to store connection parameters for places you return to often. The HyperTerminal user interface also allows file transfers if the remote computer supports one of the transfer protocols (for example, Xmodem, Zmodem, or Kermit). Figure 30-2 shows a HyperTerminal connection to the CARL site. (Compare to Figure 30-1.)



```
WELCOME TO CSI.CARL.ORG [PORT $ZTC0 #23 WINDOW $ZT2.#PTUH302]
TELSERV - T9553D40 - (20FEB98) - (IPMACT)


Available Services:

PAC      EXIT
Enter Choice> pac
Welcome to the CARL system
Please identify your terminal. Choices are:
1.ADM (all)
2.APPLE,IBM
3.TANDEM
4.TELE-914
5.VT100
6.WYSE 50
7.ZENTEC
8.HARDCOPY
9.IBM 316x
Use HARDCOPY if your terminal type isn't listed..
SELECT LINE #:
```

Figure 30-2
HyperTerminal displays a Telnet connection within a window with menus and toolbar buttons.

To open HyperTerminal, click Start | Programs | Accessories | Communications | HyperTerminal. If the New Connection dialog box does not open automatically, choose File | New Connection. Enter a name for the connection and click OK. In the Connect To dialog box (see Figure 30-3), select TCP/IP (Winsock) from the Connect Using list. This action instructs HyperTerminal to make a Telnet connection. Enter the remote computer's name or address in the Host Address text box. Click OK; HyperTerminal stores the connection parameters and makes the connection.


Connect To

CARL

Enter details for the host that you want to call:

Host address: pac.carl.org

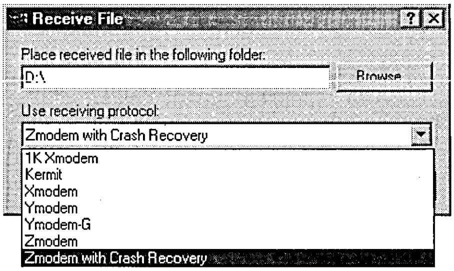
Port number: 23

Connect using: TCP/IP (Winsock)

Figure 30-3
HyperTerminal uses a dialog box for telnet session parameters.

If the remote server has file-transfer capabilities, you can use HyperTerminal to transfer files using a Telnet connection. The least sophisticated means of transferring a file is by capturing text. If you want to transfer a text file from the remote server to your computer, you can turn on text capture in HyperTerminal and then list the file within the telnet session. All the text transferred is stored in a text file. Choose Transfer | Capture Text, enter the name of the file in which you want to save the text, and click Start. In the telnet session, begin the file listing. When the listing is complete, choose Transfer | Capture Text | Stop. You might have to edit the text file that you captured to remove prompts and other extraneous text at the beginning or end of the file.

If the remote server has a file-transfer capability such as Xmodem, Zmodem, or Kermit, you can use HyperTerminal to transfer files using one of these protocols. In the telnet session, start the file transfer on the remote host using one of the transfer utilities. Then select Send File or Receive File from the Transfer menu. Enter the appropriate file names in the dialog box, select the protocol from the list corresponding to the protocol started on the remote server, and click Send or Receive. See Figure 30-4.


Receive File

Place received file in the following folder: D:\

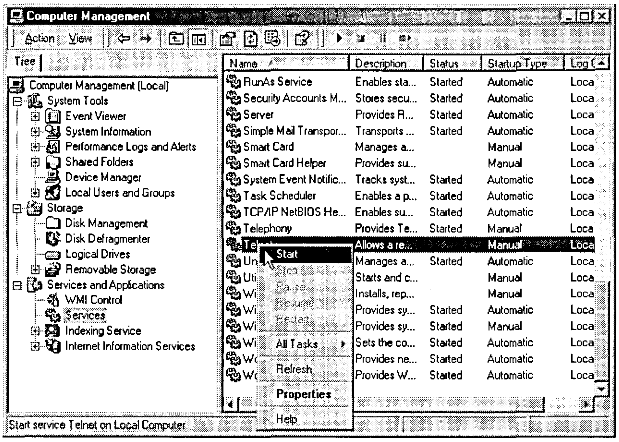
Use receiving protocol: Zmodem with Crash Recovery

Figure 30-4
Use HyperTerminal's file-transfer protocols to transfer files with Telnet.

Running a Telnet Server

Windows 2000 Professional comes with a telnet server, which runs as a service. It's not started by default. You can start the telnet server from the Services snap-in for Microsoft Management Console. (The Services snap-in is part of Computer Management; right-click My Computer and choose Manage. In Computer Management, navigate to Services And Applications\Services. Alternatively, start the Services snap-in in its own window by going to Start | Settings | Control Panel | Administrative Tools | Services or by typing *services.msc* at a command prompt.) *For more information about the Services snap-in, see Chapter 20, "Managing Services."*

To start the service, right-click Telnet and choose Start. See Figure 30-5. If you want the telnet server to start automatically when you start your computer, right-click Telnet and choose Properties. On the General tab of the Telnet Properties dialog box, select Automatic from the Startup Type list. (You can use Telnet Server Administration, described in the following paragraphs, to start and stop the Telnet service, but you can't use Telnet Server Administration to set the service to start automatically.)

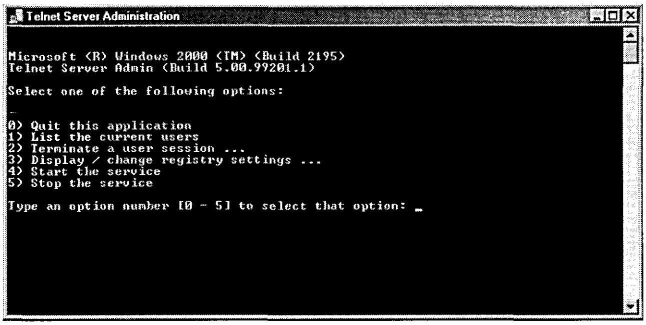


Name	Description	Status	Startup Type	Log (
RunAs Service	Enables sta...	Started	Automatic	Loca
Security Accounts M...	Stores secu...	Started	Automatic	Loca
Server	Provides R...	Started	Automatic	Loca
Simple Mail Transpor...	Transports ...	Started	Automatic	Loca
Smart Card	Manages a...		Manual	Loca
Smart Card Helper	Provides su...		Manual	Loca
System Event Notific...	Tracks syst...	Started	Automatic	Loca
Task Scheduler	Enables a p...	Started	Automatic	Loca
TCP/IP NetBIOS He...	Enables su...	Started	Automatic	Loca
Telephony	Provides Te...	Started	Manual	Loca
Te	Allows a re...		Manual	Loca
Un	Manages a...	Started	Automatic	Loca
Uti	Starts and c...		Manual	Loca
Wi	Installs, rep...		Manual	Loca
Wi	Provides sy...	Started	Automatic	Loca
Wi	Provides sy...	Started	Manual	Loca
Wi	Sets the co...	Started	Automatic	Loca
W(	Provides ne...	Started	Automatic	Loca
W(	Provides W...	Started	Automatic	Loca

Start service Telnet on Local Computer

Figure 30-5
You can start the telnet server from the Computer Management console.

Windows also provides a command-line server administration utility, Tlntadmn.exe. Click Start | Settings | Control Panel | Administrative Tools | Telnet Server Administration to launch it—or simply type *tlntadmn* at a command prompt. The Telnet Server Administration window appears with a list of options, as shown in Figure 30-6. *For more information about Telnet Server Administration, see Microsoft Knowledge Base (KB) article Q225233 on the companion CD.*



```
Microsoft (R) Windows 2000 (TM) (Build 2195)
Telnet Server Admin (Build 5.00.99201.1)

Select one of the following options:

0) Quit this application
1) List the current users
2) Terminate a user session ...
3) Display / change registry settings ...
4) Start the service
5) Stop the service

Type an option number [0 - 5] to select that option: _
```

Figure 30-6
The Telnet Server Administration window allows you to change server settings.

Several registry values control the operation of the telnet server. You can modify these values using Telnet Server Administration. Select option 3, Display/Change Registry Settings, and then select the registry value you want to change. Table 30-3 lists the registry values you can change. You can also change the registry values directly with a registry editor such as Regedt32.exe. The values for the telnet server service are located in the HKLM\Software\Microsoft\TelnetServer\1.0 registry key. *For more information about these registry values, see KB article Q226107.*

Table 30-3. Telnet Server Registry Values

Name	Data Type	Values
AllowTrustedDomain	REG_DWORD	0: Prevents users from logging on using an account from a trusted domain. 1: Allows users from a trusted domain to log on (default).
AltKeyMapping	REG_DWORD	Sets a key combination to emulate the Alt key, enabling users to send an Alt-key combination to programs running on the telnet server. Valid values are 0 (for Ctrl+A) through 25 (for Ctrl+Z).
DefaultDomain	REG_EXPAND_SZ	Specifies the default Microsoft Windows 2000 Server (or Microsoft Windows NT Server) domain for logon authentication.
DefaultShell	REG_EXPAND_SZ	Specifies the full path and command line of the shell or command interpreter that runs when a telnet user logs on. The default is Command Prompt (Cmd.exe).

(continued)

Table 30-3. Telnet Server Registry Values *(continued)*

Name	Data Type	Values
LoginScript	REG_EXPAND_SZ	Specifies the full path of a batch program to run when a telnet user logs on.
MaxConnections*	REG_DWORD	Despite this entry's default value of 63, the telnet server in Windows 2000 has a hard-coded limit of two simultaneous connections; changing this value has no effect.
MaxFailedLogins	REG_DWORD	Specifies the number of unsuccessful logon attempts before a user is disconnected. (The default is 3.)
NTLM	REG_DWORD	0: Disables Windows NT LAN Manager (NTLM) authentication. 1: Attempts NTLM first and then uses clear-text authentication. 2: Uses NTLM authentication only.
TelnetPort	REG_DWORD	Specifies the Transmission Control Protocol (TCP) port for Telnet connections. (The default is 23.)
TermCap*	REG_EXPAND_SZ	Specifies the full path to the terminal capabilities file, which defines keyboard layouts and key/code mappings.

*You can't set these values using Telnet Server Administration; to view or change them, you must use a registry editor.

By default, the Windows 2000 telnet server uses NTLM authentication for logging on users. NTLM is the challenge/response authentication protocol used by Windows NT and Windows 2000. With NTLM enabled, all users attempting to create a telnet session must have an NTLM-capable telnet client. Most telnet clients are not NTLM capable, so you might want to disable the requirement for NTLM authentication. You can change the requirement for NTLM authentication in two ways. You can change the registry value from the Telnet Server Administration window or you can use the telnet local mode command *set NTLM* or *unset NTLM*.

Whenever anyone logs on to your computer using Telnet, a logon script runs. By default, that file is %SystemRoot%\System32\Login.cmd. This is an ordinary batch program, which you can edit to modify the welcome banner or to run programs automatically when someone logs on. Edit the file using Notepad or some other plain-text editor. The logon script file name is stored in the LoginScript registry value. *For information about batch programs, see Chapter 37, "Using Batch Programs."*

Warning The default Login.cmd login script leaves connecting users at a command prompt. Depending on your computer's security settings, that result might provide much more access and control than you intend to grant to telnet users.

You can restrict the users allowed to connect to your computer using Telnet by creating a group named TelnetClients and adding the permitted users to that group. Windows 2000 recognizes that group name and, if it exists, authenticates only members of that group who attempt to log on to the telnet server.

Chapter 31

Using the FTP Clients

In This Chapter

Understanding FTP 525

Using the Command-Line FTP Client 527

Using the Graphical FTP Client in Windows Explorer 534

Using the Text-Based FTP Client in Internet Explorer 535

FTP (File Transfer Protocol) emerged from the same primordial networking soup as did TCP/IP. It's a no-frills workhorse for moving files from one computer to another over a network. The many FTP sites on the Internet offer everything from astrophysics research papers to archives of utilities for Windows, so you should find FTP a useful networking tool. It's not limited to downloads: when you upload files to your personal Web site hosted by your ISP, you'll also want to use FTP.

Microsoft Windows 2000 Professional comes with two FTP clients. One is the command-line utility Ftp.exe, which contains the full FTP feature set. The second FTP client is integrated with Windows Explorer. Microsoft Internet Explorer has always used FTP for downloading files. Now Windows Explorer adds a full-featured graphical user interface for FTP, making folders and files on an FTP server look and work much like files on a local hard drive.

In addition to these two clients, Internet Explorer offers a third alternative for interacting with FTP sites: a text-based view that visually resembles directory listings in MS-DOS—but contains hyperlinks for navigation and downloading.

Understanding FTP

The address of an FTP site is similar to that of a Web site. The uniform resource locator (URL) for an FTP site takes the form ftp://*sitename/foldername/filename* (for example, *ftp://ftp.microsoft.com/deskapps/readme.txt*). Using only the *sitename* in the address logs you in at the server's FTP root folder.

Establishing Connections

An FTP session requires a server and a client. The server responds to requests from clients. Typically, the server is the repository of files. Clients either upload files to the server or download files from the server. Clients can also perform other file operations such as renaming, creating folders, and deleting files—depending on the permissions granted by the FTP server.

To establish a connection, the client must log on to the server using an account on the server. The server controls the rights clients have and the activities clients can perform on the server's files based on the logon account. Many servers maintain a special "anonymous" account that allows anyone to log on to the server without having an account on that server. A user logs on with the user name *anonymous* and, typically, the password is the user's e-mail address. The e-mail address is usually optional, but entering a correct address is considered appropriate etiquette because that is how the server administrator monitors site use. In any case, you should not use a password that you use on your own system, because passwords are transferred as clear text.

Note Want to explore? You can find a huge list of FTP sites that allow anonymous logon at *hoohoo.ncsa.uiuc.edu/ftp*.

An FTP server might be running any one of several operating systems: Windows 2000, Windows NT, UNIX, Linux, and VMS are the most common. Each system has its own idiosyncrasies. FTP servers often have logon messages that give you information about the site, how to use it, or how its files are organized. Often, files are grouped in compressed archives. Your ability to browse might be limited by your permissions for certain folders. In any case, you are not allowed to browse anywhere outside the FTP server's root folder and its subfolders.

The protocol includes two file-transfer modes: ASCII and binary. ASCII is for text files; the character sets and end-of-line characters are translated if necessary to match those used by the receiving computer. Binary mode is for binary files such as executables, archives, and formatted documents; binary transfers copy an exact image of the file from one computer to the other.

FTP sites are often swamped with activity, which has given rise to mirror sites. A mirror site is an exact copy of an FTP site hosted by another server, which is used to offload excess demand from the primary server. Using a mirror site is often a faster means of downloading a file of interest.

Although FTP is an efficient protocol for transferring files, it has two drawbacks. First, it is not secure. Data is not encrypted, and passwords are passed as clear text. Second, FTP has no directory search capability. If you know what you are looking for, this drawback is mostly mitigated, of course. But transmitting and storing passwords as text can be a real concern if you use a Windows account to log on to a site.

Penetrating Firewalls and Proxy Servers

If you use FTP through a proxy server or a firewall, you could have a problem. When you connect to a remote computer with FTP, you create a connection used exclusively for commands and control (usually port 21). When you download a file, the server creates a second connection for the data stream (usually port 20 on the server) to avoid holding up the command stream. The problem can arise because the FTP server tries to create a connection between its port 20 and a port on your computer above 1024 (usually between 1025 and 5000). If your proxy server or firewall blocks connections on this range of ports, the server can't make the data connection. Depending on the FTP server, you might be notified that a problem exists.

Two solutions to this problem are available. The first is to open ports 1024 to 5000 for connection to remote port 20 on the proxy server or firewall. Doing this allows an FTP server to create the data connection while maintaining the security on your computer. The other option is to use passive mode. Passive mode instructs the FTP server not to create the data connection; instead, the client creates the data connection as well as the control connection. Because firewalls and proxy servers usually allow connections that are made from within the firewall, the client should not be blocked in creating the data link. The Windows Explorer–based FTP client uses nonpassive mode. The command-line FTP client can use passive mode by sending literal commands to the server. *For more information, see "Using Passive Mode," page 533.*

Using the Command-Line FTP Client

The command-line FTP client (Ftp.exe) is the older client that harkens back to the roots of the protocol. Open a Command Prompt window and type *ftp* to start the FTP client. The prompt changes to ftp>, and from there you can open FTP sites, browse their contents, and download or upload files.

The command-line format for starting FTP is

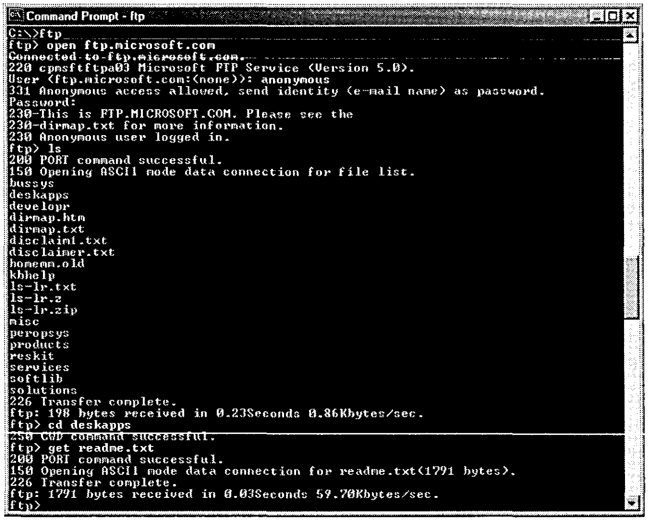
```
ftp [-v] [-n] [-i] [-d] [-g] [-s:filename] [-a] [-w:windowsize] [-A] [computer]
```

Table 31-1 describes the command-line switches. Note that, owing to its roots in the UNIX world, Ftp.exe identifies command-line switches with a hyphen (-), unlike most MS-DOS-based programs, which use a slash (/) as the switch identifier.

Table 31-1. FTP Command-Line Switches

Switch	Action
-v	Suppresses the display of messages from the remote server. Only necessary messages are displayed.
-n	Suppresses autologin upon initial connection.
-i	Turns off interactive prompting during multiple file transfers.
-d	Enables debugging, displaying all FTP commands passed between the client and the server.
-g	Disables file name globbing, which permits the use of wildcard characters (* and ?) in local file and path names.
-s:*filename*	Specifies a text file containing FTP commands; the commands automatically run after FTP starts. No spaces are allowed in this parameter. Use this switch instead of redirection (>).
-a	Use any local interface when binding data connection.
-w:*windowsize*	Overrides the default transfer buffer size of 4096.
-A	Log on as anonymous.
computer	Specifies the computer name or IP address of the remote computer to connect to. The computer, if specified, must be the last parameter on the line.

Figure 31-1 shows a full session of starting the FTP client, logging on to the Microsoft FTP server, viewing a directory listing, changing folders, and downloading a file.



```
C:\>ftp
ftp> open ftp.microsoft.com
Connected to ftp.microsoft.com.
220 cpmsftftpa03 Microsoft FTP Service (Version 5.0).
User (ftp.microsoft.com:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-This is FTP.MICROSOFT.COM. Please see the
230-dirmap.txt for more information.
230 Anonymous user logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
bussys
deskapps
developr
dirmap.htm
dirmap.txt
disclaimi.txt
disclaimer.txt
homemm.old
kbhelp
ls-lr.txt
ls-lr.z
ls-lr.zip
misc
peropsys
products
reskit
services
softlib
solutions
226 Transfer complete.
ftp: 198 bytes received in 0.23Seconds 0.86Kbytes/sec.
ftp> cd deskapps
250 CWD command successful.
ftp> get readme.txt
200 PORT command successful.
150 Opening ASCII mode data connection for readme.txt(1791 bytes).
226 Transfer complete.
ftp: 1791 bytes received in 0.03Seconds 59.70Kbytes/sec.
ftp>
```

Figure 31-1
This illustration has been "doctored" to differentiate the text you type (in bright white) from that generated by the system.

The command-line FTP client has several advantages over the graphical Windows Explorer–based FTP client. In general, it allows you to have more control over what is happening, and you get more feedback. Some commands are available with the command-line client that are not available with the graphical version (for example, append for appending a file to an existing file and trace for tracing packets). The command-line FTP client allows passive mode, whereas the Windows Explorer–based client does not. And in response to each command you send, the server returns at least one three-digit return code indicating the status of the command. You can see some of these codes in the listing shown in Figure 31-1. The first digit of each code identifies the type of message, as shown in Table 31-2.

Table 31-2. FTP Response Codes

First Digit	Description
1	The command was successful, but you need to wait for another response code before issuing your next command.
2	The command completed successfully.
3	The server needs more information before it can complete the request.
4	The system is too busy to process the command; you should try again later.
5	An error occurred; you should resolve the error before trying the command again.

Another advantage of command-line FTP sessions is that they're easy to automate. You can create files of FTP commands for transfers that you perform regularly. Entering *ftp -s:filename* at a command prompt runs the commands in the text file *filename*.

In addition, FTP provides the same command-editing and command-history features that are available in a Command Prompt session. *For information about these features, see "Editing the Command Line," page 180.* You can also use Doskey macros—predefined sequences of commands that you can recall by typing an abbreviation—within FTP, allowing you to quickly and easily enter frequently used commands and logon information. *For details, see "Using Doskey Macros in Programs," page 606.*

Entering FTP Commands

Starting Ftp.exe leaves you at an ftp> prompt. Now what? Typing *help* or *?* at the ftp> prompt displays a list of available commands. Typing *help command* or *? command* (replace *command* with the name of the command you're interested in) provides more information about a command. Table 31-3 describes the various command-line FTP commands.

Table 31-3. FTP Commands

Command	Description
! the	Opens a nested Command Prompt session within FTP session. Typing *exit* returns to the FTP session. This is useful, for example, for determining the local current folder or for working with local files while in an FTP session.
? or help	Lists the FTP commands.
? *command* or help *command*	Describes the *command* command.
append *localfile* [*remotefile*]	Appends a local file to a file on the remote computer using the current file-transfer mode.
ascii	Sets the file-transfer mode to ASCII. ASCII mode is on by default.
bell	Toggles bell mode, which sounds a bell when file transfers are complete. Bell mode is off by default.
binary	Sets the file-transfer mode to binary. Binary mode is not selected by default.
bye or quit	Ends the FTP session and returns to the command prompt.
cd *remotefolder* lcd *localfolder*	Changes the current folder on the remote or local computer.
close or disconnect	Closes the current connection to the remote computer.
debug	Toggles debug mode, which displays all commands sent to the remote computer. Debug is off by default.
delete *remotefile* mdelete *remotefiles* [...]	Deletes the file(s) from the remote system.
dir [*remotefolder*] [*localfile*] mdir *remotefiles* [...] *localfile*	Displays a list of a remote folder's files and subfolders. For mdir, you must include at least one remote file, and the last file name is interpreted as *localfile*, a text file where the listing is stored. If you want to display the list on-screen, use a hyphen (-) for *localfile*.
ls [*remotefolder*] [*localfile*] mls *remotefile* [...] *localfile*	Displays an abbreviated list of a remote folder's files and subfolders. For mls, you must include at least one remote file, and the last file name is interpreted as *localfile*, a text file where the listing is stored. If you want to display the list on-screen, use a hyphen (-) for *localfile*.

(continued)

Table 31-3. FTP Commands *(continued)*

Command	Description
get *remotefile* [*localfile*] or recv *remotefile* [*localfile*] mget *remotefile* [...]	Copies remote files to the local current folder using the current transfer mode. For get and recv, you can specify a local file name that is different from the remote file name.
glob	Toggles file name globbing. Globbing expands path and file names when wildcards are used. Globbing is on by default.
hash	Toggles hash printing mode. With hash printing mode on, a hash mark (#) is displayed for every data block transferred. The size of a data block is 2048 bytes.
literal *argument* [...] or quote *argument* [...]	Sends arguments to the remote server exactly as entered. Normally, the client translates the commands you enter into one or more server commands. If you turn on debugging, you can see the commands actually sent to the server. With the literal or quote command, you can bypass the client translation.
mkdir *folder*	Creates a new directory (folder) named *folder* in the remote current folder. Mkdir can create a lower-level folder, but only if all folders above it already exist.
open *computer* [*port*]	Opens a connection to the specified computer. The computer can be identified by IP address, URL, or computer name.
prompt	Toggles prompt mode. With prompt mode on, you are prompted to confirm each file in a multifile action. Prompt mode is on by default.
put *localfile* [*remotefile*] or send *localfile* [*remotefile*] mput *localfiles* [...]	Copies local files to the remote current folder using the current transfer mode. For put and send, you can specify a remote file name that is different from the local file name.
pwd	Lists the remote present working (current) folder. There is no corresponding command to determine the local present working folder.
remotehelp [*command*]	Requests help from the remote server. If no command argument is given, a list of commands recognized by the server is displayed.
rename *filename newfilename*	Renames the remote file *filename* to *newfilename*.
rmdir *folder*	Deletes the remote folder.

(continued)

Table 31-3. FTP Commands *(continued)*

Command	Description
status	Displays the current status of the FTP session, including any connection and the status of all toggle modes.
trace	Toggles packet tracing mode. With tracing mode on, the route of each packet is displayed. Tracing mode is off by default.
type [*transfermode*]	Displays or sets the file-transfer mode. If no mode is specified, the current mode is displayed. *Transfermode* is either ascii or binary.
user *username* [*password*] [*account*]	Identifies a user to the remote server. Allows you to change the account you are using during the FTP session.
verbose	Toggles verbose mode. When verbose mode is on, all responses from the server are displayed. Verbose mode is on by default.

Several commands have an "m" counterpart (for example, dir and mdir, ls and mls). The "m" stands for "multiple," and the respective command is meant to handle multiple files. (Note, however, that mkdir is not a form of kdir!) The syntax of each "m" command differs slightly from the corresponding standard command. In general, one or more remote file names are required, and remote file names using wild cards are expanded.

Note You can abbreviate any of the FTP commands. You need to type only enough characters to uniquely identify the command.

The FTP client uses common UNIX commands as well as MS-DOS commands. For example, to view a list of folder contents, you can use either ls (UNIX) or dir (MS-DOS).

Note FTP servers on different operating systems have a few idiosyncrasies. With some FTP servers, commands are case sensitive. If you are having problems, try typing commands in all lowercase letters only. UNIX path names use the forward slash (/) as opposed to the backslash (\) used by MS-DOS and Windows. UNIX-based FTP servers typically understand only folder names using the forward slash, whereas Windows-based FTP servers understand folder paths using either the forward slash or the backslash. It is generally best to always use the forward slash when using FTP. In addition, folder names and file names on a UNIX-based server can be case sensitive. For example, Readme.txt and README.txt might refer to two different files in the same folder. A Windows-based server could have only one file with the same spelling in a particular folder, and Windows doesn't care how you capitalize it in commands.

When retrieving nontext files, you must use binary mode. Because ASCII transfer mode is the default, you must switch by issuing the binary command. Using binary mode for text files is usually safe, but the result might look a bit different from an ASCII transfer.

Using Passive Mode

Passive mode instructs the FTP server to wait for the client to create the data link rather than attempting to create the link itself. Thus, passive mode works around the restriction in many firewalls and proxy servers that prevents incoming connections.

To use passive mode with the command-line FTP client, you must use the literal command (see Table 31-3) to send commands directly to the server. First you send the pasv command, and the server replies with a port to use for the data connection. Then you open a connection to that port. From there, you can send and receive data. For example, if you are connected to server 192.168.1.20, a passive mode session might look like the following:

```
ftp> literal pasv
227 Entering Passive Mode (192,168,1,20,12,34)
ftp> literal port 192,168,1,20, 12,34
200 Port Command Successful
```

The port number is returned in the last two numbers of the address (12, 34 in this example). They represent the high-order and low-order bytes of the port number (3106 in this case—12 times 256 plus 34). Notice that you use commas rather than periods in the address in the port command.

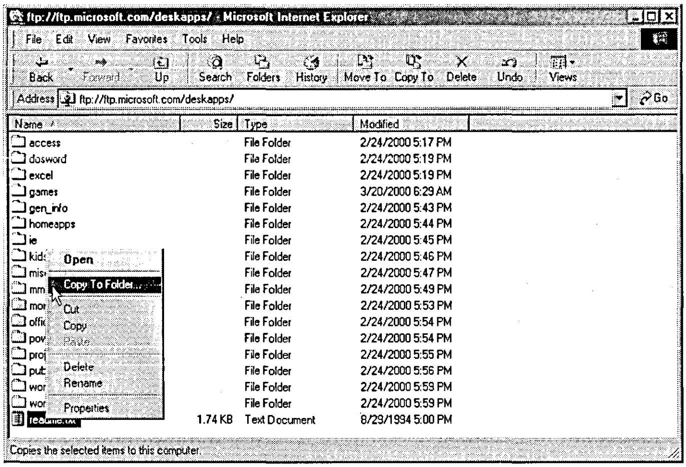
Then you must tell the server what data transfer you want to execute. Normally, the FTP client translates the commands you enter into one or more commands that the server recognizes. If you turn on debugging mode, these server commands are displayed. When you enter a command requiring a data transfer (for example, get, send, or ls), the client normally sends a port command to open a port and then sends the relevant command to transfer the data. When you use passive mode, you want to control the port that is used. Therefore, you must enter each server command yourself using the literal command—first the port command as just described and then the data transfer command. To perform the following common transfers, use these server commands after you issue the *literal port* command:

Client Command	Literal Server Command
ls (or dir)	nlist
get *filename*	retr *filename*
send *filename*	stor *filename*

Using the Graphical FTP Client in Windows Explorer

As we mentioned earlier, Windows 2000 comes with a graphical FTP client. Although it's a feature of Internet Explorer 5, it's actually implemented as a Windows Explorer shell extension. Whenever you enter an FTP address in the Address bar of a Windows Explorer or Internet Explorer window or click a link to an FTP site, you open the graphical FTP client.

The graphical FTP client provides most of the functionality of FTP in a familiar Windows Explorer environment—and it's much easier to use. Depending on the level of access you are allowed, you can browse an FTP site, download files, upload files, rename files, and move files. You can download, upload, and move files by dragging or by using menu commands. You cannot move files between FTP sites, however. Figure 31-2 shows the same operation—downloading the Readme.txt file from the Microsoft FTP site—that was depicted earlier in Figure 31-1.



Address: ftp://ftp.microsoft.com/deskapps/

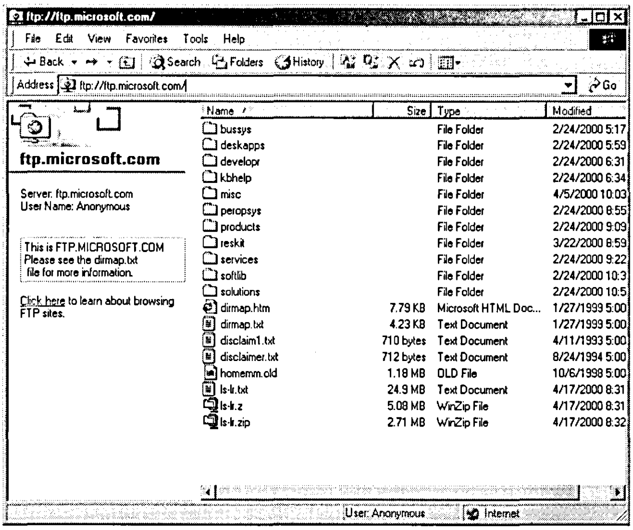
Name	Size	Type	Modified
access		File Folder	2/24/2000 5:17 PM
dosword		File Folder	2/24/2000 5:19 PM
excel		File Folder	2/24/2000 5:19 PM
games		File Folder	3/20/2000 6:29 AM
gen_info		File Folder	2/24/2000 5:43 PM
homeapps		File Folder	2/24/2000 5:44 PM
ie		File Folder	2/24/2000 5:45 PM
kid:		File Folder	2/24/2000 5:46 PM
mis		File Folder	2/24/2000 5:47 PM
mm		File Folder	2/24/2000 5:49 PM
mor		File Folder	2/24/2000 5:53 PM
offic		File Folder	2/24/2000 5:54 PM
pov		File Folder	2/24/2000 5:54 PM
proj		File Folder	2/24/2000 5:55 PM
put		File Folder	2/24/2000 5:56 PM
wor		File Folder	2/24/2000 5:59 PM
wor		File Folder	2/24/2000 5:59 PM
readme.txt	1.74 KB	Text Document	8/29/1994 5:00 PM

Copies the selected items to this computer.

Figure 31-2
You can download a file using familiar Windows-based procedures.

If you use the Copy To Folder command to download a file, you select the destination folder. (In contrast, the command-line client downloads only to the current working folder.) If a download is interrupted for some reason and the FTP server supports FTP Restart, you can start the download again and the client picks up where it left off. This is possible because the server periodically sends a marker containing the current position in the server's file system and the client records the marker in a restart control file, adding the position in the client's file system. When the transfer is taken up again, the client sends the marker to the server and they negotiate the best position to restart transmission. You can restart a transfer at any time as long as the restart control file still exists.

The welcome message that appears when you log on using the command-line FTP client is available in the graphical client by selecting FTP Server Welcome Message from the Help menu. The welcome message also appears at the left side of the window if you enable Web view (an option on the General tab of the Folder Options dialog box), as shown in Figure 31-3.



Address: ftp://ftp.microsoft.com/

Server: ftp.microsoft.com
User Name: Anonymous

This is FTP.MICROSOFT.COM
Please see the dirmap.txt
file for more information.

Click here to learn about browsing FTP sites.

Name	Size	Type	Modified
bussys		File Folder	2/24/2000 5:17
deskapps		File Folder	2/24/2000 5:59
developr		File Folder	2/24/2000 6:31
kbhelp		File Folder	2/24/2000 6:34
misc		File Folder	4/5/2000 10:03
peropsys		File Folder	2/24/2000 8:55
products		File Folder	2/24/2000 9:09
reskit		File Folder	3/22/2000 8:59
services		File Folder	2/24/2000 9:22
softlib		File Folder	2/24/2000 10:3
solutions		File Folder	2/24/2000 10:5
dirmap.htm	7.79 KB	Microsoft HTML Doc...	1/27/1999 5:00
dirmap.txt	4.23 KB	Text Document	1/27/1999 5:00
disclaim1.txt	710 bytes	Text Document	4/11/1993 5:00
disclaimer.txt	712 bytes	Text Document	8/24/1994 5:00
homemm.old	1.18 MB	OLD File	10/6/1998 5:00
ls-lr.txt	24.9 MB	Text Document	4/17/2000 8:31
ls-lr.z	5.08 MB	WinZip File	4/17/2000 8:31
ls-lr.zip	2.71 MB	WinZip File	4/17/2000 8:32

Figure 31-3
Enabling Web view displays the server URL, your current user name, and the server's welcome message at the left side of the window.

Unless you tell it otherwise, the graphical FTP client logs you on anonymously. To log on using another account, you can use either of these two methods:

- Insert the account name and password in the ftp address in this form:

  ```
  ftp://username:password@sitename
  ```

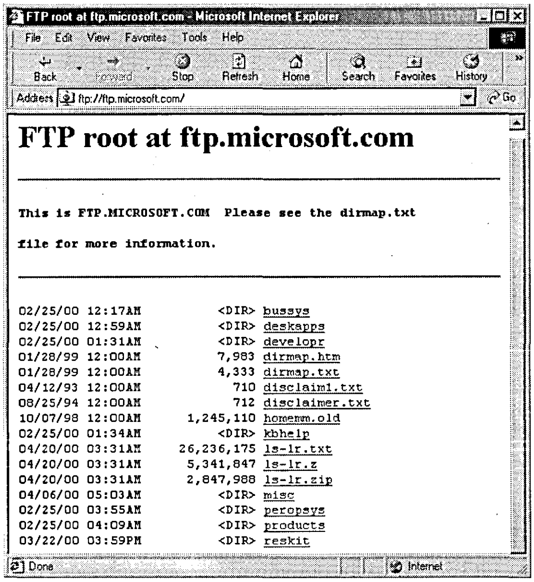
  If you omit the password, Windows prompts you for it. Note that using your password here leaves it displayed on your screen for any passersby to see.

- Use the Login As command on the File menu. (Login As also appears on the shortcut menu that opens when you right-click an unoccupied area of the Windows Explorer window—but only when you're already connected to an FTP site.) This command opens a dialog box in which you can enter your user name and password.

You can add FTP sites to your Favorites or to Network Places so that you can easily return to them.

Using the Text-Based FTP Client in Internet Explorer

The Windows Explorer–style graphical view of FTP sites is the default FTP client in Windows 2000. But if you prefer the convenience of clicking and you despise icons, a third option is available. Figure 31-4 shows the same site, *ftp://ftp.microsoft.com,* in this text-based view displayed in Internet Explorer.


FTP root at ftp.microsoft.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Address
ftp://ftp.microsoft.com/
Go
Done
Internet

FTP root at ftp.microsoft.com

```
This is FTP.MICROSOFT.COM  Please see the dirmap.txt

file for more information.

02/25/00 12:17AM        <DIR> bussys
02/25/00 12:59AM        <DIR> deskapps
02/25/00 01:31AM        <DIR> developr
01/28/99 12:00AM        7,983 dirmap.htm
01/28/99 12:00AM        4,333 dirmap.txt
04/12/93 12:00AM          710 disclaim1.txt
08/25/94 12:00AM          712 disclaimer.txt
10/07/98 12:00AM    1,245,110 homemm.old
02/25/00 01:34AM        <DIR> kbhelp
04/20/00 03:31AM   26,236,175 ls-lr.txt
04/20/00 03:31AM    5,341,847 ls-lr.z
04/20/00 03:31AM    2,847,988 ls-lr.zip
04/06/00 05:03AM        <DIR> misc
02/25/00 03:55AM        <DIR> peropsys
02/25/00 04:09AM        <DIR> products
03/22/00 03:59PM        <DIR> reskit
```

Figure 31-4
With this FTP client, you click a file name to download a file.

This client is limited in capability compared to either of the other clients included with Windows. Because it's cumbersome (and rather unsecure) to enter a user name and password, this client is best suited to sites that allow anonymous logon. It allows only browsing and downloading; you can't upload, move, delete, or rename files, regardless of your permissions.

To enable this client (and thereby disable the graphical client), open the Internet Options dialog box, click the Advanced tab, and clear the Enable Folder View For FTP Sites check box (under Browsing).

To log on to a site that requires a user name and password, you must embed them in the address as described in the preceding section. This FTP client doesn't offer a Login As command, nor does it have a command line where you can enter commands.

Part 8

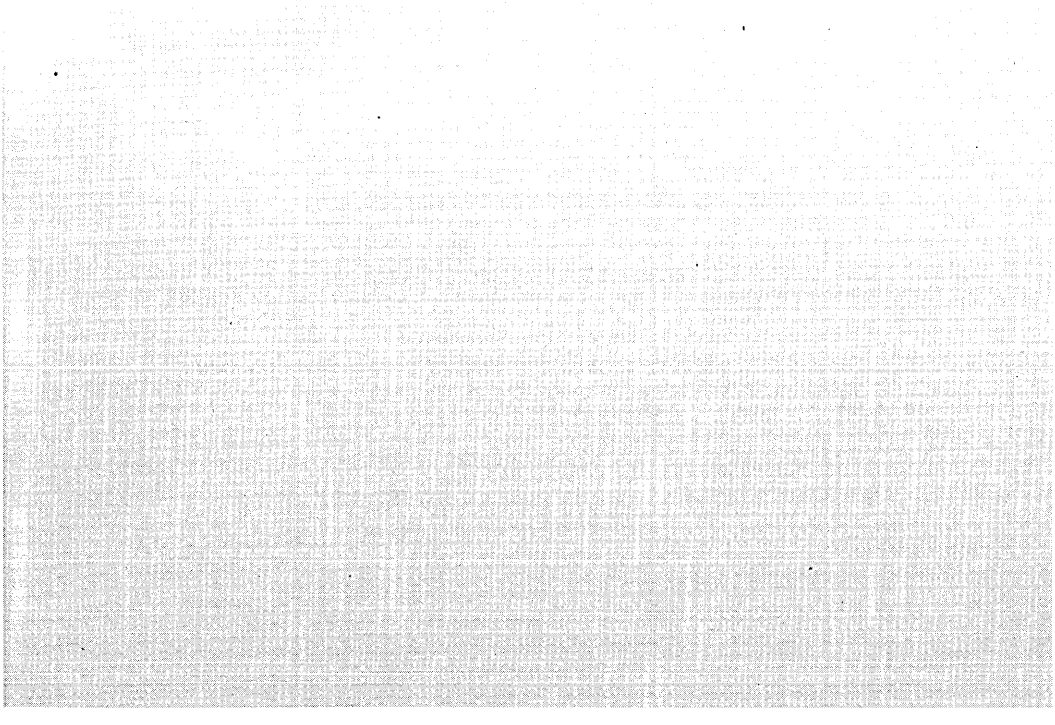
Managing Security

Chapter 32
Using the NTFS File System 539

Chapter 33
Using Encryption 555

Chapter 34
Auditing Security 573

Chapter 35
Managing Security Certificates 583



Chapter 32

Using the NTFS File System

In This Chapter

Selecting a File System 539
Securing Folders and Files 544
Using Volume Mount Points to Create Mounted Drives 548
Enforcing Disk Quotas 550

A *file system* defines the structure of the data on a volume and the way the data is organized and managed. For disks with read/write capabilities, Microsoft Windows 2000 supports two file systems: the NTFS file system and three variants of the file allocation table (FAT) file system (FAT12, FAT16, and FAT32). The FAT system (in its various permutations) has been used in all versions of Windows and MS-DOS. NTFS, which is used only in Windows NT and Windows 2000, has a number of advantages and features that are not available with FAT. Those advantages and features are the subject of this chapter.

Note Windows 2000 also supports two other file systems for CD and DVD media: Compact Disc File System (CDFS) and Universal Disk Format (UDF). For information about these file systems, as well as details on the structure and organization of NTFS and FAT volumes, see *Microsoft Windows 2000 Professional Resource Kit* (Microsoft Press, 2000).

Selecting a File System

Windows 2000 includes NTFS version 5, which offers several enhancements over previous versions. With few exceptions, NTFS should be the file system of choice for all your hard disk volumes.

Advantages of NTFS

The advantages of NTFS over other file systems include the following:

- **Security.** NTFS provides file-level access control. The permissions you set on files and folders on an NTFS volume apply to users who log on locally as well as those who connect to your computer over a network. These security settings are in addition to the share permissions that control network access. (Share permissions are also available for FAT volumes.) With NTFS security, you can specify for each folder and file which users and groups have access. Furthermore, you have more options on the type of access you allow than you do with share permissions on non-NTFS volumes. *For more information, see "Securing Folders and Files," page 544.*
- **Compression.** NTFS compression transparently compresses files as they're written to disk, thereby reducing the amount of disk space needed. Of course, Windows also decompresses the files transparently when it reads from disk. That's where the similarity to the DriveSpace compression feature included with Windows 9x ends. NTFS compression can be applied to a volume, a folder, or an individual file; DriveSpace can be applied only to an entire volume. Most important, with NTFS compression, if a compressed file becomes corrupt from a physical disk error, only that file is affected. With FAT compression in Windows 9x, a single corrupt sector could cause the loss of an entire volume. Ouch! *For details, see "Using NTFS File Compression," page 671.*
- **Recovery.** NTFS logs all changes made on an NTFS volume. Its transaction log ensures that disk operations are either completed correctly or rolled back to a known good state. The transaction log also allows Windows to redo or undo any changes to correct problems caused by a system failure or power loss; this happens transparently.
- **Encryption.** A new feature of Windows 2000 is the Encrypting File System (EFS), a service that provides file-level encryption for protecting your locally stored data. Only your user account can view files that you have encrypted. *For details, see Chapter 33, "Using Encryption."*
- **Volume mount points.** Volume mount points let you create mounted drives, whereby you assign a drive path to a volume instead of assigning a drive letter. This feature effectively lets you append a new volume to a path on an existing NTFS volume. Volume mount points also remove the limit of 26 mounted volumes imposed by the old system in which each volume had to be assigned a drive letter. *For more information, see "Using Volume Mount Points to Create Mounted Drives," page 548.*
- **Native property sets.** Files and folders on an NTFS drive can have descriptive properties associated with them, such as Title, Subject, Keywords, Author, and so on. You can view or modify these properties by clicking the Summary tab

in the properties dialog box for a file or folder. Some file types—notably Microsoft Office documents—provide a similar capability that shows properties regardless of the file system. Those Component Object Model (COM) properties are stored in the document itself, however. With NTFS, the COM-like native property sets are available for all types of files, including plain-text files. And these properties can be useful: the Indexing Service can index all properties on a file (including NTFS native properties and COM document properties), which means that you can search the index for files with certain properties. *For information about the Indexing Service, see Chapter 6, "Finding Files with the Indexing Service."*

- **Disk quotas.** Disk quotas allow members of the Administrators group to track and, optionally, limit each user's disk space on an NTFS volume. *For details, see "Enforcing Disk Quotas," page 550.*
- **Capacity.** NTFS can be used on huge volumes—up to 2 terabytes (TB). (A terabyte is roughly a trillion bytes, or a million megabytes.) You can have an unlimited number of entries in the root folder. Because NTFS uses smaller clusters, less disk space is wasted.

File Names on an NTFS Volume

Names of folders and files on an NTFS volume can be as long as 255 characters. You can use any characters except the following:

```
* | \ < > ? / " :
```

By default, Windows also creates an 8.3 name (eight-character name, three-character extension) for each folder and file, which provides compatibility with MS-DOS-based applications and 16-bit Windows-based applications. (You can see these file names by appending the /X switch to the Dir command at a command prompt.) If you no longer use any of these archaic programs, you can edit the registry to disable 8.3 file name creation. Doing so can speed up performance of your NTFS volumes.

To make this change, use a registry editor to navigate to the HKLM\System \CurrentControlSet\Control\FileSystem registry key. Change the data in the NtfsDisable8dot3NameCreation value to 1. The change becomes effective after your next restart.

Advantages of FAT

It's not yet time to write off FAT altogether. It has the following advantages over NTFS:

- **Speed.** In some cases, FAT volumes can be faster than NTFS volumes because of the overhead involved in managing NTFS. This is particularly true for small volumes with a large number of small files.
- **Small volume support.** FAT can be (and in fact must be) used on floppy disks and on small hard disks. (Although you can format a volume as small as 2 MB with NTFS, that leaves absolutely no room for storing data; the entire volume is consumed by NTFS overhead. Don't even consider NTFS for volumes smaller than about 200 MB.) On the other hand, FAT can't be used on large volumes. (The maximum recommended size for FAT16 is 511 MB; for FAT32 it's 2 GB.)
- **Compatibility.** The FAT file system is compatible with Windows 9x and Windows NT. However, compatibility is an issue only when your computer is set up to boot more than one operating system. (That is, if you boot into an operating system other than Windows 2000, you might not be able to access all the local volumes on your computer. *For more information, see "Using Compatible File Systems," page 49.*) Other users on your network (as long as you've granted them the requisite permissions) can access files in shared folders on your system, regardless of what file system you use and regardless of what operating system they're running.

Converting a Volume to NTFS

For the reasons explained in the previous sections, you might want to convert an existing FAT volume that you use only with Windows 2000 (or Windows NT) to NTFS. The Convert command lets you do just that, and, unlike formatting, it does so without destroying the files on the volume. Note, however, that this is a one-way process; once you convert to NTFS, there's no going back without formatting.

The Convert command needs some free space on your FAT volume to work its magic. Its first step is to calculate and report the amount of space needed, and it proceeds no further if adequate free space is not available. The calculation of the free-space requirement is a convoluted formula based on the size of the volume and the number of files and folders; it varies considerably from one drive to another. On today's typical drives, Convert can easily need 30 MB or more. For details about the calculation, see Microsoft Knowledge Base (KB) article Q156560.

To convert a volume to NTFS, type this command at a command prompt:

```
convert d: /fs:ntfs
```

Replace *d* with the letter of the drive you want to convert. The drive you specify can't be the current drive. If Windows 2000 can't lock all users off the drive—for example, if a running program is using a file on the drive or if the drive is being shared over the network—the conversion is delayed until the next time you restart your computer.

If you're interested in seeing the names of the folders and files on a drive as you convert it to NTFS, append the /V (verbose) switch.

If you're interested in getting the very best performance out of your hard drive, you might consider the alternative method to using the Convert command: backing up all your data to tape or to another volume, formatting the volume, and then restoring your data. The reason for the improved performance is the difference in the way the Convert and Format commands create the Master File Table (MFT)—the section of the volume that acts as a directory of the volume contents:

- When you format a volume (whether by using the Format command at the command prompt, the File | Format command in Windows Explorer, or the Action | All Tasks | Format command in Disk Management), Windows creates the MFT in a contiguous block at the beginning of the disk, the area that offers the fastest data transfer rates. In addition to the MFT itself, an NTFS volume includes an MFT "buffer zone"—an area that allows MFT growth with minimal fragmentation. Format places this buffer zone adjacent to the MFT.
- When you use the Convert command, Windows creates the MFT and its buffer zone wherever free space is available. This could be any location on the disk, and it might not be a contiguous block. Because Windows 2000 doesn't include any tools that let you defragment the MFT, you're stuck with this arrangement. (Some third-party utilities, such as Diskeeper from Executive Software, can defragment the MFT.)

The MFT is a single-file relational database of file information. It's an essential component of NTFS, because all information about a file—its size, time and date stamps, permissions, and data—is either stored within MFT entries or described by MFT entries. The MFT is continually referenced as the system locates data, reads data, and writes data to disk; therefore, improving its performance can make a significant difference.

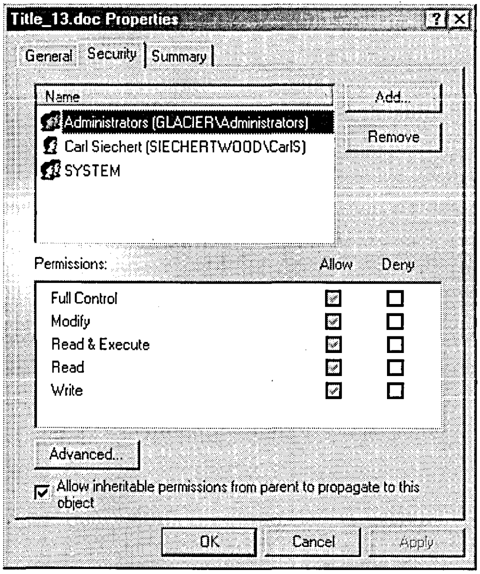
Note By adding an NtfsMftZoneReservation value to the HKLM\System\CurrentControlSet\Control\FileSystem registry key, you can specify the size of the MFT buffer zone before you format an NTFS volume. The default size is 12 percent of the total volume size, but you might want to increase this allocation if you intend to store a large number of small files. For details, see KB article Q174619.

Securing Folders and Files

NTFS security maintains an access control list (ACL) for each folder and file on an NTFS volume. When a user makes a request, the file system compares the user's security identifier (SID) with the SIDs included in the ACL. If the user's SID matches one in the ACL, the user is granted the level of access specified in the ACL. If the SID is not in the ACL, the user gets an error message and can't access the file. Simple, huh?

But how do SIDs get placed in an ACL? And what determines the access level for each SID? That's the subject of this section.

You can view or modify the names in an object's SID by displaying the Security tab of its properties dialog box. Figure 32-1 shows an example. The settings in this dialog box are pretty straightforward and are explained in detail in other texts, so we won't cover old ground here.



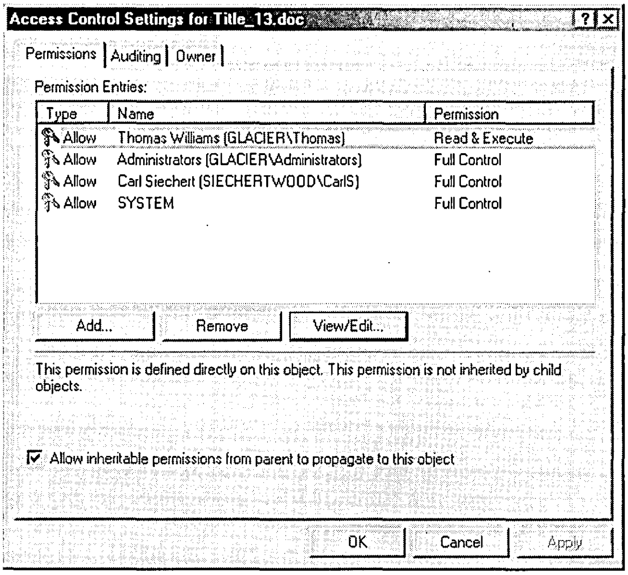
Administrators (GLACIER\Administrators)
Carl Siechert (SIECHERTWOOD\CarlS)
SYSTEM

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

Figure 32-1
On the Security tab, you can add or remove users or groups and then assign permissions to each one.

An area that's often left unexplored is the dialog box that appears when you click Advanced on the Security tab. (See Figure 32-2.) From that dialog box, you can add, remove, view, or edit individual permission entries. You'll seldom have any reason to do so, but you can set "advanced" permissions with this method. Advanced permissions are simply a breakdown of the basic permissions, which are visible on the Security tab. Table 32-1 shows the basic permissions and lists the advanced permissions that make up each basic permission. If you want to set a special combination of permissions that you can't create with the basic permissions alone, visit the dialog box shown in Figure 32-2.



Permission Entries:

Type	Name	Permission
Allow	Thomas Williams (GLACIER\Thomas)	Read & Execute
Allow	Administrators (GLACIER\Administrators)	Full Control
Allow	Carl Siechert (SIECHERTWOOD\CarlS)	Full Control
Allow	SYSTEM	Full Control

This permission is defined directly on this object. This permission is not inherited by child objects.

☑ Allow inheritable permissions from parent to propagate to this object

Figure 32-2
Clicking Advanced on the Security tab leads to a dialog box like this one, in which you can set custom permissions.

Table 32-1. Basic File Permissions

Permission	Description	Advanced Permissions
Read	Allows the user to view the contents of a data file	• List Folder / Read Data • Read Attributes • Read Extended Attributes • Read Permissions • Synchronize
Read & Execute	Allows the user to run a program file	• All Read permissions listed above • Traverse Folder / Execute File
List Folder Contents*	Allows the user to display folder contents	• All Read & Execute permissions listed above
Write	Allows the user to change the contents of the file	• Create Files / Write Data • Create Folders /Append Data • Write Attributes • Write Extended Attributes • Read Permissions • Synchronize
Modify	Allows the user to read, change, or delete the file	• All Read & Execute permissions listed above • All Write permissions listed above • Delete

(continued)

Table 32-1. Basic File Permissions *(continued)*

Permission	Description	Advanced Permissions
Full Control	Allows full control of the file	• All permissions listed above • Delete Subfolders And Files • Change Permissions • Take Ownership

* List Folder Contents, which is available only on the Security tab for a folder, provides the same individual permissions as Read & Execute. The difference is the way the permissions are inherited. List Folder Contents permission is inherited by folders but not by files within the folders; Read & Execute permission is inherited by folders and files.

One area that can cause confusion is inheritance. A shaded check box in the Permissions area of the Security tab (Figure 32-1) indicates an inherited permission, which means that the permission has been inherited from the object's parent. The parent of a folder or file object is the folder that contains it. A shaded check box, therefore, indicates a permission that is applied by default because the file was created in a folder with that check box selected.

Inheritance is a wonderful feature that allows you to apply permissions to many files with a single change at the top of the inheritance chain. (And inherited properties are handled more intelligently in NTFS 5 than in previous versions. Instead of retaining a complete ACL for each object—wasting disk space and time to look up ACLs—NTFS now stores only a pointer to the ACL that is the source of the inherited permissions.) By default, all objects are set to inherit permissions, as shown in Figure 32-1.

You can change or override inherited permissions in the following ways:

- Change the permissions for an object's parent; the changed permissions will be inherited automatically.
- Select the opposite setting (Allow or Deny) to override a specific inherited permission.
- Apply additional permissions (that is, permissions for another user or group, or additional check boxes for a user or group that already obtains some permissions through inheritance).

Breaking the inheritance chain so that you can apply direct permissions exclusively is also easy: simply clear the check box at the bottom of the Security tab. Windows then asks what you want to do with the existing inherited permissions. You can remove them altogether or you can copy them to the object. Either way, you can then modify the permissions as needed; your changes apply to that object and to its child objects, if any.

Cacls.exe, a command-line utility, provides another way to view and edit permissions. With Cacls (presumably, short for *change ACLs*), you can view existing permissions simply by typing *cacls filename* at a command prompt, replacing *filename* with the name of the file you're interested in. The display isn't particularly friendly, however. For example, next to each user account name, Cacls displays a single letter for any of three standard permission settings:

- F (for *full control*) is equivalent to having all Allow boxes selected on the Security tab.
- C (for *change*) is equivalent to having all Allow boxes selected except Full Control.
- R (for *read*) is equivalent to having the Allow boxes for Read and Read & Execute selected.

Any other combination of settings from the Security tab or the advanced permissions dialog box generates output only a programmer could love. Nonetheless, Cacls can be useful for quickly finding the permissions for an object—particularly if you're already working in a Command Prompt window. As an administrator, you should remember that it's in your toolkit.

Caution You can also set permissions with Cacls—but we recommend that you don't. It's too easy to make a mistake that causes you to lose existing permissions on a file. If you append the /E switch (which is supposed to edit the existing ACL instead of replacing it), Cacls sometimes garbles the permissions settings because it's based on an old NTFS inheritance model.

Who Is SID?

Windows 2000 security relies on the use of a security identifier to identify a user. When you create a user account, Windows assigns a unique SID to that account. The SID remains uniquely associated with that user account until the account is deleted, whereupon the SID is never used again—for that user or any other. Even if you recreate an account with identical information, a new SID is created.

A SID is a variable-length value that contains a revision level, a 48-bit Identifier Authority value, and a number of 32-bit subauthority values. You'll sometimes see the SID, which takes the form S-1-*x*-*y1*-*y2*-..., in a security dialog box before Windows has had time to look up the user account name. S-1 identifies it as a revision 1 SID; *x* is the value for the IdentifierAuthority; and *y1*, *y2*, and so on are values for subauthorities.

Using Volume Mount Points to Create Mounted Drives

Volume mount points allow you to assign, for any local volume, a path to a folder on a local NTFS volume. For example, you could assign your CD-ROM drive to a folder named CD and thereafter address it as C:\CD instead of drive D. (You can retain the existing drive letter too; for each volume you can assign one drive letter and any number of alternative drive paths.) The volume that hosts the mounted drive must be an NTFS volume, because volume mount points are a unique feature of NTFS. The volumes that you mount, however, can be formatted with any file system: NTFS, FAT, FAT32, CDFS, and so on.

This can be very useful, for example, if your boot volume is becoming full and you don't have room to install more programs in the \Program Files folder. Solution: install an additional hard disk, create a volume on the disk, move the contents of your existing \Program Files folder to the new volume, and mount the new volume to your (now empty) \Program Files folder. Instant expansion! You couldn't do this by simply moving your \Program Files folder to a new drive, because the registry, shortcuts, and other configuration files are littered with references to the full path of your programs, including the drive letter. By creating a mounted drive in the \Program Files folder, all your programs continue to work because—as far as they can tell—the files are still on drive C (or wherever your \Program Files folder resides).

Note As an alternative to moving the existing content, you could create a More Programs subfolder in your existing \Program Files folder and mount the new volume to the subfolder. (You can mount a volume only to an empty folder.) When you install a new program, change its target folder from a subfolder of \Program Files to a subfolder of \Program Files\More Programs.

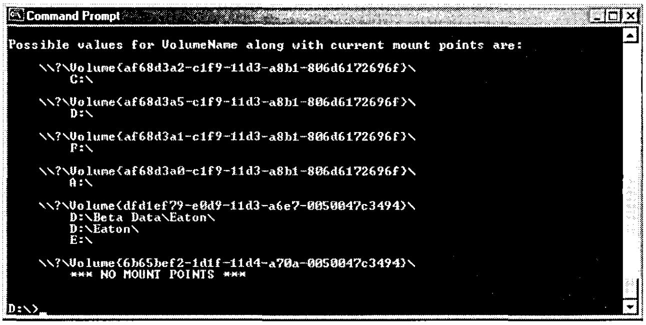
Here's another scenario: You might want to store documents for different purposes (say, work and personal projects) on two different drives. Your work documents, for example, should be stored on your local hard drive; you want your personal documents on your Zip drive. Because many programs use My Documents as their default folder for storing new documents, you must switch between drives to store the documents on the appropriate drive. Solution: create a mounted drive that links the Zip drive to an empty folder in My Documents. Thereafter, the Zip drive appears as a subfolder of My Documents, and switching between that drive and other folders in My Documents becomes much easier.

Note In this scenario, you might want to mount a network drive. Alas, you can't do that with NTFS volume mount points. If your computer is part of a Microsoft Windows 2000 Server–based domain, you can use Distributed File System (Dfs) to perform this type of drive mapping.

Mounted drives act exactly like any other subfolder. The only difference you'll notice is that in Windows Explorer, the folder that hosts the mounted drive (the volume mount point) appears with a drive icon instead of a folder icon. If you use the Dir command in a Command Prompt window to display a folder directory, volume mount points are identified as <JUNCTION> (for *junction point*, another name for volume mount point), whereas ordinary folders are identified as <DIR> (for *directory*, the MS-DOS term for a folder).

You create mounted drives using the Disk Management snap-in. *For details, see "Assigning a Drive Letter or Drive Path," page 215.*

As an alternative to the Disk Management snap-in, you can use Mountvol.exe, a command-line utility. In a Command Prompt window, type *mountvol* to display Mountvol syntax information, a list of globally unique identifiers (GUIDs) for your local volumes, and a list of current mounted drives. Figure 32-3 shows an example. To create or delete a mounted drive using Mountvol, you must use the GUID of the volume you want to link to a volume mount point. Because of the difficulty of accurately typing a GUID, even diehard command-line fans might eschew Mountvol.exe in favor of Disk Management.



```
Possible values for VolumeName along with current mount points are:

    \\?\Volume{af68d3a2-c1f9-11d3-a8b1-806d6172696f}\
        C:\

    \\?\Volume{af68d3a5-c1f9-11d3-a8b1-806d6172696f}\
        D:\

    \\?\Volume{af68d3a1-c1f9-11d3-a8b1-806d6172696f}\
        F:\

    \\?\Volume{af68d3a0-c1f9-11d3-a8b1-806d6172696f}\
        A:\

    \\?\Volume{dfd1ef79-e0d9-11d3-a6e7-0050047c3494}\
        D:\Beta Data\Eaton\
        D:\Eaton\
        E:\

    \\?\Volume{6b65bef2-1d1f-11d4-a70a-0050047c3494}\
        *** NO MOUNT POINTS ***

D:\>_
```

Figure 32-3
The Mountvol command shows the current mount points for each volume, which is identified by its GUID.

In Figure 32-3, you can see that the volume with GUID {dfd1ef79-e0d9-11d3-a6e7-0050047c3494} (the fifth one in the list) actually has *three* mount points. You can navigate to its files by going to either of two folders on drive D (\Beta Data\Eaton or \Eaton) or by using its drive letter, E. The last volume in the list has no mount points—that is, no drive letter or path—so it's essentially unusable in its current configuration.

Suppose you want to use that volume to create a mounted drive so that it appears in your folder hierarchy as D:\Newvol. To do that using Mountvol, open a Command Prompt window and enter the following commands:

```
md newvol

mountvol newvol \\?\Volume{6b65bef2-1d1f-11d4-a70a-0050047c3494}\
```

You can find more information about Mountvol.exe in KB article Q205524. In addition, that article describes Linkd.exe, a command-line utility included with the *Microsoft Windows 2000 Professional Resource Kit,* which lets you mount *any* folder (not just the root folder) to a volume mount point on a local NTFS drive.

Enforcing Disk Quotas

Disk quotas, a new feature of Windows 2000, allow you to monitor and limit disk-space usage. You set quotas for each user and each volume. Quotas are tracked separately for each volume, even for separate volumes on the same hard disk. Disk quotas are based on uncompressed file sizes; compressing files doesn't increase the amount of free space available to a user.

Using disk quotas causes a slight performance reduction, so you might want to enable them only periodically. That way, you can identify users who are using too much disk space without incurring the performance hit all the time.

With disk quotas enabled, volume usage is tracked by file ownership. That is, a file counts against a user's quota if the SID of the file's owner is the same as the user's SID.

Note Disk quotas rely on the SID, not the user account name. In a workgroup environment—where each user has a separate, identically named user account on each computer—this can cause quotas to be less reliable than in a domain. That's because the user's account on each computer has a different SID. Depending on how a file is created, it might be owned by the user's account on a different computer. If your NTFS volume contains files that are owned by a user account from another computer, you'll see the owner's SID in the Quota Entries window instead of (or in addition to) the user's name.

Enabling Disk Quotas

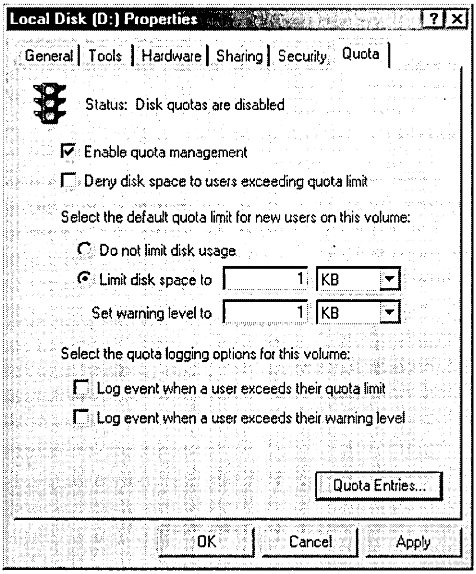
You can enable disk quotas in either of two ways:

- You can make individual settings using the Quota tab in a volume's properties dialog box.
- You can use Group Policy to apply consistent settings to all volumes on a computer.

To enable quotas using the properties dialog box:

1. While logged on as a member of the Administrators group, right-click a disk in My Computer and choose Properties.

2. Click the Quota tab and select the Enable Quota Management check box to enable the other items on the Quota tab.



Local Disk (D:) Properties

Status: Disk quotas are disabled

☑ Enable quota management

□ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

○ Do not limit disk usage

● Limit disk space to 1 KB

Set warning level to 1 KB

Select the quota logging options for this volume:

□ Log event when a user exceeds their quota limit

□ Log event when a user exceeds their warning level

3. Set the other options on the Quota tab:

   - Select Deny Disk Space To Users Exceeding Quota Limit if you want Windows to prevent users from saving files that would exceed their assigned space limit. (They'll see an "insufficient disk space" error message.) If you don't select this check box, Windows doesn't stop users from exceeding their limit—but it allows you to track disk usage by user.
   - To specify a default limit for new users (that is, users who don't have an entry in the Quota Entries window, described in the following section), select Limit Disk Space To and set a limit and a warning level. (Exceeding the warning level doesn't trigger a warning to the user, but administrators can use this setting to more easily monitor users who are nearing their limit.) If you don't want to set limits on new users, select Do Not Limit Disk Usage.
   - If you want Windows to make an entry in the System log whenever a user exceeds his or her quota limit or warning level, select the appropriate check box.

To enable disk quotas using Group Policy:

1. In the Group Policy console (Gpedit.msc), navigate to Computer Configuration \Administrative Templates\System\Disk Quotas. *(For details about Group Policy, see Chapter 18, "Using Group Policy.")*

2. Enable the Enable Disk Quotas policy.
3. Make other policy settings:
   - Enable Enforce Disk Quota Limit to prevent users from saving files that would exceed their assigned limit.
   - Enable and configure Default Quota Limit And Warning Level to specify default limits for new users.
   - Enable Log Event When Quota Limit Exceeded, Log Event When Quota Warning Level Exceeded, or both if you want Windows to record disk quota violations in the System log.

Using Group Policy to enable disk quotas instead of using the Quota tab produces several effects:

- Policy settings affect disk quotas for all local NTFS volumes.
- Policy settings in Computer Configuration\Administrative Templates\System \Disk Quotas override their counterparts on the Quota tab in the properties dialog box and in the Quota Entries window. For example, if disk quotas are enabled (or disabled) through Group Policy, no one can change that setting via the Quota tab. As an administrator, you can override the default limits by modifying quota entries for particular users, however.

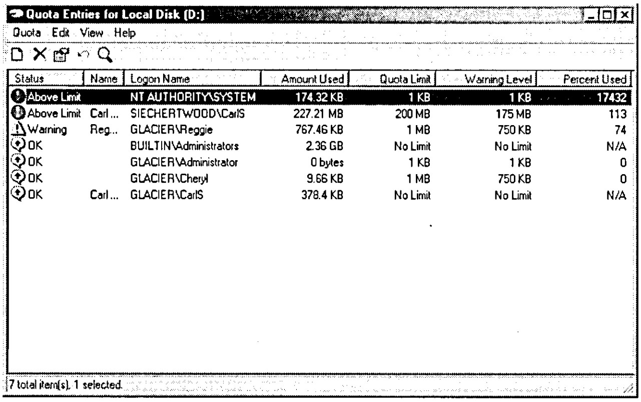
Enabling Disk Quotas on Remote Volumes

You can enable disk quotas on other computers on your network as long as the following conditions are met:

- The other computer must be running Windows 2000.
- The volume to be managed must be formatted as NTFS, and it must be shared from the volume's root folder.
- You must be a member of the Administrators group on the other computer.

Managing Disk Quotas

When you enable quotas on a volume that has existing files, Windows calculates the disk space used by each user who has created, copied, or taken ownership of the existing files. The default quota limits and warning levels are then applied to all current users and to any new user who saves a file. To view and modify the quota entries, open the disk's properties dialog box, click the Quota tab, and click Quota Entries. The Quota Entries window opens, as shown in Figure 32-4.



Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
Above Limit		NT AUTHORITY\SYSTEM	174.32 KB	1 KB	1 KB	17432
Above Limit	Carl ...	SIECHERTWOOD\CarlS	227.21 MB	200 MB	175 MB	113
Warning	Reg...	GLACIER\Reggie	767.46 KB	1 MB	750 KB	74
OK		BUILTIN\Administrators	2.36 GB	No Limit	No Limit	N/A
OK		GLACIER\Administrator	0 bytes	1 KB	1 KB	0
OK		GLACIER\Cheryl	9.66 KB	1 MB	750 KB	0
OK	Carl ...	GLACIER\CarlS	378.4 KB	No Limit	No Limit	N/A

7 total item(s), 1 selected.

Figure 32-4
In Quota Entries, you can review disk usage and impose limits by user.

For each user, Quota Entries displays

- A status indicator (OK for users who are below their warning level and quota limit, Warning for users who are above their warning level, and Above Limit for users who are above their quota limit)
- The user's name and his or her logon name
- The amount of disk space occupied by files that the user owns
- The user's quota limit and warning level
- The percentage of the quota limit currently in use

To change a user's limits, double-click his or her entry. A dialog box appears that offers choices for this user similar to the choices offered on the Quota tab for all new users.

Note By default, the Administrators group has no limit—meaning that while you're logged on as a member of the Administrators group, you might be able to create files that exceed the limits for your own account. Although you can set a warning limit for the Administrators group, you cannot set a quota limit.

Creating a New Quota Entry

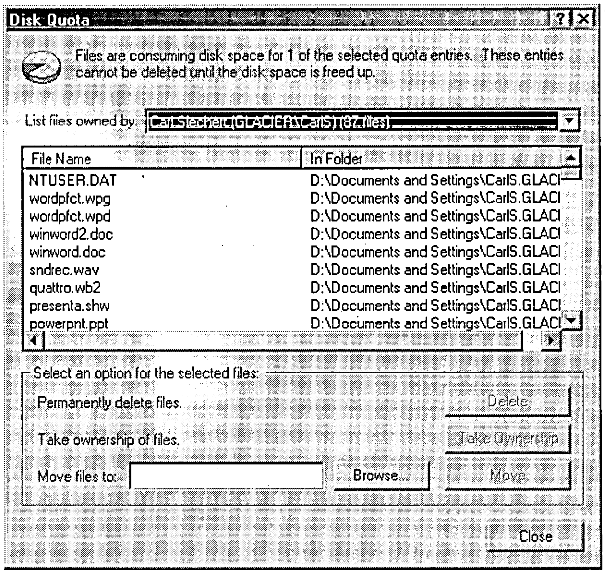
To specify limits for a user who doesn't yet have an entry, open the Quota Entries window and choose Quota | New Quota Entry. Select the local user accounts or domain user accounts to which you'd like to apply limits. After you select one or more user accounts, specify the limits you want to impose in the Add New Quota Entry dialog box that appears.

The sum of the quota limits you set can exceed the size of the volume; Windows makes no attempt to ensure that the space you allow is actually set aside for a particular user.

Deleting a Quota Entry

If a user no longer has files on your NTFS volume, you can delete the user's quota entry by right-clicking it and choosing Delete. Because Windows insists on tracking all files if you enable disk quotas, you can't delete an entry for a user who has files on the disk.

However, the Delete command has another nifty purpose: use it to find out exactly which files belong to a user. (See Figure 32-5.) If you do want to delete the quota entry, you can delete, take ownership of, or move the user's files by selecting the files you want to act on and then clicking the appropriate button. When you've eliminated all the user's files in one way or another, click Close to finish deleting the quota entry for the user.



Files are consuming disk space for 1 of the selected quota entries. These entries cannot be deleted until the disk space is freed up.

List files owned by: Carl Siechert (GLACIER\CarlS) (87 files)

File Name	In Folder
NTUSER.DAT	D:\Documents and Settings\CarlS.GLACI
wordpfct.wpg	D:\Documents and Settings\CarlS.GLACI
wordpfct.wpd	D:\Documents and Settings\CarlS.GLACI
winword2.doc	D:\Documents and Settings\CarlS.GLACI
winword.doc	D:\Documents and Settings\CarlS.GLACI
sndrec.wav	D:\Documents and Settings\CarlS.GLACI
quattro.wb2	D:\Documents and Settings\CarlS.GLACI
presenta.shw	D:\Documents and Settings\CarlS.GLACI
powerpnt.ppt	D:\Documents and Settings\CarlS.GLACI

Select an option for the selected files:

Permanently delete files.

Take ownership of files.

Move files to:

Figure 32-5
Deleting a user's quota entry lets you see exactly which files a user owns.

Chapter 33

Using Encryption

In This Chapter

Installing the High Encryption Pack 555
Encrypting Folders and Files 557
Backing Up Your Certificates 564
Recovering Encrypted Files and Folders 568
Disabling or Reenabling EFS 569

Encryption is the process of encoding sensitive data using a key algorithm. Without the correct key, the data can't be decrypted. Microsoft Windows 2000 uses encryption for several purposes:

- Encrypting files on an NTFS volume. *(See "Encrypting Folders and Files," page 557.)*
- Encrypting data sent between a Web browser and a server using Secure Sockets Layer (SSL). *(See "Managing Security on Your Site," page 472.)*
- Encrypting data sent between computers using a virtual private network (VPN). *(See "Understanding Tunnels and Virtual Private Networks," page 489.)*
- Encrypting or signing e-mail messages. *(See "Signing and Encrypting E-mail Messages," page 595.)*

Installing the High Encryption Pack

Microsoft makes available a Windows 2000 High Encryption Pack, which provides 128-bit encryption for encrypted files on NTFS volumes and for secure network connections, such as those using Internet Protocol security (IPSec).

Note Some online banking services and other secure sites require 128-bit encryption, so you might want to install the High Encryption Pack even if you don't plan to use encrypted files.

The original Windows 2000 Professional CD includes only 56-bit encryption—the maximum allowed for export at the time Windows 2000 was completed. In January 2000—only a few weeks before the retail release of Windows 2000—the United States government issued new export regulations that allow shipping strong encryption products to almost all countries. (*Strong encryption* refers to cryptographic operations that use keys of 128 bits or longer.) Because the Windows 2000 CDs had already been manufactured, Microsoft instead provides the High Encryption Pack as a free add-on product.

The Windows 2000 Professional retail package includes a High Encryption Floppy Disk that you can use to upgrade from 56-bit encryption to 128-bit encryption. If you don't have the floppy disk, you can download the High Encryption Pack from *www.microsoft.com/windows2000/downloads/recommended/encryption.*

Before you seek out the High Encryption Pack, take a moment to determine whether 128-bit encryption is already installed on your computer; you might have it and not realize it. For example, if you installed strong encryption in Windows NT 4 and then upgraded to Windows 2000, your upgraded installation includes 128-bit encryption. To find out whether you have strong encryption installed, do any of the following:

- In Microsoft Internet Explorer, choose Help | About Internet Explorer. The About Internet Explorer dialog box reports a Cipher Strength of either 56-bit (the High Encryption Pack has not been installed) or 128-bit (it has).
- Search for a file named Rsaenh.dll; the file exists in %SystemRoot%\System32 only if the High Encryption Pack has been installed.
- In the Computer Management console, go to System Tools\System Information \Internet Explorer 5\Summary. Cipher Strength appears as an item in the details pane.

You ought to know one more thing before you install the High Encryption Pack: you can't uninstall it. Furthermore, if you install service packs or other upgrades to Windows 2000, those upgrades will include updated versions of the strong encryption files. Unless you format your hard drive and start with a clean installation, you won't ever need to install the High Encryption Pack again.

If you determine that you have only 56-bit encryption, you can install 128-bit encryption simply by running Encpack.exe from the High Encryption Floppy Disk or running the file you download from the Microsoft Web site. The installation is straightforward, requiring only that you click Yes in three successive dialog boxes—the last of which offers to restart your computer.

The installation adds or modifies several .dll files. If you're interested in the complete details, look in %SystemRoot%\System32\Export\Encinst.txt.

If you want to automatically install strong encryption as you install Windows 2000 on other computers, be sure to read the release notes (in a file named Encread.txt), which provide detailed instructions for incorporating encryption into the automated installation methods described in this book. *For more information, see "Automating the Installation Process," page 14.*

Encrypting Folders and Files

The encrypting file system (EFS) allows you to encrypt files on a local NTFS volume so that only you can use them. This offers an additional level of protection beyond that provided by NTFS permissions, which you can use to restrict access to your files by others who log on to your computer. NTFS permissions are vulnerable in a couple of ways. First, all those with administrative privileges can grant themselves (or others) permission to access your files. Worse, anyone who gains physical access to your computer can boot from a floppy disk (or from another operating system, if your computer is set up for dual booting) and use a utility such as NTFSDOS (from *www.sysinternals.com*) to read the files on your hard drive—without having to provide a user name or password. Portable computers, which are more easily stolen, are especially vulnerable to this type of information loss.

Note On most computers, you can use BIOS settings as another protection against this type of loss. Set your BIOS so that a password is required to start the computer or to enter the BIOS setup program, and set the boot options so that the computer can't be booted from a floppy disk. Unfortunately, this type of protection can also be circumvented by a determined snoop. For example, removing the hard drive and installing it in another computer makes its files available to someone with the proper tools.

Securing the Paging File

If you're truly concerned about the possibility of your computer falling into the wrong hands, you should be sure that you don't leave any tracks in the paging file. By default, when you shut down your system, the paging file remains intact. People who have access to your computer could conceivably paw through the unencrypted paging file to find information they shouldn't have.

You can foil such snooping by changing a registry entry. Use a registry editor to navigate to the HKLM\System\CurrentControlSet\Control\Session Manager \Memory Management key and set the value of ClearPageFileAtShutdown to 1. After you do that, Windows fills inactive pages in the paging file with zeros whenever you shut down. Because this could slow down your system, don't make this change unless your security needs demand it.

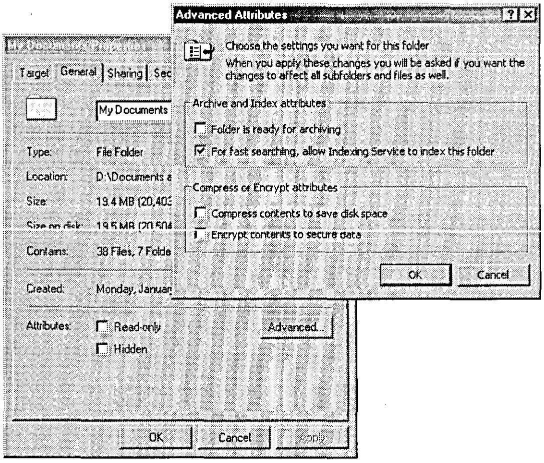
EFS provides a secure way to store your sensitive data. EFS uses your public key to create a randomly generated file encryption key (FEK). Windows transparently encrypts the data using this FEK as data is written to disk. The data can be decrypted only with your certificate and its associated private key, which are available only when you log on with your user name and password. (Designated recovery agents can also decrypt your data. *For details, see "Recovering Encrypted Files and Folders," page 568.*) Other users who attempt to use your encrypted files receive an "access denied" message.

You can encrypt individual files or folders. We recommend that you encrypt folders instead of individual files. That way, not only are the existing files in the folder encrypted, but new files that you create in the folder are also encrypted automatically. This includes temporary files that your applications create in the folder. (For example, Microsoft Word creates a copy of a document when you open it for editing. If the document's folder isn't encrypted, the temporary copy isn't encrypted—giving curious eyes a potential opportunity to view your data.) For this reason, you should consider encrypting your %Temp% and %Tmp% folders, which many applications use to store temporary copies of documents that are open for editing, in addition to the folder where your sensitive documents are stored.

Caution Before you encrypt anything important, you should back up your personal encryption certificate (with its associated private key) and the recovery agent certificate to a floppy disk and store it in a secure location. If you ever lose your original certificate (because of a hard disk failure, for example), you can restore the backup copy and regain access to your files. If you lose all copies of your certificate (and no recovery agent certificates exist), you won't be able to use your encrypted files. No back door exists, nor is there any practical way to hack these files. (If there were, it wouldn't be very good encryption, now would it?) *For details, see "Backing Up Your Certificates," page 564.*

To encrypt a folder:

1. Right-click the folder and choose Properties | General | Advanced.



My Documents

Type: File Folder

Location: D:\Documents a

Size: 19.4 MB (20,40

Size on disk: 19.5 MB (20,504

Contains: 38 Files, 7 Folde

Created: Monday, Januar

Attributes: □ Read-only

□ Hidden

Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

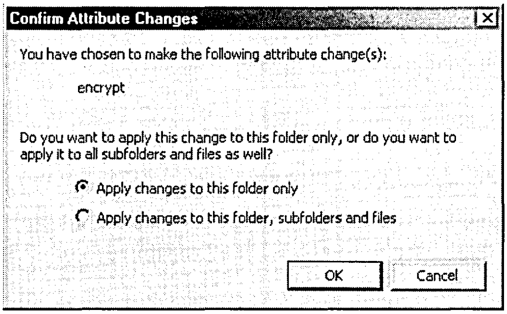
☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes

□ Compress contents to save disk space

□ Encrypt contents to secure data

2. Select Encrypt Contents To Secure Data. (Note that you can't encrypt compressed files. If the files are already compressed, Windows clears the Compressed attribute. Because encryption and compression are mutually exclusive, this section of the dialog box really should contain option buttons rather than check boxes—with the addition of a "Neither" option button.)
3. Click OK two times. Windows then displays a confirmation message.



Confirm Attribute Changes

You have chosen to make the following attribute change(s):

encrypt

Do you want to apply this change to this folder only, or do you want to apply it to all subfolders and files as well?

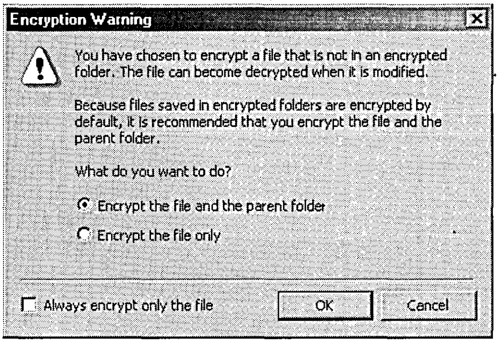
● Apply changes to this folder only

○ Apply changes to this folder, subfolders and files

Note If you select Apply Changes To This Folder Only, Windows doesn't encrypt any of the files currently in the folder. Any new files that you create in the folder, including files that you copy or move to the folder, will be encrypted.

To encrypt a file, follow the same procedure. You'll see a different confirmation message (shown in Figure 33-1) to remind you that the file's folder is not encrypted and to give you an opportunity to encrypt it. You generally don't want to encrypt individual files, because the information you intend to protect can too easily become decrypted without your knowledge. For example, with some applications, when you open a document for editing, the application creates a copy of the original document. When you save the document after editing, the application saves the copy—which is not encrypted—and deletes the original, encrypted document. Static files that you use for reference only—but never for editing—can safely be encrypted without encrypting the parent folder. Even in that situation, however, you'll probably find it simpler to encrypt the whole folder.

Note You can't encrypt any files that have the system attribute. (Not surprisingly, those files are usually system files—and the system might be rendered unusable if some of its essential files were encrypted.)



Encryption Warning

You have chosen to encrypt a file that is not in an encrypted folder. The file can become decrypted when it is modified.

Because files saved in encrypted folders are encrypted by default, it is recommended that you encrypt the file and the parent folder.

What do you want to do?

● Encrypt the file and the parent folder

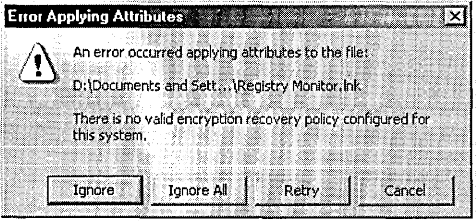
○ Encrypt the file only

□ Always encrypt only the file

Figure 33-1
In this dialog box, Microsoft prods you to encrypt folders rather than individual files.

Troubleshooting

If EFS has been disabled on your computer (because no recovery agent certificates are installed), you'll see a message box like the one shown here when you try to encrypt a file or folder. Although its four buttons might lead you to believe that you have a choice in the matter, you don't. Regardless of which button you click, Windows refuses to encrypt your files—just as if you clicked Cancel.



Error Applying Attributes

An error occurred applying attributes to the file:

D:\Documents and Sett...\Registry Monitor.lnk

There is no valid encryption recovery policy configured for this system.

To solve this problem, you need to create a recovery policy. *For details, see "Enabling EFS," page 570.*

You'll notice no significant difference in working with encrypted folders or files while you're logged on using the same account as when you encrypted them. But encrypted files do act differently in several subtle ways. Table 33-1 describes the important differences.

Table 33-1. Behavior of Encrypted Files

When You Do This	This Happens
Log on using a different account	• If you try to open an encrypted file, you get an "access denied" message. • If you try to decrypt an encrypted file by clearing the encryption attribute, you get an "access denied" message. • If you have Modify or Full Control permission, you can delete or rename an encrypted file.
Copy or move an unencrypted file to an encrypted folder	• The copy in the encrypted folder becomes encrypted.
Copy an encrypted file	• If you copy an encrypted file to an NTFS volume on your computer or another computer running Windows 2000, it remains encrypted. (If EFS is disabled on the target computer, you get a red-herring "access denied" message.) • If you copy to a FAT volume (including floppy disks) or to an NTFS volume on a computer that is running Windows NT, the file becomes decrypted.
Move an encrypted file*	• If you move to another folder on the same volume, the file remains encrypted. • Moving the file to another volume is essentially a "copy and then delete" process; moving your own encrypted files is handled as in copy operations, described above. • If you move someone else's encrypted file to a FAT volume, you get an "access denied" message.
Rename an encrypted file	• The file is renamed and it remains encrypted.
Delete an encrypted file	• If you delete to the Recycle Bin, the restorable file remains encrypted.
Back up an encrypted file using Backup	• You've picked the best way to back up encrypted files or move them between systems! The files in the backup media remain encrypted, whether they're on disk or tape. (Because most removable media can't be formatted as NTFS, an ordinary copy becomes decrypted.)

(continued)

Table 33-1. Behavior of Encrypted Files *(continued)*

When You Do This	This Happens
Use encrypted files on a different computer	• Your personal encryption certificate and its private key must be available on the computer. You can copy the keys manually. *(For details, see "Backing Up Your Certificates," page 564.)* • If you use roaming profiles, your encryption keys are automatically available on all computers you log on to with that user account. *(For more information, see "Using Roaming User Profiles," page 323).*

*Microsoft recommends using cut and paste to move encrypted files instead of using drag and drop. According to the documentation, files moved to an encrypted folder with a drag-and-drop operation are not automatically encrypted. In our own testing, files moved to an encrypted folder were always encrypted—regardless of the method. Whichever method you use, you should confirm that the file remains encrypted by viewing its properties or using Cipher.exe.

Caution Other users with permission to delete a file (that is, users with Modify or Full Control permission) can't use your encrypted files—but they can make them difficult for you to use. Any such user can rename your files, which can make them difficult to find, and also can delete your files. (Even if the user merely deletes them to the Recycle Bin and doesn't remove them altogether, the deleted files are unavailable to you because you don't have access to any other user's Recycle Bin.) Therefore, if you're concerned about protecting your files from other authorized users as well as from a thief who steals your computer, you should modify the NTFS permissions to prevent any type of modification by other users. *For more information, see "Securing Folders and Files," page 543.*

Decrypting Folders and Files

Like the encryption process, decryption is done transparently. That is, you simply work with your encrypted files exactly the same way you work with nonencrypted files. When Windows detects that a file you're accessing is encrypted, it finds your certificate and uses its private key to decrypt the data as it is read from the disk.

To permanently decrypt a folder or file, simply clear the Encrypt Contents To Secure Data check box in the Advanced Attributes dialog box. If you decrypt a folder, Windows asks whether you want to decrypt only the folder or the folder and its contents. If you choose the latter option, Windows prohibits you from decrypting any files for which you don't hold a valid encryption certificate. If you change the attribute for a file that you encrypted, Windows decrypts it without further ado. If you attempt to decrypt a file that someone else encrypted, you get an "access denied" message.

Note Unless you use a command-line utility like Cipher.exe, it's difficult to see at a glance which files are encrypted and which are not. Right-clicking each file and then choosing Properties | General | Advanced (followed by Cancel | Cancel) is a royal pain. Fortunately, there's an easier way. In Windows Explorer, use Details view. Choose View | Choose Columns and then select Attributes. Encrypted files show a letter *E* in the Attributes column.

Using the Cipher Command

If you're a command-line junkie, you'll be pleased to know that a non-GUI alternative to the Advanced Attributes dialog box is available for encrypting and decrypting folders and files. Like the Windows Explorer methods described earlier in this chapter, Cipher.exe lets you encrypt or decrypt folders or individual files. If you specify a folder, you can choose whether to include existing files and subfolders.

Type *cipher* with no parameters to display the encryption state of the current folder and its files.

To encrypt or decrypt a folder or file, include the path and the appropriate switches. Use the /E switch to encrypt the folders or files you specify or the /D switch to decrypt. For example, to encrypt the My Documents folder, including its files and subfolders, type *cipher /e /a /s:"%userprofile%\my documents"* at a command prompt.

In the file specification, you can use wildcards. You can also specify multiple folders and files in a single instance of the command; simply separate each name with a space. Table 33-2 shows the most commonly used switches for Cipher; for a complete list, type *cipher /?* at a command prompt.

Table 33-2. Command-Line Switches for Cipher.exe

Switch	Description
/E	Encrypt the specified folders or files. If the operation includes folders, the folders are marked as encrypted.
/D	Decrypt the specified folders or files. If the operation includes folders, the folders' encryption attribute is cleared.
/S:*folder*	Perform the operation on *folder* and its subfolders (but not files).
/A	Perform the operation on specified files and files in specified folders.
/I	Ignore errors and continue.

Backing Up Your Certificates

When you use encryption for the first time, Windows automatically creates a self-signed certificate for EFS. (*Self-signed* means that it's not granted by a trusted certification authority that can confirm your identity. Such verification is unnecessary for this purpose; it's merely confirming that the certificate was created while your account was logged on.) This certificate becomes your *personal encryption certificate*, and it contains the public/private key pair used for encrypting and decrypting files while you're logged on.

Each user who encrypts files on a system has a personal encryption certificate. In addition, Windows creates a certificate for the designated recovery agent (the Administrator account on a computer running Windows 2000 that is not part of a domain). This certificate, whose purpose is File Recovery, is not the same as that user's personal encryption certificate, whose purpose is shown as Encrypting File System.

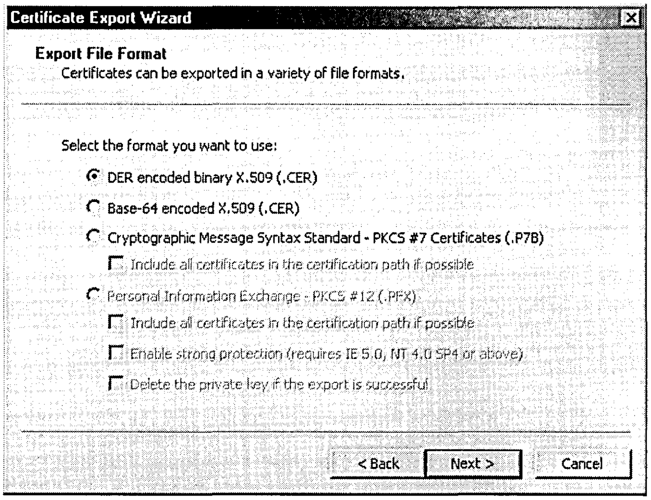
All users should have a backup of their personal encryption certificate. More important, the system administrator should have a backup of the recovery agent certificate. Without one or the other, encrypted files are unusable.

Backing Up the Recovery Agent Certificate

The recovery agent certificate serves two purposes: it provides an administrative alternative for decrypting files if a user's personal encryption certificate is unavailable for any reason, and it enables EFS. In other words, if a computer has no recovery agent certificate installed, no one can encrypt files. Therefore, having a backup of this certificate is essential if you plan to use EFS.

To back up the recovery agent certificate:

1. Log on as a member of the Administrators group.
2. In Local Security Settings (Control Panel | Administrative Tools | Local Security Policy or Start | Run | *secpol.msc*), go to Public Key Policies\Encrypted Data Recovery Agents.
3. Right-click the certificate issued to Administrator for the purpose of File Recovery, choose All Tasks | Export to launch the Certificate Export Wizard, and click Next.
4. Select No, Do Not Export The Private Key and click Next.
5. Select DER Encoded Binary X.509 (.CER) and click Next.



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

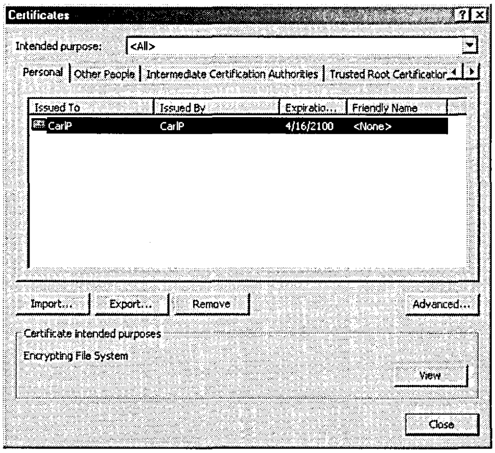
□ Delete the private key if the export is successful

6. Specify the path and file name for the exported file.
7. Click Next and then click Finish.

Exporting a Personal Encryption Certificate

To back up a personal encryption certificate:

1. Log on as the user whose certificate you want to back up.
2. On the Content tab of the Internet Options dialog box (Control Panel | Internet Options), click Certificates to open the Certificates dialog box.



Certificates

Intended purpose: <All>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior

Issued To	Issued By	Expiratio...	Friendly Name
CarlP	CarlP	4/16/2100	<None>

Import...
Export...
Remove
Advanced...

Certificate intended purposes
Encrypting File System

Note If you prefer, you can use the Certificates snap-in for Microsoft Management Console for this procedure. We chose to open the Certificates dialog box via Internet Options because this route is available and easily understandable for all users; no special privileges are required. *For more information, see "Using the Certificates Snap-In," page 592.*

3. On the Personal tab, select the certificate that shows Encrypting File System in the Certificate Intended Purposes box at the bottom of the dialog box.

Note Windows creates this certificate the first time you encrypt a folder or file. Unless you have encrypted something—or you created an encryption certificate in some other way—the certificate won't exist.

4. Click Export to launch the Certificate Export Wizard and then click Next.
5. Select Yes, Export The Private Key and click Next two times.
6. Specify a password for the .pfx file. It doesn't need to be the same as your logon password. Click Next.
7. Specify the path and file name for the exported file.
8. Click Next and then click Finish.

As you'll see in the next section, the import process makes it very easy to install your certificate on another computer—and thereby provide access to your encrypted files. For that reason, be careful to observe these guidelines:

- When you export your certificate, be sure to protect it with a password that can't be guessed easily. Unlike the case of logon attempts, no policies exist to prevent further attempts after a certain number of incorrect guesses. (On the other hand, be sure to use a password that *you* can remember when the need arises!)
- Be sure to keep your certificate files—whether they're on a floppy disk, a hard disk, or some other medium—in a secure place.

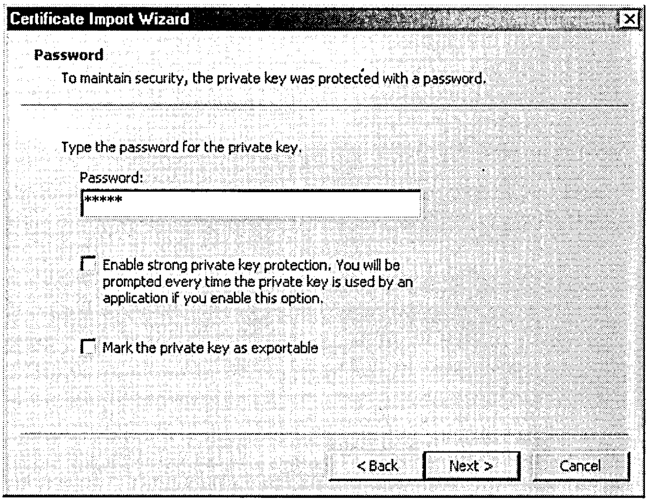
Importing a Personal Encryption Certificate

You need to import your personal certificate—one that you exported to disk using the procedure in the preceding section—in either of the following situations:

- You want to use your encrypted files on a different computer.
- Your original personal certificate is accidentally lost or becomes corrupt.

To import a personal encryption certificate:

1. On the Content tab of the Internet Options dialog box (Control Panel | Internet Options), click Certificates to open the Certificates dialog box.
2. Click Import to launch the Certificate Import Wizard and then click Next.
3. Enter the path and file name of the encryption certificate (a .pfx file) you exported and click Next.
4. Enter the password, select other options if you want, and click Next.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

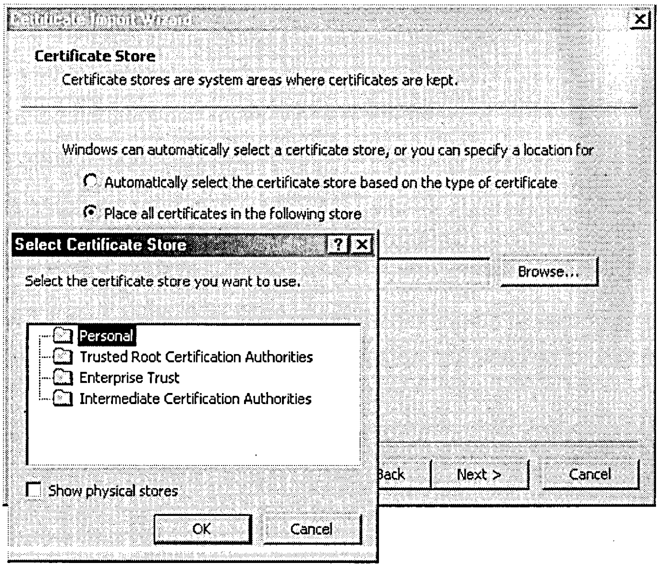
Type the password for the private key.

Password: *****

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark the private key as exportable

5. Select Place All Certificates In The Following Store, click Browse, and select Personal. Click OK and then click Next.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities

□ Show physical stores

6. Click Finish.

Creating a New Personal Encryption Certificate

If you lose your personal encryption certificate, you can create a new one using Cipher.exe, the command-line encryption utility. At a command prompt, simply type *cipher /k,* and it creates a new personal encryption certificate for the user running Cipher. (By using the RunAs command to launch Cipher, you can create certificates for other users.) Of course, you can't use the new certificate to decrypt files that were encrypted using the public key from your old certificate.

Recovering Encrypted Files and Folders

The security policy for a computer or a domain includes a data recovery policy. This policy designates one or more users as data recovery agents; these users can decrypt encrypted files even if the personal encryption certificate that was used to encrypt the file is no longer available. This makes it possible to recover encrypted files after an employee leaves a company, for example.

If your computer is running Windows 2000 and is not part of a Microsoft Windows 2000 Server–based domain, the local Administrator account is the default recovery agent. In a domain environment, the default recovery agent is the Administrator account for the domain.

If your computer is a member of a Windows 2000 domain, the domain administrator can designate additional users as recovery agents. Using the domain's Enterprise Certificate Authority, the domain administrator creates recovery agent certificates for these users and adds them to Public Key Policies\Encrypted Data Recovery Agents in Local Security Settings or, more likely, in the domain security policy.

The recovery agent has a special certificate and an associated private key that allow data recovery. When this user logs on, he or she can work with encrypted files just as the users who encrypted them can. To prevent misuse of this capability—including inadvertent use—you should back up and then remove the recovery agent's file recovery certificate from the personal store (not from the security policy, which would disable EFS). Store the backup on a floppy disk in a secure place and then restore it only when needed.

To back up and remove the recovery agent's file recovery certificate:

1. Log on as the recovery agent. On a system running Windows 2000 Professional that is not part of a Windows 2000 domain, this is the Administrator account. (Logging on as a member of the Administrators group won't work.)
2. Use the Certificates dialog box to export the file recovery certificate and its associated private key. Use the same procedure as for exporting a personal encryption certificate, except that you must select the certificate whose intended purpose is File Recovery (step 3). *For details of this procedure, see "Exporting a Personal Encryption Certificate," page 565.*

3. While the Certificates dialog box is still open, select the certificate you just exported and click Remove.

To restore this certificate when it's needed:

1. Log on as Administrator.
2. Use the Certificates dialog box to import the file recovery certificate. Use the same procedure as for importing a personal encryption certificate. *For details, see "Importing a Personal Encryption Certificate," page 566.*

Note If you don't have a domain with an Enterprise Certificate Authority and you want to use an account other than Administrator as the recovery agent, log on as that user and then restore Administrator's file recovery certificate to the personal store. Thereafter, any time you log on with that user account, you can work with any encrypted files on the system.

If you're in a situation where you need to recover encrypted files, it might be useful to know who encrypted the files in the first place. With Windows 2000 alone, you have no easy way to find out. However, *Microsoft Windows 2000 Professional Resource Kit* (Microsoft Press, 2000) contains a tool named Efsinfo.exe that shows who encrypted each file and who has permission to decrypt it, including any recovery agents. Microsoft Knowledge Base article Q243026 (on the companion CD) has more information about Efsinfo.

Disabling or Reenabling EFS

If you want to prevent users from encrypting files on a particular machine, you can disable the encrypting file system. You do that by deleting all recovery agent certificates on the computer. Doing so doesn't prevent users from decrypting and using files that are already encrypted, but it doesn't allow them to encrypt any additional files or folders.

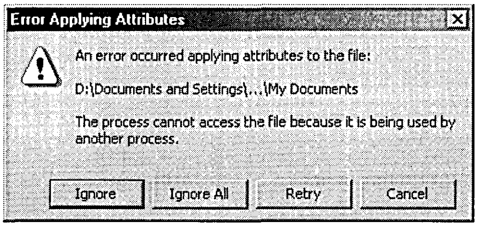
Disabling EFS

To disable EFS on a computer that is not part of a domain:

1. Log on as a member of the Administrators group.
2. In Local Security Settings (Secpol.msc), go to Public Key Policies\Encrypted Data Recovery Agents.
3. Right-click the Administrator certificate and choose Delete.
4. In response to the confirmation dialog box, click Yes.

Caution Before you delete a certificate, be *sure* you have exported the recovery agent certificate so that its key is available for data recovery. *For details, see "Backing Up the Recovery Agent Certificate," page 564.* Without it (or another valid recovery agent certificate, such as one from a domain controller), you won't be able to reenable EFS unless you reinstall Windows 2000.

This procedure creates an *empty recovery policy.* When the policy is empty—that is, all the recovery agent certificates have been deleted—users who attempt to encrypt files will see an error message, as shown in Figure 33-2.


Error Applying Attributes

An error occurred applying attributes to the file:

D:\Documents and Settings\...\My Documents

The process cannot access the file because it is being used by another process.

Figure 33-2
If no data recovery agents are available, Windows won't let you encrypt any more files.

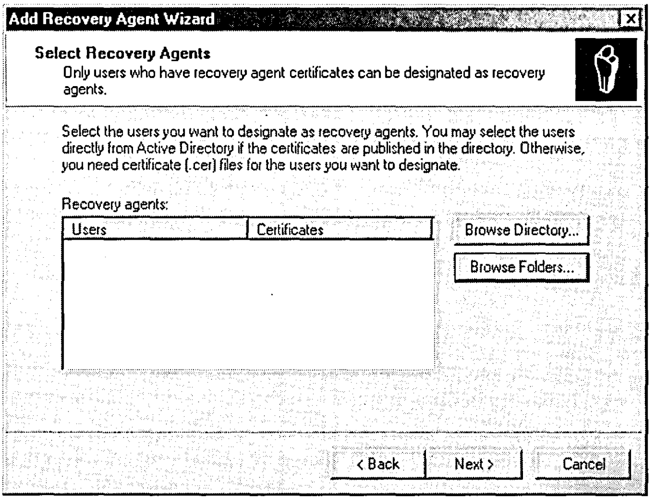
If the computer is part of a domain, higher-level policies supersede your settings in Local Security Settings, which controls only the local Group Policy object. If the default domain policy includes recovery agent certificates, EFS continues to be available. Of course, by applying the changes to a domain-based policy instead of the local policy, you can disable EFS on all computers to which the policy is applied. *Microsoft Windows 2000 Server Resource Kit* (Microsoft Press, 2000) provides information about EFS in a domain environment.

Enabling EFS

If you have disabled EFS by setting no recovery policy or by setting an empty policy, you can reenable it. To enable EFS:

1. Log on as a member of the Administrators group.
2. In Local Security Settings (Secpol.msc), go to Public Key Policies\Encrypted Data Recovery Agents.
3. Right-click Encrypted Data Recovery Agents and choose Initialize Empty Policy. (If the command is not on the shortcut menu, you already have an empty policy; skip this step.)
4. Right-click Encrypted Data Recovery Agents and choose Add to launch the Add Recovery Agent Wizard. Click Next.
5. On the Select Recovery Agents page, click Browse Folders and then navigate to the folder that contains the .cer file for the recovery agent certificate you want

to add. (The Browse Directory button searches Active Directory, a feature of Windows 2000 Server–based domains.)



Add Recovery Agent Wizard

Select Recovery Agents

Only users who have recovery agent certificates can be designated as recovery agents.

Select the users you want to designate as recovery agents. You may select the users directly from Active Directory if the certificates are published in the directory. Otherwise, you need certificate (.cer) files for the users you want to designate.

Recovery agents:

Users	Certificates

6. Here's where the wizard becomes confusing. The Select Recovery Agents page now shows the new agent as USER_UNKNOWN. This is normal. Simply click Next and then click Finish.
7. A message appears: "The certificate cannot be validated." Again, this is normal. Click OK.

The Administrator certificate now appears in the details pane—and you can begin encrypting files again.

Chapter 34

Auditing Security

In This Chapter

About Auditing 573

Viewing Audit Events 575

Enabling Auditing 576

Auditing File and Folder Access 578

Auditing Access to Printers 580

Monitoring, or *auditing*, system usage is often a helpful tool in the administration of system security. For example, repeated attempts to log on with an improper password might be an indication that unauthorized users are trying to gain access to the system. Repeated failure to access a folder might indicate that software has been incorrectly installed or that security for the folder is set up improperly.

Microsoft Windows 2000 provides the ability to audit security events by recording attempts to access system resources. In this chapter, we describe the various auditing tools at the disposal of a system administrator or resource owner. We examine their purpose and use and explain what information they supply when they are used properly.

About Auditing

When a user attempts to access a system resource, Windows checks the resource's access control list to determine whether the user should be allowed access. This is the essence of Windows 2000 security.

If auditing is enabled, you can also request that Windows audit access to a given resource. *(See "Enabling Auditing," page 576.)* Windows will then record in a log file any attempts to access that resource. You might direct Windows to record all failed print jobs on a given printer, for example, or to record all failed file-read requests for a certain folder.

Windows records this information in the Security log (SecEvent.evt), one of the three system-wide logs that Windows manages. The other two are the System log (SysEvent.evt), which records events generated by components of the operating system—such as display or network drivers—and the Application log (AppEvent.evt), which records events generated by applications. For example, Microsoft Windows Backup generates events when you erase a tape, restore files, and so on and records them in the Application log. *(For information about the System and Application logs, see Chapter 5, "Monitoring System and Application Activities with Event Viewer.")*

Avoid auditing if you don't need it. Like IRS audits, security audits can be time-consuming. (OK, security audits aren't *that* bad.) When you enable auditing, the system must write an event record to the Security log for each audit check the system performs. Because this can severely degrade system performance, you should audit only the events that are important to you.

Ensuring That You Don't Miss Any Security Events

By default, when the Security log fills up, Windows erases the oldest entries when it needs to make a new entry—just as it does with the System log and the Application log. But if security is critical to your operation, you can make a registry setting that ensures that events can be deleted only by a member of the Administrators group. (Even without this registry setting, only administrators—and others with the Manage Auditing And Security Log right—can view the Security log or clear its contents. To prevent someone from covering their tracks, no one can delete individual entries; authorized individuals must delete all or none.)

This solution is rather drastic and should therefore be used only when it's essential that every security event be preserved. With this registry entry, the system halts when the Security log becomes full, preventing all further use—and possibly losing data if document files happen to be open when this occurs. If you want to enable this level of security, here's how it's done:

1. In Event Viewer, right-click Security Log and choose Properties.
2. On the General tab, select either Overwrite Events Older Than or, for maximum security, Do Not Overwrite Events (Clear Log Manually).
3. Use a registry editor to create a DWORD value named CrashOnAuditFail in HKLM\System\CurrentControlSet\Lsa. Set its value to 1.
4. Restart the computer.

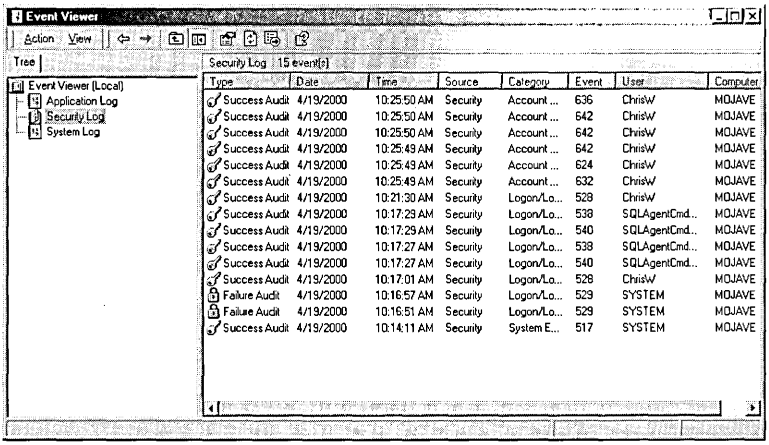
(continued)

Ensuring That You Don't Miss Any Security Events *(continued)*

After you've followed these steps, the computer will halt when the Security log becomes full. At that point, you need to restart the computer and log on as a member of the Administrators group; no other accounts are allowed to log on. Your first action after logging on should be to review, export if desired, and clear the Security log. You then need to reset the value of the registry entry to 1. (The operating system automatically sets it to 2, which is the mechanism that prevents others from logging on.)

Viewing Audit Events

Before we examine how to audit events, let's first take a look at Event Viewer—the Microsoft Management Console snap-in that allows you to examine the events that have been recorded. Event Viewer is in Computer Management, under System Tools. Or, for the uncluttered view, go to Start | Settings | Control Panel | Administrative Tools | Event Viewer or simply type *eventvwr.msc* at a command prompt. *(For additional information, see Chapter 5, "Monitoring System and Application Activities with Event Viewer.")* You can use Event Viewer to examine any of the three logs: System, Security, or Application. If you select the Security log, you'll see a window similar to the one shown in Figure 34-1.



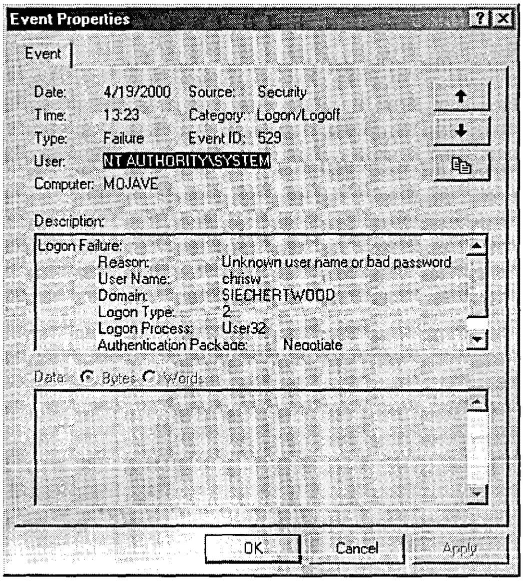
Security Log 15 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Success Audit	4/19/2000	10:25:50 AM	Security	Account ...	636	ChrisW	MOJAVE
Success Audit	4/19/2000	10:25:50 AM	Security	Account ...	642	ChrisW	MOJAVE
Success Audit	4/19/2000	10:25:50 AM	Security	Account ...	642	ChrisW	MOJAVE
Success Audit	4/19/2000	10:25:49 AM	Security	Account ...	642	ChrisW	MOJAVE
Success Audit	4/19/2000	10:25:49 AM	Security	Account ...	624	ChrisW	MOJAVE
Success Audit	4/19/2000	10:25:49 AM	Security	Account ...	632	ChrisW	MOJAVE
Success Audit	4/19/2000	10:21:30 AM	Security	Logon/Lo...	528	ChrisW	MOJAVE
Success Audit	4/19/2000	10:17:29 AM	Security	Logon/Lo...	538	SQLAgentCmd...	MOJAVE
Success Audit	4/19/2000	10:17:29 AM	Security	Logon/Lo...	540	SQLAgentCmd...	MOJAVE
Success Audit	4/19/2000	10:17:27 AM	Security	Logon/Lo...	538	SQLAgentCmd...	MOJAVE
Success Audit	4/19/2000	10:17:27 AM	Security	Logon/Lo...	540	SQLAgentCmd...	MOJAVE
Success Audit	4/19/2000	10:17:01 AM	Security	Logon/Lo...	528	ChrisW	MOJAVE
Failure Audit	4/19/2000	10:16:57 AM	Security	Logon/Lo...	529	SYSTEM	MOJAVE
Failure Audit	4/19/2000	10:16:51 AM	Security	Logon/Lo...	529	SYSTEM	MOJAVE
Success Audit	4/19/2000	10:14:11 AM	Security	System E...	517	SYSTEM	MOJAVE

Figure 34-1
The Security log shown here indicates that an unauthorized user has apparently been attempting to gain access to the system. These unsuccessful logon events, identified with a lock icon, happened within a few seconds of each other.

Note You must be logged on as a member of the Administrators group to view the Security log. (A system administrator can grant Security log access to other groups and user accounts by assigning the Manage Auditing And Security Log right. *For details, see "Setting User Rights," page 296.*)

If you want more information about an event in the Security log, double-click the event, or select it and choose Action | Properties. The Event Properties dialog box appears, similar to the one shown in Figure 34-2.



Date: 4/19/2000 Source: Security
Time: 13:23 Category: Logon/Logoff
Type: Failure Event ID: 529
User: NT AUTHORITY\SYSTEM
Computer: MOJAVE

Description:

```
Logon Failure:
        Reason:                  Unknown user name or bad password
        User Name:               chrisw
        Domain:                  SIECHERTWOOD
        Logon Type:              2
        Logon Process:           User32
        Authentication Package:      Negotiate
```

Data: ● Bytes ○ Words

Figure 34-2
This properties dialog box indicates that someone has tried to log on to ChrisW's account without the proper password.

By carefully examining all unsuccessful logon events, you might be able to find a pattern in attempts to gain access to the system. You can then take measures to tighten security, such as warning users to change their passwords and monitoring the Security log more closely.

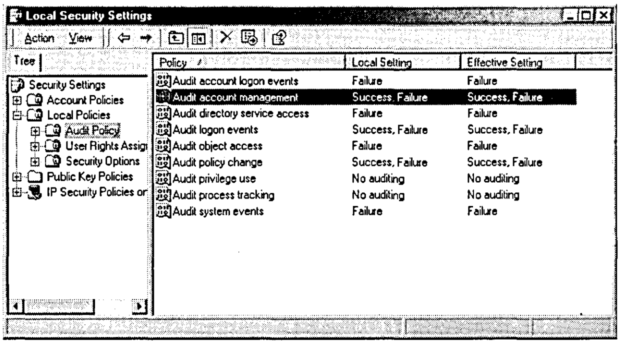
Enabling Auditing

No events are written to the Security log until you enable auditing, which you do via Local Security Settings. Even if you set up auditing for files, folders, or printers, as explained later in this chapter, those events aren't recorded unless you also enable auditing in Local Security Settings. You must be logged on as a member of the Administrators group to enable auditing. (And unlike most rights, the right to enable auditing can't be given to other users or groups.)

Note Like most other settings in Local Security Settings, the audit policy settings can be overridden by domain-level policy settings. If your computer is part of a Microsoft Windows 2000 Server–based domain, you should use domain-level Group Policy to make audit policy settings instead of using Local Security Settings.

To enable auditing, follow these steps:

1. Click Start | Settings | Control Panel | Administrative Tools | Local Security Policy. (Alternatively, you can type *secpol.msc* at a command prompt.)
2. Expand Local Policies and then click Audit Policy to display the list shown in Figure 34-3.
3. Double-click each policy for which you want to enable auditing, and then select Success, Failure, or both.



Policy	Local Setting	Effective Setting
Audit account logon events	Failure	Failure
Audit account management	Success, Failure	Success, Failure
Audit directory service access	Failure	Failure
Audit logon events	Success, Failure	Success, Failure
Audit object access	Failure	Failure
Audit policy change	Success, Failure	Success, Failure
Audit privilege use	No auditing	No auditing
Audit process tracking	No auditing	No auditing
Audit system events	Failure	Failure

Figure 34-3
You enable auditing using the Local Security Settings console.

Figure 34-3 shows the types of activities you can audit. Some, such as account management and policy change, can provide an audit trail for administrative changes. Others, such as logon events and object access, can help you better secure your system. Still others, including system events and process tracking, can assist you in locating problems with your system. Table 34-1 provides more details.

Table 34-1. Audit Events

Audit Policy	Description
Audit account logon events	Account logon events occur when a user logs on or logs off another computer that uses this computer to validate the account (which happens only on a computer running Windows 2000 Server).
Audit account management	Account management events occur when a user account or group is created, changed, or deleted; when a user account is renamed, enabled, or disabled; or when a password is set or changed.
Audit directory service access	Directory service access events occur when a user accesses an Active Directory object that has its own system access control list. (This is the same as object access except that it applies only to Active Directory objects.)

(continued)

Table 34-1. Audit Events *(continued)*

Audit Policy	Description
Audit logon events	Logon events occur when a user logs on or logs off a workstation or connects via a network.
Audit object access	Object access events occur when a user accesses a file, folder, printer, registry key, or other object that is set for auditing, as described in this chapter.
Audit policy change	Policy change events occur when a change is made to user rights assignment policies, audit policies, or trust policies.
Audit privilege use	Privilege use events occur when a user exercises a user right (other than logon, logoff, and network access rights, which trigger other types of events).
Audit process tracking	Process tracking includes arcane events such as program activation, handle duplication, indirect object access, and process exit. This policy is generally not useful for everyday security concerns.
Audit system events	System events occur when a user restarts or shuts down the computer or when an event occurs that affects the system security or the Security log.

Auditing File and Folder Access

If you have the proper permissions, you can set up auditing of certain files or folders on your system. Windows 2000 can audit a variety of events and can audit different events for different users.

Note You must be logged on as a member of the Administrators group (or your logon account must have the Manage Auditing And Security Log right) to set up auditing of files and folders.

Avoid auditing too many successful events. Although auditing is a useful technique for monitoring access to your system, you should be careful when auditing busy folders or files—and be particularly careful about auditing successful accesses. Each time a user successfully completes an operation on the file or folder, Windows 2000 writes one or more records to the Security log to reflect the access. This slows down your system and adds many events of little value to the log, thereby making it more difficult to find real security breaches. On the other hand, selectively auditing successful file access can be beneficial in some situations. For example, you might want to log all access to a payroll database file, which would allow you to track down who did what (and when) as well as find out if someone without the proper authority accessed the file.

Use the Security tab in the properties dialog box for a file or folder to display its audit settings. You can specify the users and groups whose access to the selected file or folder you want to audit. For each user and group, you can specify which types of access should generate entries in the Security log. You can specify different auditing events for each user and group.

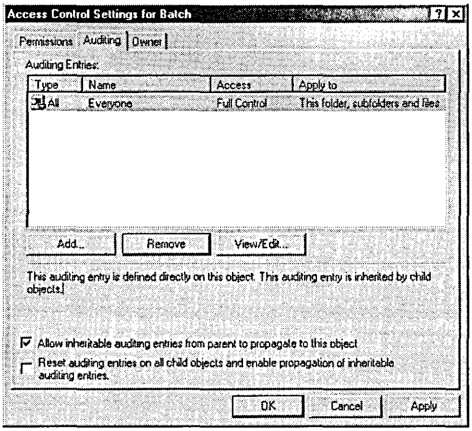
Note The settings you make on the Auditing tab of the Access Control Settings dialog box (as described in the following procedure) are effective only if you also enable auditing. If you haven't done so already, visit Local Security Settings to enable auditing. Be sure to set Audit Object Access events to audit success and failure. *(For details, see the preceding section.)*

To set up auditing for files and folders, follow these steps:

1. Right-click a file or folder in Windows Explorer and choose Properties.
2. Click the Security tab.

Note If the selected file or folder is not stored on an NTFS volume, the Security tab doesn't appear, because auditing and other security features are implemented only for NTFS volumes.

3. Click the Advanced button. The Access Control Settings dialog box appears.
4. Click the Auditing tab.



Access Control Settings for Batch

Auditing Entries:

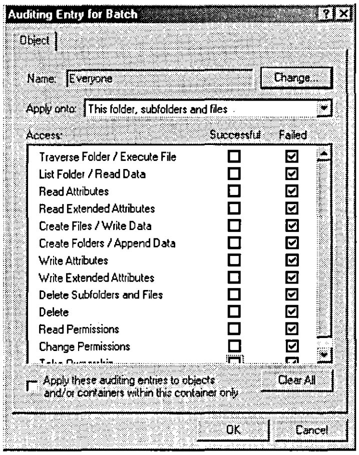
Type	Name	Access	Apply to
All	Everyone	Full Control	This folder, subfolders and files

This auditing entry is defined directly on this object. This auditing entry is inherited by child objects.

☑ Allow inheritable auditing entries from parent to propagate to this object

□ Reset auditing entries on all child objects and enable propagation of inheritable auditing entries.

5. Click Add to add a new user or group, or click View/Edit to change audit settings for an existing user or group.
6. In the Auditing Entry dialog box (similar to the one shown here), select the types of access you want to audit.



Auditing Entry for Batch

Name: Everyone

Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Traverse Folder / Execute File	□	☑
List Folder / Read Data	□	☑
Read Attributes	□	☑
Read Extended Attributes	□	☑
Create Files / Write Data	□	☑
Create Folders / Append Data	□	☑
Write Attributes	□	☑
Write Extended Attributes	□	☑
Delete Subfolders and Files	□	☑
Delete	□	☑
Read Permissions	□	☑
Change Permissions	□	☑

□ Apply these auditing entries to objects and/or containers within this container only

7. If you're making audit settings for a folder, select the scope of objects you want audited from the Apply Onto list.

If you select an event's Successful check box, Windows generates a Security log record containing (among other information) the time and date of each successful attempt at the event by the specified user or group for the specified file or folder. Similarly, if you select an event's Failed check box, Windows generates a Security log record each time the specified user or group unsuccessfully attempts the event for the specified file or folder.

Note You can change audit settings for multiple files or folders simultaneously. If you select more than one file or folder in Windows Explorer before you click the Security tab in the properties dialog box, the changes you make affect all the selected files or folders. If the existing security settings are not the same for all the items in your selection, a message appears, asking whether you want the same audit settings for the entire selection.

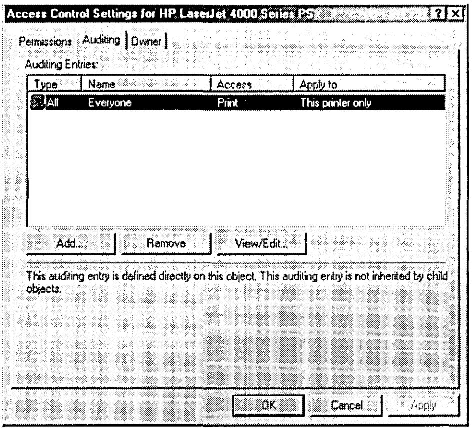
Auditing Access to Printers

Windows 2000 can audit several printer events as well as auditing different events for different users. You can manage all the printer security features through the Printers folder.

Note You must be logged on as a member of the Administrators group (or your logon account must have the Manage Auditing And Security Log right) to set up auditing of printers.

To set up printer security auditing, follow these steps:

1. Use Local Security Settings to enable auditing. Be sure to set Audit Object Access events to audit success and failure. *(For details, see "Enabling Auditing," page 576.)*
2. Open the Printers folder by clicking Start | Settings | Printers.
3. Right-click the icon for the printer you want to audit and choose Properties.
4. Click the Security tab.
5. Click the Advanced button. The Access Control Settings dialog box appears.
6. Click the Auditing tab.

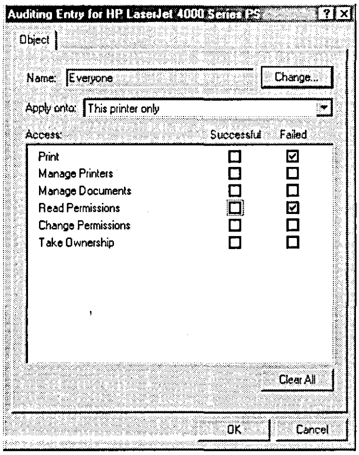


Auditing Entries:

Type	Name	Access	Apply to
All	Everyone	Print	This printer only

This auditing entry is defined directly on this object. This auditing entry is not inherited by child objects.

7. Click Add to add a new user or group, or click View/Edit to change audit settings for an existing user or group.
8. In the Auditing Entry dialog box (similar to the one shown here), select the types of access you want to audit.



Name: Everyone

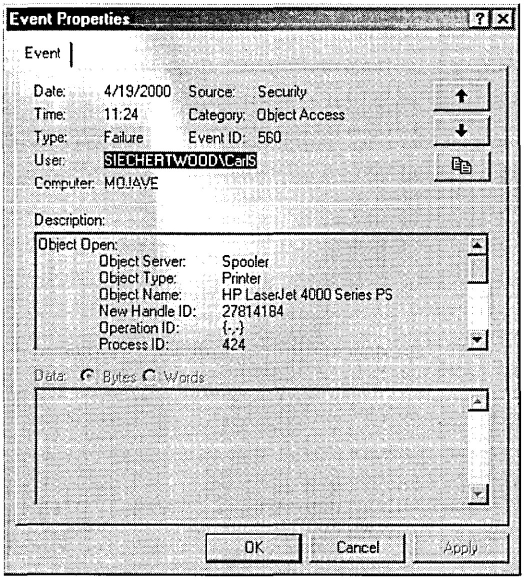
Apply onto: This printer only

Access:	Successful	Failed
Print	□	☑
Manage Printers	□	□
Manage Documents	□	□
Read Permissions	□	☑
Change Permissions	□	□
Take Ownership	□	□

Logging printer successes generates a large number of relatively useless log entries. You might want to do this for only a short time to identify users who should not have access to a printer. Printer failures, on the other hand, create few entries and can be used to quickly identify people who attempt to access a printer for which they do not have permission.

When Windows logs a printer event, such as successful printing or a deletion from the print queue, the event record is written to the System log. In contrast, security events, such as attempts to access a printer for which an account does not have permission, result in an event record being written to the Security log. Figure 34-4 shows the Event Properties dialog box for a record in the Security log that was generated by an attempt to access a printer using an account that lacks permission to use the printer.

Note It is often useful to monitor unsuccessful print jobs and deletions from the print queue, because these events might indicate a problem with the printer or difficulty using the printer. These are printer operation events, however, not security events. On the Advanced tab of the Print Server Properties dialog box, select Log Spooler Information Events. *For more information, see "Setting Server Properties," page 232.*



Date: 4/19/2000 Source: Security
Time: 11:24 Category: Object Access
Type: Failure Event ID: 560
User: SIECHERTWOOD\CarlS
Computer: MOJAVE

Description:

```
Object Open:
        Object Server:      Spooler
        Object Type:        Printer
        Object Name:        HP LaserJet 4000 Series PS
        New Handle ID:      27814184
        Operation ID:       {-,-}
        Process ID:         424
```

Data: ● Bytes ○ Words

Figure 34-4
The user logged on as CarlS from the SIECHERTWOOD domain has been caught trying to use a printer without permission.

Chapter 35

Managing Security Certificates

In This Chapter

Understanding Digital Certificates 584
Using the Certificates Dialog Box 591
Using the Certificates Snap-In 592
Signing and Encrypting E-mail Messages 595

As security becomes an increasingly important component of everyday computer use, certificates are emerging as a tool that more and more computer users need to understand and manage. You can use certificates for everything from signing e-mail messages and authenticating downloaded programs to encrypting files and creating secure communication links.

You need to manage a number of components when you start using certificates, and keeping track of everything can be difficult. You might have personal certificates with private and public keys, client certificates, and—if you run any server—server certificates. This is just for your own computer. You might also have public certificates for people who send you encrypted e-mail and for companies from whom you download software. If that's not enough, you have certificates from trusted third parties who authenticate your certificates and the certificates of those you do business with. Microsoft Windows 2000 gives you two interfaces with which to manage all your certificate components: the Certificates dialog box and a Certificates snap-in for Microsoft Management Console (MMC).

Both interfaces allow you to perform essentially the same tasks. The Certificates dialog box is less complicated and easier to use. The Certificates snap-in has a few more options. We suggest you try the Certificates dialog box first. If you can't accomplish your goal with that, try the MMC snap-in. We discuss both in this chapter.

Understanding Digital Certificates

Before we explain how to manage certificates, you should understand what certificates are and how they work. The use of digital certificates is the basis of two important Internet security features: signing and encrypting. Signing authenticates the identity of individuals and organizations on the Internet. If you receive a digitally signed e-mail message or download a digitally signed program, the signature assures you that the claimed identity of the sender or the originating organization is genuine.

Encryption hides information from people who are not authorized to see it. Encryption uses keys to translate data from its base format to another, unintelligible format. That's the encryption part. The only way the data becomes intelligible again is to translate it back—and of course it takes a key to translate the data back to its base format. That's the decryption part. The most efficient and longest-used encryption methods, called *symmetric encryption,* use the same key for both encrypting and decrypting (that is, the same key at both ends of the process).

Another method of encryption, called *asymmetric encryption,* uses different keys to encrypt and decrypt data. The asymmetric encryption method commonly used on the Internet today is called Public Key Infrastructure (PKI). PKI uses a private key, known only to a single entity, and a public key, available to anyone who needs it. Data encrypted with a public key can be decrypted only with its corresponding private key. For example, say that Ahmad wants to send a private message to Irving. If Ahmad uses Irving's public key to encrypt the message, only Irving can decrypt it, because he is the only one with the corresponding private key.

It turns out that public and private keys can be used for more than just encryption. They can be used to create a whole network of security and authentication (hence the word *Infrastructure* in Public Key Infrastructure) that can be tracked back to a trusted source. In the preceding example, how did Ahmad get Irving's public key? Irving sent it to him, of course. But then, how did Ahmad know the key was really from Irving and not from someone pretending to be Irving? The message Irving sent was signed with the private key of a third party trusted by both Ahmad and Irving that verified Irving's identity. Because the trusted third party is the only one who could sign a message with its own private key, Ahmad was assured that the message from Irving with his public key actually came from Irving.

The messages going back and forth identifying sources and passing around public keys are certificates. Certificates are an integral part of PKI. Certificates contain several pieces of information, including the sender's identification and public key and the signature of a trusted third party. The trusted third party, a certification authority (CA), is another integral part of PKI.

A CA assigns certificates to individuals and organizations. Before granting a certificate, the CA is responsible for verifying the identity of the person or organization who is applying for the certificate. After the requester's identity is verified, the CA assigns the requester both a public key and a private key and then supplies a digital certificate signed with the CA's private key. The validity of the certificate, then, is only as good as the credibility and level of trust maintained by the CA.

Note Microsoft maintains a Web page that discusses certification authorities at *www.microsoft.com/windows/oe/certpage.htm.*

Why Do You Want One?

After having marveled at the technical acumen of those who developed certificates and PKI, you might pause to wonder why you would ever want a certificate or even what you would do with one if you had it. One way to answer that question is to point out that you already have lots of them. Microsoft Internet Explorer comes with a whole passel of certificates, mostly for trusted certification authorities. Internet Explorer uses these certificates when you begin to download a program that has been digitally signed. *(For information about certificates and downloading software, see "Understanding Digital Certificates," page 440.)* So, whenever you download a signed program, you're using certificates, whether you know it or not. Also, when you connect to a secure Web site (the lock icon appears on the Internet Explorer status bar), you're using a certificate to create the encrypted link.

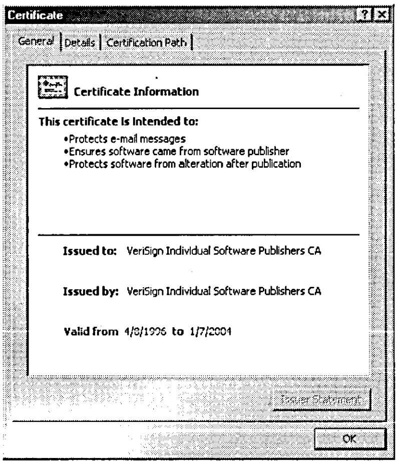
For several good reasons, however, you might want to go a little further and begin to actively use certificates, or at least maintain a little more control over their use on your computer. For example, only a few people today digitally sign their e-mail messages, but the trend is increasing. If you have reason to be cautious about who reads your e-mail, you will want to acquire public keys from your clandestine recipients. Or, if you want to receive secure e-mail from someone, you need to understand how to give the sender your public key. If you publish software on the Internet, you also need to deal with certificates.

Caring for Your Certificates

For the most part, you can leave your certificates alone. Internet Explorer and Windows 2000 automatically take care of business and bother you only when necessary. However, if you need to do anything other than the most basic security tasks, you must know how to work with your certificates. You shouldn't be surprised that Windows offers more than one way to manage certificates. In fact, Windows 2000 gives you two distinct interfaces for certificate management. We'll talk about how you perform each of the following tasks using each interface later in this chapter:

- **Request.** When you want a new certificate, you must request it from a CA. If the Certificate Services service is running on a server on your network, you can request a certificate from that service. Otherwise, you must make your request to an external CA.

- **View.** You might want to view the contents of a certificate to note its expiration date, purpose, or certifying authority. When you open a certificate, you see a Certificate dialog box like the one shown in Figure 35-1. The Details tab displays a list of all the parameters in a certificate and their values. The Certification Path tab shows the chain of authentication back to a root certification authority.



Certificate Information

This certificate is intended to:

- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: VeriSign Individual Software Publishers CA

Issued by: VeriSign Individual Software Publishers CA

Valid from 4/8/1996 **to** 1/7/2004

Figure 35-1
You can view the data held in any certificate.

- **Import/Export.** Certificates are moved in and out of the certificate storage by importing and exporting. When you receive a new certificate, you import it into the store. If you have a personal certificate you want to use on more than one computer, you export it to a file, copy the file to another computer, and then import the certificate on the second computer.
- **Renew.** When certificates expire, they can be renewed. You can renew a certificate with its existing keys or have a new set generated.

Kinds of Certificates

Certificates have specified purposes. The allowed purposes are listed within the certificate, and the certificate can be used only for its specified purposes. A certificate can have more than one purpose. On the General tab of the Certificate dialog box is the statement "This certificate is intended to:" followed by a list of the certificate's purposes. (Refer to Figure 35-1.) Table 35-1 describes the most common certificate purposes.

Table 35-1. Common Certificate Purposes

Purpose	Description
Client Authentication	Used by clients to authenticate themselves to servers
Server Authentication	Used by servers to authenticate themselves to clients
Code Signing	Used by software producers to authenticate software to users
Secure Email	Used to sign e-mail messages
Trust List Signing	Used to create Certificate Trust Lists
Encrypting File System	Used with the symmetric key for encrypting and decrypting files
File Recovery	Used with the symmetric key for recovering encrypted files

Certificates can also be logically grouped into the role they play within PKI or the specific application that uses them. See Table 35-2.

Table 35-2. Logical Certificate Stores

Store	Description
Personal	Any certificates assigned to you and associated with your private keys
Trusted Root Certification Authorities	Self-signed certificates of certification authorities
Intermediate Certification Authorities	Certificates issued to other people or to CAs
Enterprise Trust	Any Certified Trust Lists you create
Request	Pending or rejected certificate requests

Some applications that use certificates create a logical group. Microsoft NetMeeting is an example. Note that personal certificates are the only ones on your computer that might contain private keys.

Certificate Stores

We mentioned in the previous section how certificates are grouped. In the world of certificates, these groupings are called *stores*. Windows 2000 has two stores for certificates:

- **Physical.** The physical store references where certificates are physically stored in your system. Most are stored somewhere in the registry. If your computer is part of a Windows 2000 domain, some might be stored in Active Directory. Other physical stores are Local Group Policy and Local Computer.
- **Logical.** The logical store is a functional grouping of certificates irrespective of their physical location. Logical stores include Personal, Trusted Root Certification Authorities, Enterprise Trust, Intermediate Certification Authorities,

Active Directory User Object, Requests, and Software Publisher Certificates. In most cases, you operate on certificates from their logical stores. Any certificate can be in multiple logical stores.

Certification Authorities

Certification authorities grant or deny a certificate when a requester applies for one. It is the CA's responsibility to confirm the identity of the requester. Each CA applies its own set of requirements to requests. The requirements might depend on the purpose of the certificate. It is relatively easy to get a certificate for signing e-mail messages and harder to get one for signing software.

Just How Does a Certification Authority Know Who You Are?

The hierarchy of certificate authentication and trust rests on the certification authorities. It is their job to verify the identity of everyone requesting a certificate. But how do they do that? Their policies differ, but as an example we'll look at how one certification authority does it. Thawte is a CA that provides, among other things, free personal certificates. These certificates have two possible purposes: e-mail signing or encryption, and personal identification. The procedure Thawte uses to verify your identity depends on which purpose you specify in your request.

If you request a certificate for e-mail signing or encryption, the verification is quite simple. Thawte sends an e-mail message to the address listed in the request. The message contains the URL of a reply page at Thawte's Web site. To open the page, you must sign on with your Thawte account and password. Thawte interprets your opening that page as verification of the e-mail address, and the certificate is granted. This certificate contains your e-mail address but not your name. Then, whenever anyone receives an e-mail message signed with this certificate, he or she can be assured that you actually own the source e-mail account (even if the recipient has no assurance that you are who you say you are).

If you request a certificate for personal identification (that is, a certificate containing your name), the verification process is a bit more complicated. Thawte created a "Web of Trust"—essentially a worldwide group of notaries who verify your identity face-to-face. You must personally visit at least two notaries and present some valid identification, such as a driver's license or passport. If the notary is satisfied with your documents, he or she can award you between 10 and 35 points. When you receive 50 points, your identity is validated. In this system, you must identify yourself to at least two and as many as five people before Thawte validates your identity. Then Thawte approves your request for a certificate containing your name.

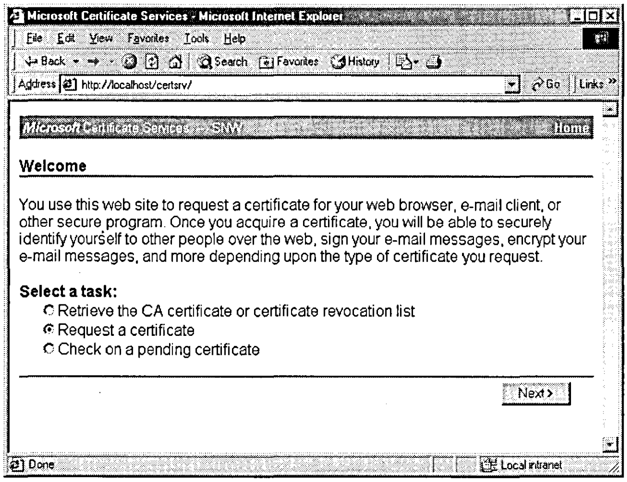
If you receive an e-mail message signed with a certificate that itself is signed by Thawte, and the certificate contains the name of a person, you know that person had to go through the steps just described to get that certificate. If the certificate is signed by Thawte but does not include a person's name, you know that the person confirmed only his or her e-mail account with Thawte.

Microsoft Windows 2000 Server offers certificate-granting services to computers in its domain or on its network. Microsoft Certificate Services is a CA with two potential means of access.

Certificate Services can be run as an enterprise service. In this case, it is available to all domain computers and grants certificates based on the requester's permissions in Active Directory. The Certificate Request Wizard works only with enterprise-wide Certificate Services.

Certificate Services can also be run in stand-alone mode. When run stand-alone, Certificate Services is available through an HTML interface, as shown in Figure 35-2. The stand-alone service does not automatically grant or deny requests. Requests are placed in a queue, and an administrator manually reviews them and decides whether to grant them. After you submit a request for a certificate from stand-alone Certificate Services on your network, you need to return to the service to find whether your request has been granted. The address of the stand-alone service is *http://*servername */certsrv,* where *servername* is the name of the computer running Certificate Services.

Note Lest you think an unscrupulous system administrator can use Certificate Services to create falsified certificates—he or she can. But remember that other users won't trust this certification authority. (Because it's not included in your list of trusted CAs, Windows 2000 displays a warning message if such a certificate is sent to you.)


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
Microsoft Certificate Services -- SNW
Home
Next >
Done
Local intranet

Address http://localhost/certsrv/

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

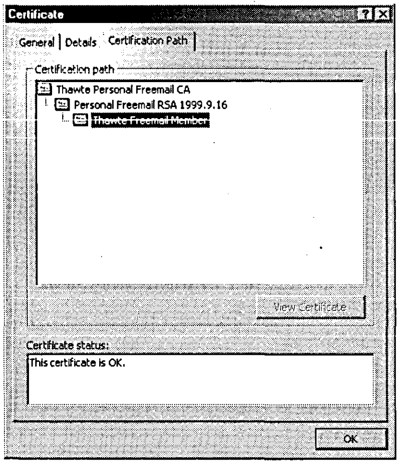
○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

Figure 35-2
The Windows 2000 Server Certificate Services is a certification authority with an HTML interface.

You can also request a certificate from one of the many certification authorities available on the Internet. Microsoft offers a list of CAs at *www.microsoft.com/windows/oe/certpage.htm.* Most of these services charge a fee for granting certificates, and each has its own method of verifying your identity. The fees and verification might also vary based on the type of certificate you request. If you are granted a certificate from a CA that is included in the trusted root certificates by default, you can be fairly sure that your certificate will be accepted by any Internet Explorer user and most likely by anyone else.

Two popular certification authorities are VeriSign (*https://digitalid.verisign.com*) and Thawte (*www.thawte.com*). To request a certificate from one of these CAs, go to its site and follow the instructions. When your certificate is approved, you download it and import it into your certificate store. Some sites perform the import as part of the download; other sites download a file that you must then manually import.

Certificate authentication works within a hierarchy of trust. At some point, there are CAs you trust because you choose to trust them. Unless you remove them, all the CAs installed by default in your Trusted Root Certification Authorities store are trusted without question. Trusted root authority certificates are self-signed—that is, they authenticate themselves. By contrast, the certificates of an intermediate CA are signed not by that CA itself but by another CA. If the other CA is a trusted root authority, the first CA is trusted by inference. You might have a whole chain of CA authentication ending with a trusted root authority. This chain is called the certificate path. The Certificate dialog box contains a tab called Certificate Path showing this chain of authentication back to a trusted root authority. See Figure 35-3.



Certification path

- Thawte Personal Freemail CA
  - Personal Freemail RSA 1999.9.16
    - Thawte Freemail Member

Certificate status:

This certificate is OK.

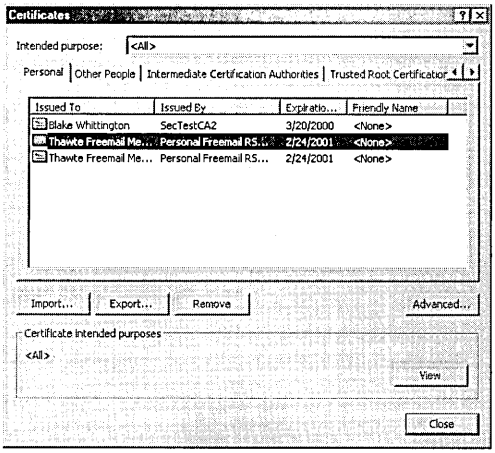
Figure 35-3
Each certificate has a certificate path, a chain of authentication back to a trusted root authority.

Using the Certificates Dialog Box

Open the Certificates dialog box in either of two ways:

- From Control Panel, go to Users And Passwords | Advanced | Certificates.
- From Internet Explorer, go to Tools | Internet Options | Content | Certificates.

However you open it, the Certificates dialog box you see looks like the one shown in Figure 35-4.



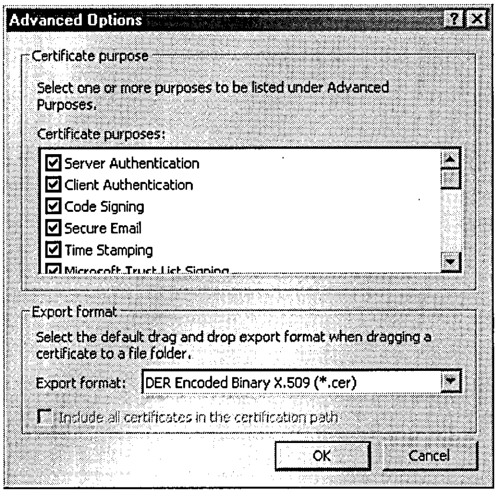
Issued To	Issued By	Expiratio...	Friendly Name
Blake Whittington	SecTestCA2	3/20/2000	<None>
Thawte Freemail Me...	Personal Freemail RS...	2/24/2001	<None>
Thawte Freemail Me...	Personal Freemail RS...	2/24/2001	<None>

Figure 35-4
You can manage all your certificate components from one dialog box.

The Certificates dialog box organizes your certificates on four tabs that roughly correspond to logical stores:

- **Personal.** This tab contains certificates with an associated private key (typically, your own personal certificates).
- **Other People.** This tab contains certificates with an associated public key. This category contains all certificates that are not in the Personal category and did not come from CAs.
- **Intermediate Certification Authorities.** This tab contains all certificates from CAs, including trusted root certificates.
- **Trusted Root Certificates.** This tab contains self-signing certificates. You intrinsically trust content from people and publishers with certificates issued by these CAs.

You can filter the certificates listed on each tab according to their purposes. In the Intended Purpose box, you can choose to see all certificates with any purpose (All) or only those certificates with advanced purposes. To set up or change the Advanced Purposes list, click the Advanced button. The Advanced Options dialog box presents you with a list of certificate purposes. (See Figure 35-5.) From this list, select the ones that you want to include in the Advanced Purposes list.


Advanced Options

Certificate purpose

Select one or more purposes to be listed under Advanced Purposes.

Certificate purposes:

☑ Server Authentication
☑ Client Authentication
☑ Code Signing
☑ Secure Email
☑ Time Stamping
☑ Microsoft Trust List Signing

Export format

Select the default drag and drop export format when dragging a certificate to a file folder.

Export format: DER Encoded Binary X.509 (*.cer)

□ Include all certificates in the certification path

Figure 35-5
Select the certificate purposes you want to include in the Advanced Purposes list.

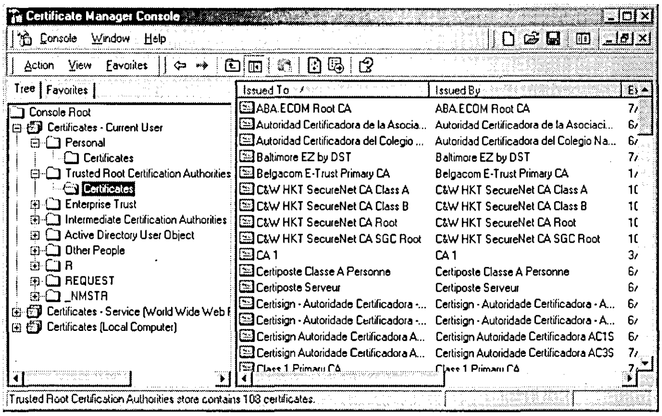
In the Certificates dialog box, double-click any certificate to view its contents. Click Remove to delete a selected certificate from your certificate stores. Be careful when removing a certificate. If you have encrypted anything using the keys in the certificate, you will never be able to decrypt the item again without the certificate.

Click Import or Export to start the Certificate Import Wizard or the Certificate Export Wizard. When you export a personal certificate that contains a private key, you have the option of exporting the private key with the certificate. If you choose to export the private key, you must supply a password to protect it. You will want to export the private key if you are exporting the certificate in order to import it to another computer of yours where you want to use the same keys.

Using the Certificates Snap-In

To use the Certificates snap-in for MMC, you must create a new console with the snap-in or add the snap-in to an existing console. *For details, see Chapter 4, "Using and Customizing Microsoft Management Console."* Note that the Certificates snap-in handles one of three accounts: current user, services, and local computer. Certificates can be associated with one or more of these accounts. To include all accounts in a console, you must add the snap-in three times, selecting a different account each time.

When you open a console with the Certificates snap-in, it looks something like the one shown in Figure 35-6. This example shows a snap-in for each of the three accounts. Under each account, folders organize certificates according to logical stores. To view a certificate, double-click its name in the details pane.


Certificate Manager Console
Console Window Help
Action View Favorites
Tree | Favorites
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Other People
R
REQUEST
_NMSTR
Certificates - Service (World Wide Web P
Certificates (Local Computer)

Issued To	Issued By	E›
ABA.ECOM Root CA	ABA.ECOM Root CA	7/
Autoridad Certificadora de la Asocia...	Autoridad Certificadora de la Asociaci...	6/
Autoridad Certificadora del Colegio ...	Autoridad Certificadora del Colegio Na...	6/
Baltimore EZ by DST	Baltimore EZ by DST	7/
Belgacom E-Trust Primary CA	Belgacom E-Trust Primary CA	1/
C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	1(
C&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	1(
C&W HKT SecureNet CA Root	C&W HKT SecureNet CA Root	1(
C&W HKT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	1(
CA 1	CA 1	3/
Certiposte Classe A Personne	Certiposte Classe A Personne	6/
Certiposte Serveur	Certiposte Serveur	6/
Certisign - Autoridade Certificadora -...	Certisign - Autoridade Certificadora - A...	6/
Certisign - Autoridade Certificadora -...	Certisign - Autoridade Certificadora - A...	6/
Certisign Autoridade Certificadora A...	Certisign Autoridade Certificadora AC1S	6/
Certisign Autoridade Certificadora A...	Certisign Autoridade Certificadora AC3S	7/
Class 1 Primary CA	Class 1 Primary CA	7

Trusted Root Certification Authorities store contains 108 certificates.

Figure 35-6
The Certificates snap-in allows you to manage all your certificates from an MMC console.

Exporting and Importing Certificates

The Certificates snap-in calls the same wizards for importing and exporting as the Certificates dialog box does. To export a certificate, right-click its icon in the details pane and choose All Tasks | Export. The Certificate Export Wizard starts.

To import a certificate, right-click an empty area of the details pane of the certificate folder into which you want to import and choose All Tasks | Import. Note that the Import Certificate Wizard imports a certificate into the most appropriate folder, which might not be the one that you select. For instance, if you attempt to import a personal certificate into the Intermediate Certification Authorities folder, you will find that it actually shows up in the Personal folder.

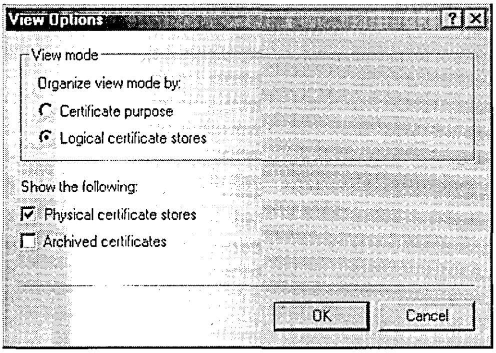
Requesting Certificates

The snap-in gives you two options for renewing expired or about-to-expire certificates: you can renew them with the same keys or with new keys. If you are concerned that the keys might be compromised, you might want to renew the certificate with new keys. You renew a certificate by right-clicking its icon and choosing All Tasks | Renew Certificate With Same Key or All Tasks | Renew Certificate With New Keys.

The snap-in allows you to request a new certificate from enterprise Certificate Services on your domain. If you have enterprise Certificate Services, you can right-click a blank area of the details pane of a certificate folder and choose All Tasks | Request New Certificate. Follow the wizard's instructions to request a certificate. You must have the proper permissions set in Active Directory to be granted a certificate.

Changing View Options

By default, the snap-in displays certificates organized by logical stores. But you can set up views that organize them differently. Select a top-level Certificates snap-in and then choose View | Options. The View Options dialog box appears, as shown in Figure 35-7.



View mode

Organize view mode by:

○ Certificate purpose

● Logical certificate stores

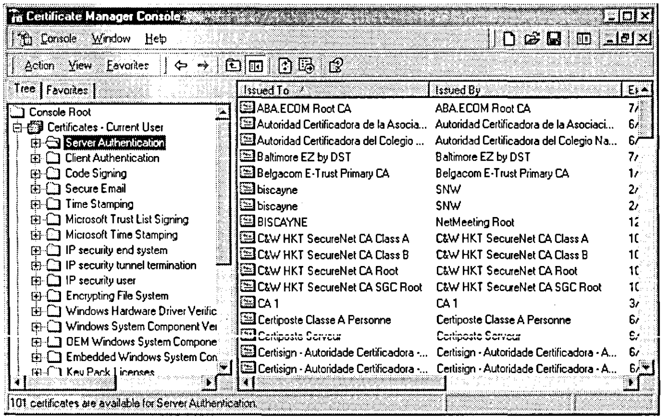
Show the following:

☑ Physical certificate stores

□ Archived certificates

Figure 35-7
The Certificates snap-in organizes its display of certificates by certificate purpose or logical store.

The View Options dialog box has two view modes: Certificate Purpose and Logical Certificate Stores (the default). Selecting Certificate Purpose causes the certificates to be displayed in folders organized according to purpose, as shown in Figure 35-8. If you select Logical Certificate Stores, you can also choose to show Physical Certificate Stores. If both logical and physical stores are displayed, the console tree is organized as shown in Figure 35-9. When physical stores are displayed, the All Tasks menu for a store folder includes an Export Store command. Choosing this command exports the entire store to a backup file. By default, the snap-in does not display archived certificates, but you can select Archived Certificates in the View Options dialog box to display them.

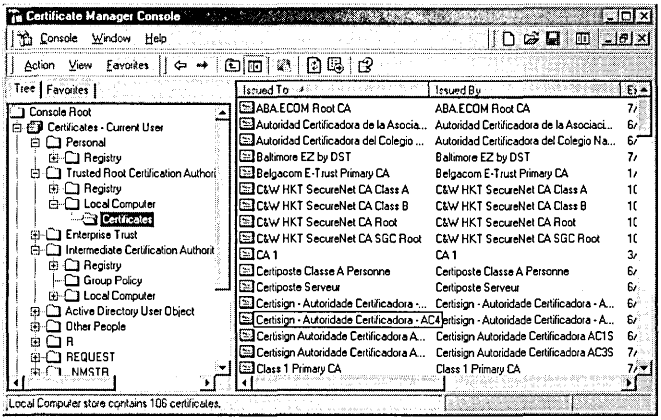


- Console Root
  - Certificates - Current User
    - Server Authentication
    - Client Authentication
    - Code Signing
    - Secure Email
    - Time Stamping
    - Microsoft Trust List Signing
    - Microsoft Time Stamping
    - IP security end system
    - IP security tunnel termination
    - IP security user
    - Encrypting File System
    - Windows Hardware Driver Verific
    - Windows System Component Ver
    - OEM Windows System Compone
    - Embedded Windows System Con
    - Key Pack Licenses

Issued To	Issued By	E
ABA.ECOM Root CA	ABA.ECOM Root CA	7/
Autoridad Certificadora de la Asocia...	Autoridad Certificadora de la Asociaci...	6/
Autoridad Certificadora del Colegio ...	Autoridad Certificadora del Colegio Na...	6/
Baltimore EZ by DST	Baltimore EZ by DST	7/
Belgacom E-Trust Primary CA	Belgacom E-Trust Primary CA	1/
biscayne	SNW	2/
biscayne	SNW	2/
BISCAYNE	NetMeeting Root	12
C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	10
C&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	10
C&W HKT SecureNet CA Root	C&W HKT SecureNet CA Root	10
C&W HKT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	10
CA 1	CA 1	3/
Certiposte Classe A Personne	Certiposte Classe A Personne	6/
Certiposte Serveur	Certiposte Serveur	6/
Certisign - Autoridade Certificadora -...	Certisign - Autoridade Certificadora - A...	6/
Certisign - Autoridade Certificadora -...	Certisign - Autoridade Certificadora - A...	6/

101 certificates are available for Server Authentication.

Figure 35-8
You can display certificates organized by purpose.



Issued To	Issued By	E›
ABA.ECOM Root CA	ABA.ECOM Root CA	7/
Autoridad Certificadora de la Asocia...	Autoridad Certificadora de la Asociaci...	6/
Autoridad Certificadora del Colegio ...	Autoridad Certificadora del Colegio Na...	6/
Baltimore EZ by DST	Baltimore EZ by DST	7/
Belgacom E-Trust Primary CA	Belgacom E-Trust Primary CA	1/
C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	1(
C&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	1(
C&W HKT SecureNet CA Root	C&W HKT SecureNet CA Root	1(
C&W HKT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	1(
CA 1	CA 1	3/
Certiposte Classe A Personne	Certiposte Classe A Personne	6/
Certiposte Serveur	Certiposte Serveur	6/
Certisign - Autoridade Certificadora -...	Certisign - Autoridade Certificadora - A...	6/
Certisign - Autoridade Certificadora - AC4	ertisign - Autoridade Certificadora - A...	6/
Certisign Autoridade Certificadora A...	Certisign Autoridade Certificadora AC1S	6/
Certisign Autoridade Certificadora A...	Certisign Autoridade Certificadora AC3S	7/
Class 1 Primary CA	Class 1 Primary CA	7/

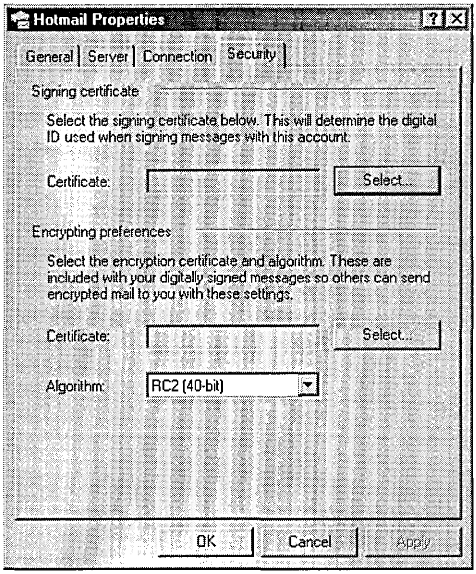
Local Computer store contains 106 certificates.

Figure 35-9
You can display physical stores as well as logical stores.

Signing and Encrypting E-mail Messages

Signing and encrypting e-mail messages are two distinct tasks that use certificates in different ways. When you sign a message, you mark it with your own private key. A person with your public key can be assured that you sent the message, because only you have access to your private key. When you encrypt a message, you want only the recipient to be able to decrypt it. Therefore, you use the recipient's public key for encryption. Only the person with the private key can decrypt it. That might seem counterintuitive at first: you might think that you should encrypt outgoing e-mail messages with your own private key. But remember, anyone with your public key can decrypt the message, and your public key is, well, public.

Different e-mail clients work slightly differently when it comes to certificates. In most cases, you must let the client know which certificates you want to use for signing and the certificate containing the public key that you want others to use when sending you encrypted messages. These can be the same certificate. In Microsoft Outlook Express, you configure these for each e-mail account. Open the properties dialog box for an account (choose Tools | Accounts, select an account, and click Properties) and click the Security tab. See Figure 35-10. The Security tab has selections for the signing certificate and the encrypting preferences. The encryption preferences include the certificate and the encryption algorithm. When you send a signed message, the encryption certificate is sent along with the message so that the recipient can store your certificate.



Signing certificate

Select the signing certificate below. This will determine the digital ID used when signing messages with this account.

Certificate:

Encrypting preferences

Select the encryption certificate and algorithm. These are included with your digitally signed messages so others can send encrypted mail to you with these settings.

Certificate:

Algorithm: RC2 (40-bit)

Figure 35-10
You must configure your e-mail client in order to use certificates for signing and encryption.

When you receive a message with a certificate, Outlook Express stores a reference to the certificate in your Address Book. Then, if you want to send an encrypted message to that person, Outlook Express automatically knows which key and algorithm to use.

Part 9

Automating Tasks

Chapter 36
Using Doskey Macros 599

Chapter 37
Using Batch Programs 609

Chapter 38
Using Windows Script Host 627

Chapter 36

Using Doskey Macros

In This Chapter

Defining Macros 600

Managing Macros 600

Placing Comments in Macro Files 601

Using Parameters in Macros 601

Using Symbols in Macros 602

Replacing Windows 2000 Commands with Doskey Macros 604

Understanding Doskey Switches 606

Using Doskey Macros in Programs 606

When you want to automate a task that can be performed at the command prompt, Doskey macros serve as the first level of automation. *(For information about the command prompt, see Chapter 11, "Using the Command Prompt.")* A *macro* is a keystroke sequence that is passed to the command interpreter (Cmd.exe or Command.com) or other character-based program when you type the name of the macro. Macros are easy to define, they take up little disk space and memory, and they execute instantly. They work best for shortening long commands and assigning a name to a simple sequence of commands. At some point, you'll find that the tasks you want to automate are too complex for macros. When that happens, move up to the second level of automation—batch programs.

Doskey macros and batch programs are two similar ways to create new commands by combining existing commands and programs. In both cases, you essentially give simple names to longer commands or sequences of commands. *(For information about batch programs, see Chapter 37, "Using Batch Programs.")*

Defining Macros

The simplest Doskey macro is one that gives a short name to a long command. Starting the command-reference Help program at the Windows 2000 command prompt normally requires a long command line. You can abbreviate that command by entering the following at the command prompt:

```
C:\>doskey h=hh.exe mk:@MSITStore:C:\WINNT\Help\windows.chm::/ntcmds.htm
```

Note To find the address of a help topic, go to the topic, right-click the topic, and choose Properties. Although you can't edit the Address field in the properties dialog box, you can select and copy the text.

This command defines a macro named H; the content of the macro is the text that follows the equal sign. After defining this macro, you can get help information about Windows 2000 commands at any time with the following command:

```
C:\>h
```

You can make this macro a little more reliable by using the %SystemRoot% environment variable instead of providing an absolute path. Your Help folder might not be in the C:\Winnt folder, but it will definitely be in the %SystemRoot% folder.

```
C:\>doskey h=hh.exe mk:@MSITStore:%SystemRoot%\Help\windows.chm::/ntcmds.htm
```

The new macro overrides the previous definition of the H macro.

If you want to eliminate an existing macro (perhaps because you gave it the wrong name), simply assign the name a blank value, like this:

```
C:\>doskey h=
```

Managing Macros

Doskey macros are local to each Command Prompt session. If you define a macro in one session, it won't be available in other sessions. If you exit the session in which you defined it, your macro is gone. You should save useful macros so that you can load them whenever and wherever you want.

The easiest way to save macros in a file is with Doskey's /Macros switch. This switch displays all active macros on the screen. However, the default action isn't very useful; normally you'll want to redirect your macros to a file. For example:

```
C:\>doskey /macros > c:\cmdinit.mac
```

After you create a file with Doskey macros from one session, you can read them into another session with the /Macrofile switch, like this:

```
C:\>doskey /macrofile=c:\cmdinit.mac
```

Of course, you don't really want to type this command line every time you start a new Command Prompt session, so you should put it in your AutoRun file. *For more information, see "Using AutoRun to Execute Commands When Command Prompt Starts," page 188.*

After you develop a library of macros, you can organize them in different files. You'll probably want one group that you load automatically in every Command Prompt window. Then you might want to add a few more files for different types of work. You might have an Organize.mac file that you load only when you're organizing files, or a Program.mac for programming tasks. You can create or edit macro files with any text editor (WordPad, Notepad, or Edit, for example).

Note If you use WordPad to create or edit macro files, be sure to save your files as text documents.

Placing Comments in Macro Files

Windows 2000 doesn't have a comment character for macro files, but you can define your own. Choose a character that you would never use as a command—a semicolon is a good choice—and follow it by an equal sign so that Doskey won't complain about an illegal macro. Then add the text of your comment. (Technically, you're defining a macro named ";" with the comment text.) For example:

```
;= Set 80x50 line mode
50=mode con:lines=50

;= Set 80x25 line mode
25=mode con:lines=25

;= Set a given number of lines
Lines=mode con:lines=$1

;= Set a given number of columns
Cols=mode con:cols=$1

;=
```

The ;= at the end cleans up by clearing the macro assigned to the semicolon character.

Using Parameters in Macros

In macros, you use $1 to $9 to represent up to nine command-line parameters. (In batch programs, you use %1 to %9 for the same purpose.) For example, you might write the following macro to shorten the name of the Start command to the letter *S*:

```
C:\>doskey s=start $1
```

You wouldn't really want this macro because it accepts only one parameter. If you type *s edit /h autoexec.nt*, you start the editor, but the /H switch and the name of the file to edit are lost. You could add $2 $3 $4 (and maybe more) to your macro, but Doskey has a better solution.

In Doskey macros, $* represents all the arguments passed, even if there are more than nine.

```
C:\>doskey s=start $*
```

Using Symbols in Macros

You can use redirection, piping, and command combination symbols in macros, but you must insert a caret (^) before each one. *For more information about these symbols, see "Using Command Symbols," page 181.* Otherwise, the symbols are interpreted as part of the command line rather than as part of the macro. For example, you might try defining a macro that saves your current macros to a file, like this:

```
C:\>doskey macsave=doskey /macros > %temp%\current.mac
```

This command actually redirects the output of the macro definition line up to the redirection symbol (>) to Current.mac. But the Doskey command doesn't produce any output, so you end up with an empty file. Meanwhile, the Macsave macro has been defined to display macros to the screen rather than to a file. Here's the correct definition command:

```
C:\>doskey macsave=doskey /macros ^> %temp%\current.mac
```

Here's an example in which the pipe symbol requires a caret. The macro creates an enhanced Type command that pipes output through the More filter.

```
C:\>doskey mtype=type $* ^| more /e
```

You need the caret only when defining a macro at the command prompt. Don't put it in your macro files. It won't show up when you display current macros with the /Macros switch.

Although the caret preceding a symbol works properly with macros written for Cmd.exe (that is, macros that replace something you would type at the Cmd.exe command prompt), some other programs don't recognize this sequence. The original version of Doskey, which was part of MS-DOS 5, used character sequences of a dollar sign ($) and a letter rather than a caret/symbol combination. Some character-based programs (such as Ftp.exe) recognize only the dollar sign character sequences. For compatibility, Cmd.exe recognizes both types of sequences. Table 36-1 shows the symbols you can use in Doskey macros.

Table 36-1. Special Characters in Macros

Command-Line Symbol	Function	Macro Sequence (Cmd.exe)	Macro Sequence (Universal)*
<	Redirects input	^<	$L
>	Redirects output	^>	$G
>>	Appends redirected output	^>^>	GG
|	Pipes output	^|	$B
&	Combines multiple commands in a command line	^&	$T
&&	Runs the command after && only if the command before && is successful	^&^&	
||	Runs the command after || only if the command before || fails	^|^|	
^	Displays caret	^^	^
	Command-line parameters	$1 through $9	$1 through $9
	All command-line parameters	$*	$*
	Dollar sign character ($)	^$	$$

* The Doskey character sequences are not case sensitive; you can also use lowercase letters.

Sample Macros

You might find it useful to create a group of folder-listing commands. The idea here is that each variation of the Dir command starts with D and has one or two modifying letters that indicate its function.

```
;= Default folder listing
D=dir $*
;= Folder listing with pause
Dp=dir /p $*
;= Folder listing of visible files sorted by extension
De=dir /a-d-h-s $* /oe
;= Folder listing of visible files only
Df=dir /a-d-h-s $*
;= Wide folder listing sorted in columns
```

(continued)

Sample Macros *(continued)*

```
Dc=dir /d $*
;= Wide folder listing sorted in rows
Dr=dir /w $*
;= Bare folder listing of visible files only
Db=dir /b /a-d-h-s $*
;= Tree folder listing of visible files only
Dt=dir /s /a-d-h-s $*
;= Folder listing of both short and long file names
Dx=dir /x $*
;=
```

To use these macros, enter the data in your editor, save it as a macro file called Dir.mac, and load it with the Doskey /Macrofile switch. When using the macros, you can include additional options on the command line.

Replacing Windows 2000 Commands with Doskey Macros

If you define a Doskey macro with the same name as a Windows 2000 command, the macro will replace that command. This is handy if you always (or almost always) want to use a specific set of switches with a command. You can still use the Windows 2000 command as well as the Doskey macro.

- To run the macro, type the macro name immediately after the command prompt.
- To run the Windows 2000 command, type one or more spaces before you type the command.

You can also use Doskey macros to change the behavior of Windows commands. Consider the Copy command and the Xcopy command. Why are they separate? Xcopy does a better job of almost everything Copy does, plus more. You can enhance the Copy command by entering the following command:

```
C:\>doskey copy=xcopy /i /f $*
```

Copy now works faster, has a neater and more consistent output, and can do nearly any copy operation you can imagine except one—combine multiple files into one. If you need to combine files, nothing but the real Copy command will do—but you don't have the real Copy command because you've defined it away.

To use the built-in Copy command, you have two alternatives. First, you can still use the Copy command. Simply precede it with one or more spaces on the command line:

```
C:\>  copy one.doc+two.doc onetwo.doc
```

Better yet, create a Combine command that does what the Copy command used to do:

```
C:\>doskey combine=copy $*
```

Notice that the Combine macro calls Copy, but Copy has been redefined to mean Xcopy. So, which Copy does Combine use, the built-in command or the macro? It turns out that macros know nothing about other macros and can't call them. The Combine command uses the built-in Copy command.

We've defined Copy to mean Xcopy, so now we don't need Xcopy anymore. Now we'll redefine Xcopy to do the most common Xcopy task, copying entire folder trees:

```
C:\>doskey xcopy=xcopy /e /i /f /k $*
```

The /E switch makes Xcopy always copy entire trees, including empty folders. The /F switch shows both the source and destination of each file copied. The /K switch copies the file attributes of the files copied.

The /I switch fixes an annoying characteristic of the Xcopy command. Assume that you try to copy a folder full of files to a new folder.

```
C:\>xcopy olddir newdir
Does newdir specify a file name
or directory name on the target
(F = file, D = directory)?
```

The /I switch assumes that you want to copy to a folder (directory) and suppresses the question. We also used it earlier when redefining Copy to Xcopy.

It's a bit risky to change Windows 2000 commands. You might forget what you did and try to use the old version. If someone else uses your computer, that person might be confused. If you use someone else's computer, *you* might be confused. Think of the previous examples as illustrations of what you *can* do, not what you *should* do. Redefining commands can be useful if you always want to use certain switches with a command, but it can cause problems as well.

For example, our new, more powerful Copy command usually works the same as the old version, but not always, as the following command illustrates:

```
C:\>copy *.doc docfiles
```

The built-in Copy command appends all the .doc files to create one combined file named Docfiles. The new Copy command copies the first .doc file to Docfile, then overwrites it with the second, and so on. The resulting Docfile contains only the last .doc file.

Understanding Doskey Switches

Doskey has additional options beyond the /Macros and /Macrofile switches we discuss in this chapter. Table 36-2 describes all the Doskey switches.

Table 36-2. Doskey Switches

Switch	Purpose
/Reinstall	Loads a new copy of Doskey and clears the command history buffer
/Listsize=*size*	Sets the maximum number of commands in the command history buffer
/Macros or /M	Displays the active command prompt macros; you can save this to a file with the redirection symbol (>)
/Macros:all	Displays the active macros for all programs
/History	Displays the command history; you can save this to a file with the redirection symbol (>)
/Insert or /Overwrite	Sets editing to insert or overwrite (the default); you can change this for one line with the Insert key
/Exename=*program*	Specifies the program in which the macro will run
/Macrofile=*filename*	Loads macros from a file

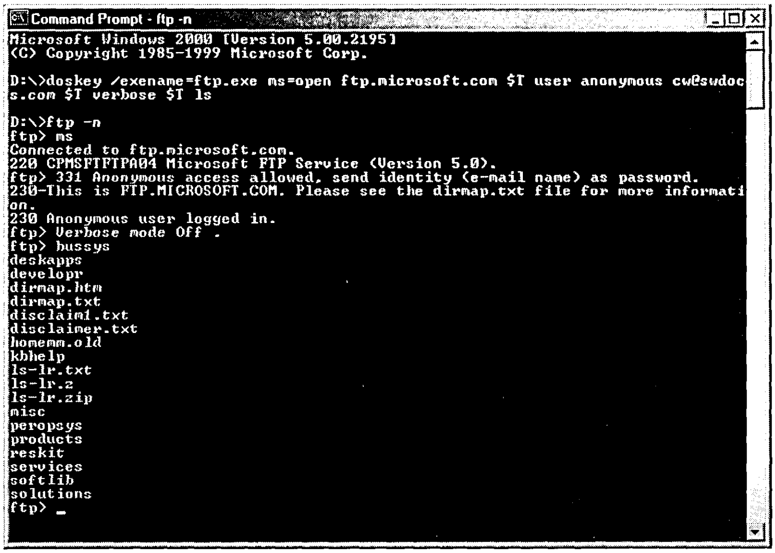
Using Doskey Macros in Programs

You can use Doskey macros in some character-based interactive programs, such as program debuggers or Ftp.exe. To use Doskey, a character-based program (that is, one that runs in a console or Command Prompt window) must use buffered input. Just as it does at the command prompt, Doskey maintains a command history for each program you start, which allows you to repeat and edit previous commands at the program's prompt. *For information about command history, see "Editing the Command Line," page 180.*

Here's an example of a macro definition that works inside a program:

```
C:\>doskey /exename=ftp.exe ms=open ftp.microsoft.com $T user anonymous cw@swdocs.com
   $T verbose $T ls
```

The addition of the /Exename switch tells Doskey which program the command is to be used with. This command works in the Internet file-transfer program FTP. (You must start FTP with the -N switch to turn off autologin.) When you type *ms* in FTP, it opens *ftp.microsoft.com* and logs in anonymously. It turns off verbose messages and retrieves an abbreviated directory, as shown in Figure 36-1.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

D:\>doskey /exename=ftp.exe ms=open ftp.microsoft.com $T user anonymous cw@swdoc
s.com $T verbose $T ls

D:\>ftp -n
ftp> ms
Connected to ftp.microsoft.com.
220 CPMSFTFTPA04 Microsoft FTP Service (Version 5.0).
ftp> 331 Anonymous access allowed, send identity (e-mail name) as password.
230-This is FTP.MICROSOFT.COM. Please see the dirmap.txt file for more informati
on.
230 Anonymous user logged in.
ftp> Verbose mode Off .
ftp> bussys
deskapps
developr
dirmap.htm
dirmap.txt
disclaim1.txt
disclaimer.txt
homemm.old
kbhelp
ls-lr.txt
ls-lr.z
ls-lr.zip
misc
peropsys
products
reskit
services
softlib
solutions
ftp> _
```

Figure 36-1
In this figure, the entries you would type have been highlighted for illustrative purposes.

By convention, the password for anonymous logon to FTP sites is your e-mail address. You should change the e-mail address in the command shown previously to your own e-mail address.

You must define your Doskey macros at the command prompt. You can't define a macro or use any Doskey options when you are in a program. As with command prompt macros, the easiest way to load a set of macros for a program is by saving them in a file. You might, for example, want to create a command prompt macro that loads your collected FTP macros from a file called Ftp.mac and then starts Ftp.exe with the -N switch, like this:

```
C:\>doskey ftp=doskey /exename=ftp.exe /macrofile=ftp.mac ^& ftp -n
```

Chapter 37

Using Batch Programs

In This Chapter

Understanding Batch Program Basics 610

Using Batch Commands 610

Learning from a Simple Batch Program 612

Creating More Complex Batch Programs 615

Using Other Batch Program Tricks 624

A *batch program* (also commonly called a *batch file*) is a text file that contains a sequence of commands to be executed. You define the sequence of commands, name the sequence, and then execute the commands by entering the name at a command prompt.

When you type the name of your batch program at the command prompt, the command interpreter opens the file and starts reading the statements. It reads the first line, executes the command, and then goes on to the next line. On the surface, this seems to operate just as if you were typing each line yourself at the command prompt. In fact, however, it can be much more complicated because you can use parameters with batch programs to vary their behavior just as you can with other types of programs. Batch programs can also respond to values returned by programs and to the values of environment variables.

At this level, writing batch programs becomes computer programming. You might not feel like a programmer after writing your first batch program—it seems too simple. But as you learn to handle parameters, environment variables, and values returned from programs, you'll start to feel first a sense of accomplishment and then eventually some frustration. Developing batch programs turns out to be one of the most complex and difficult forms of programming because the batch language doesn't provide many tools to work with. Microsoft Windows 2000 has other tools, such as Windows Script Host, that are much more capable. *(For more information, see Chapter 38, "Using Windows Script Host.")*

Understanding Batch Program Basics

Batch programs are text files created with a text editor. You can use Notepad if you like a graphics-based editor or Edit if you prefer a character-based editor. More likely, you already have a favorite text editor or a word processor that can produce unformatted files. If you use a word processor, remember to save your batch programs as text-only files.

In Windows 2000, you can name your batch programs with a .bat or .cmd file name extension. The Windows 2000 command interpreter, Cmd.exe, attempts to execute commands from any file with either of these extensions. If you're coming to Windows 2000 from MS-DOS or Windows 9x, you might already have some batch programs with the .bat extension. They should work fine under Windows 2000. If you're coming from OS/2 and have batch programs with the .cmd extension, they should also work without change. If you're writing new batch programs to run only under Windows 2000, you can take your pick of the two extensions. When you type the name of a batch program at a command prompt, Cmd.exe looks first for a file with a .bat extension. If you have two batch programs in the same folder with the same base name but different extensions, the .bat file will be executed—not the .cmd file. You can override this behavior by including the extension when you type the file name. We use .bat for the sample batch programs in this chapter.

The rules for capitalization in batch programs are the same as at the command prompt: there are none. Commands and labels are not case sensitive, and you can mix capital and lowercase letters at will. (With certain commands, however, switches and parameters are case sensitive.) In the examples in this book, we show commands in lowercase because that's the easiest to type (although we capitalize command names in explanatory text). Labels are uppercase so that they stand out clearly. We use mixed case for messages that appear on the screen and for creating folders or files, because the capitalization is retained when the text is transferred to screen or disk.

Note Several examples in this chapter include commands that won't fit on a single line on the printed page of this book. The second and subsequent lines of such commands are indented. You, however, should type these commands on a single line.

Using Batch Commands

Batch commands are the commands that generally make sense only when used from a batch program. Some of the commands we discuss here can actually be used from the command line but generally aren't. With a few exceptions, Windows 2000 has the same batch program commands as MS-DOS. We start by summarizing all the batch commands, in Table 37-1, and then look at some Windows 2000 batch programs. We explain some of the commands, but for most of them, this table—along with the command reference in Windows 2000 Help—should suffice. To display the command reference, go to Start | Help | Contents | Reference\MS-DOS Commands. Alternatively, at the command prompt, type *hh windows.chm::/ntcmds.htm*. You can also get help about the commands using the /? option. (That is, at the command prompt, type the command followed by /?.)

Table 37-1. Batch Commands

Command	Purpose
@	When used as the first character in a line, prevents the line from being displayed on the screen.
Echo [Off | On]	Turns screen echoing off or on.
Echo *msg*	Displays *msg* on the screen.
Echo.	Displays a blank line on the screen.
Rem *msg*	Identifies *msg* as a comment.
If [Not] Errorlevel *num cmd*	If the error level value returned from the previous command is less than or equal to *num*, *cmd* is executed. (Not reverses the logic.)
If [Not] Exist *file cmd*	If *file* exists, *cmd* is executed. (Not reverses the logic.)
If [Not] *txt1*== *txt2 cmd*	If *txt1* is the same as *txt2*, including case, *cmd* is executed. (Not reverses the logic.)
Goto *label*	Transfers control to the line marked by *label*.
: *label*	Names the line to be reached by a Goto command.
For %%*var* In (*set*) Do [*cmd*] %%*var*	Loops through the items in *set*, executing *cmd* for each loop and replacing any instances of *var* with the matching item from *set*, which can be a list separated by spaces or can contain the wildcard characters * and ?.
Shift	Shifts command-line parameters one place so that %2 becomes %1, %3 becomes %2, and so on.
Call *batfile args*	Executes *batfile* with *args* and then returns to the calling batch program.
Setlocal	Makes current environment variables local to this batch program; any changes to variables are known only in this batch program until Endlocal is executed.
Endlocal	Makes environment variables known to the system; any changes made after Endlocal remain in effect when the batch program terminates.
Pushd *path*	Saves the current folder on a stack and changes to *path*.
Popd	Restores the last folder saved by Pushd.
Pause	Suspends processing until a key is pressed.
Title	Sets the title of the Command Prompt window.

Putting Comments in Batch Programs

Using the Rem command is the documented way to put comments in your batch programs, but it is intrusive because the command looks like part of the comment. Furthermore, if you leave echoing on while debugging a batch program, all your comments are echoed, making it harder to read commands. A better way to comment code is to use two colons:

```
:: This line is for humans; computers ignore it
```

This kind of comment is never echoed. Be sure to use two colons; using only one creates a label that might conflict with a legitimate label. Although this commenting style is handy, we use the conventional Rem statement in this book's examples to avoid confusing readers who miss this tip.

Learning from a Simple Batch Program

Rather than trying to discuss each batch program feature in succession, let's plunge into the deep end and learn by example. If you're new to batch programs, the following program is simple enough that you can probably figure it out, though it won't be easy going. Yet the example is interesting enough that you might learn something new even if you're a batch program wizard.

The most important step in writing a batch program (or any other kind of computer program) is to state the problem correctly. In this case, the problem is to connect to a dial-up connection by repeatedly dialing different connections until a successful connection is made. If a connection fails (because the line is busy or you enter the wrong password, for example), the program should try another dial-up connection.

This batch program relies on Rasdial.exe, the command-line version of the dialing component used by dial-up connections. The program uses dial-up connections that you have previously created in the Network And Dial-Up Connections folder.

You execute a batch program by typing its name at the command prompt, like this:

```
C:>dial
```

You don't have to add the .bat extension unless another program or built-in command has the same name.

The following listing shows Dial.bat in its entirety:

```
@echo off
rem Connects to a Dial-up Connection
title Dialing Connections
```

```
:START
echo Connecting to MSN
rasdial msn pct_hiker *
if not errorlevel 1 goto end

echo Connecting to Earthlink
rasdial earthlink swdocs *
if not errorlevel 1 goto end

echo Connecting to local ISP
rasdial "pasadena isp" swdocs *
if errorlevel 1 goto start

:END
title Command Prompt
```

By default, batch programs display each line on the screen before attempting to execute it. Because this is seldom desirable, most batch programs start with the same line that ours starts with:

```
@echo off
```

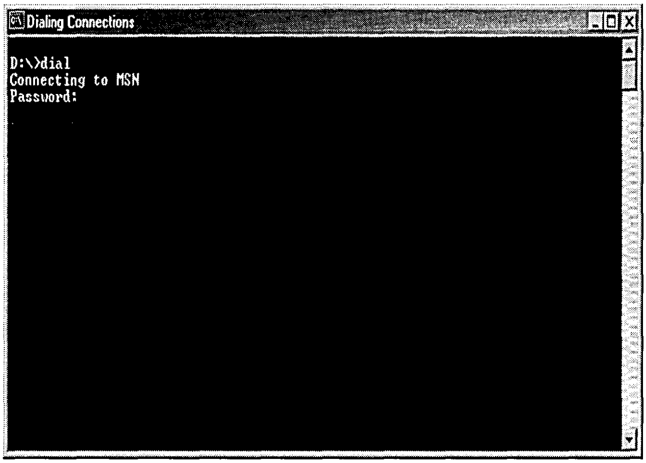
The at sign (@) says not to display the Echo Off command. The Echo Off command says not to display any more lines for the rest of the batch program.

The line that follows the descriptive Rem statement,

```
title Dialing Connections
```

sets the title of the Command Prompt window to Dialing Connections, as shown in Figure 37-1. This title helps orient users to the task at hand.

Between the Start and End labels are three sets of dialing commands—one for each Internet service provider (ISP) for which we've created a dial-up connection. As we've used it here, the parameters following Rasdial are the connection name (the name that appears in the Network And Dial-Up Connections folder) and the user name. The asterisk causes Rasdial to prompt for your password; you could put the password in your batch program (in plain text) if you're sure that it won't be compromised. Like many programs, when Rasdial exits, it sets an error level, which is simply a numeric result code. The If statement in Dial.bat tests the error level for values of 1 *or greater.* An error level of 0 indicates a successful connection. (Rasdial uses many other values to indicate various error conditions. For a list of error codes, type *hh netcfg.chm* to open Network And Dial-Up Connections help; on the Contents tab, go to Troubleshooting\Error Messages.)



```
D:\>dial
Connecting to MSN
Password:
```

Figure 37-1
The Title command sets the title of the Command Prompt window.

Better Options for Testing Error Level Values

If you want your batch program to take different actions based on different error level values, you can use successive If statements to test for each value. With MS-DOS and earlier versions of Windows, it was necessary to test error level values in decreasing order, because the condition is true if the error level value is equal to or greater than the value you specify. But if you're writing a batch program for use only on computers running Windows 2000, you can use comparison operators to more easily act on different error level values. To do that, you must use the %ErrorLevel% environment variable, which expands into the current value of error level. For example, you might use a statement like the following to jump to a certain section of the program if Rasdial sets e rror level to 676, the result code that indicates the line is busy:

```
if %errorlevel% equ 676 goto busy
```

The available comparison operators are Equ (equal to), Neq (not equal to), Lss (less than), Leq (less than or equal to), Gtr (greater than), and Geq (greater than or equal to). You can use comparison operators only if command extensions are enabled. *For information about command extensions, see "Using Command Extensions," page 190.*

Each of the If commands includes a Goto command that directs processing to the correct part of the batch program. When a Goto is executed, the command interpreter jumps to the line with the matching label and starts executing the lines it finds following the label. (A label is a line starting with a colon.) Following the first two connection attempts, if the error level value is *not* greater than or equal to 1, the command processor transfers control to the End label; otherwise, it drops down to the next statement. In the final If statement, the program jumps back up to the Start label if the error level is greater than or equal to 1.

The Goto End statement prevents the subsequent commands from being executed by directing processing to the End label. Without these statements, Rasdial would dial the second and third connections, even if the first one was successful.

The single statement that follows the End label simply resets the window title.

Creating More Complex Batch Programs

This section offers a few example batch programs that illustrate some additional programming techniques. You can find these batch files on the companion CD.

Backing Up the Removable Storage Database

This batch program creates a backup copy of the Removable Storage database. Although this batch program is not terribly useful, it illustrates some commonly used techniques, including stopping and starting services and using environment variables. The following program is called Rsbackup.bat:

```
@echo off
rem Backs up the Removable Storage database
title Removable Storage Backup
echo Removable Storage database backup in process...

echo Stopping the Removable Storage service
net stop "removable storage" > nul

echo Copying the Removable Storage database
xcopy /y %systemroot%\system32\ntmsdata %systemroot%\system32\ntmsdata
    \backup\ > nul

echo Starting the Removable Storage service
net start "removable storage" > nul

echo.
echo Removable Storage database was backed up to
echo %SystemRoot%\System32\NtmsData\Backup\
title Command Prompt
```

The first command to examine is Net Stop:

```
net stop "removable storage" > nul
```

The Net command is frequently included in batch programs because it can be used to control so many functions in Windows. In this case, we are stopping the Removable Storage service to ensure that it doesn't have the database files open when we try to copy them. To stop or start a service, you can use the service's "friendly name" (the name that appears in the Services snap-in), as we've done here, or you can use the actual service name if you know it. (In the case of Removable Storage, the service name is Ntmssvc.)

Throughout the program, Echo statements keep the user informed of the progress. Therefore, we use > Nul to redirect the output of the Net statement to the Nul device—colloquially known as the "bit bucket"—because its output is redundant.

The Xcopy command then makes a copy of the files:

```
xcopy /y %systemroot%\system32\ntmsdata systemroot%\system32\ntmsdata
    \backup\ > nul
```

On most computers, the Removable Storage database files are stored in C:\Winnt\System32\Ntmsdata. However, if you installed Windows to a different folder, the files will be in a different location. In this Xcopy statement, %SystemRoot% is an environment variable that specifies where Windows is installed on the local computer. By using environment variables, we can ensure that our batch programs work on any computer that is running Windows 2000.

Table 37-2 lists some useful environment variables. You can see the current environment variables for your computer by typing *set* at the command prompt. To use an environment variable in a batch file or at the command prompt, precede and follow its name with a percent sign (%). When the batch program executes, the value of the environment variable replaces its name in the batch program. *For more information, see "Using Environment Variables," page 185.*

Table 37-2. Useful Environment Variables

Environment Variable	Value
AppData	Location of the Application Data folder for the current user (for example, C:\Documents And Settings\CarlS\Application Data).
CommonProgramFiles	Location of the Common Files folder (typically C:\Program Files\Common Files).
ComSpec	Executable file for the command processor (typically C:\Winnt\System32\Cmd.exe).
HomeDrive	Drive letter that's mapped to the home folder for a user profile. By default, it's the same as the letter of the system volume (typically C:).
HomePath	Folder for a user profile on the home drive (typically \). Together, HomeDrive and HomePath specify the default folder for a user profile.
OS	Operating system on the user's workstation (Windows_NT on a system running Windows 2000).

(continued)

Table 37-2. Useful Environment Variables *(continued)*

Environment Variable	Value
Path	Application search path. When you type the name of an executable at a command prompt, Windows looks in each folder in the search path if the executable file is not in the current folder.
PathExt	Extensions for executable files (typically .com, .exe, .bat, and .cmd).
ProgramFiles	Location of the Program Files folder (typically C:\Program Files).
Prompt	Codes to specify a command prompt (typically PG, which displays the current folder followed by a greater-than symbol).
SystemDrive	Drive on which the system folder resides (typically C:).
SystemRoot	System folder; the folder that contains the Windows 2000 operating-system files (typically C:\Winnt).
Temp	Folder for storing temporary files (typically C:\Temp).
Tmp	Folder for storing temporary files (typically C:\Temp).
UserDomain	Domain the user is logged into (for example, SWDOCS).
UserName	User's logon name (for example, CarlS).
UserProfile	Location of the current user's profile (for example, C:\Documents And Settings\CarlS).
Windir	Same as SystemRoot; included for compatibility with earlier versions of Windows.

When the database files have been copied, another Net command restarts the Removable Storage service:

```
net start "removable storage" > nul
```

Cleaning Out the Recent Documents List

This batch program, called CleanRecent.bat, removes some of the files from the recently used documents list that you see if you select Documents from the Start menu. By removing document types that you don't want on this list, it allows room for more of the documents that you do want to see.

Note CleanRecent.bat is effective only if you have cleared the option to hide file name extensions in Folder Options | View. If extensions don't appear on the Recent menu, this program can't identify the files to be deleted.

```
@echo off
rem Cleans unwanted file types from the Recent folder
title Clean Recent
echo Cleaning Recent folder...

for %%t in (wav log ini) do del "%userprofile%\recent\*.%%t.lnk"

echo.
echo Done cleaning Recent folder.
title Command Prompt
```

This batch program uses the For...In...Do command to repeatedly execute the Del command. The document-type file name extensions that you want to remove from the list are enclosed in the parentheses. The For command executes the Del command once for each entry in this list. The variable %%T contains the current extension and is substituted in the Del command. This is effectively the same as typing three Del commands.

Note that the file names have an .lnk extension added. This is because the Recent folder contains shortcuts, which have the extension .lnk, rather than the actual recently used files.

Alphabetizing Your Favorites Menu and Your Start Menu

This batch program is somewhat more complex than the ones we have looked at so far. It uses more advanced techniques to control program flow.

Alphabetize.bat alphabetizes your Favorites menu and the Programs branch of your Start menu. (You can have it act on your Favorites menu, your Start menu, or both.) The menus become unsorted as you add new items—which are appended to the bottom of the menu—or manually reorder them by dragging menu items. Windows 2000 includes a Sort By Name command on the shortcut menu that appears if you right-click one of these menus. But Alphabetize.bat offers something more: if you decide you like the previous order better, Alphabetize.bat can restore the previous order—giving it an "undo" capability.

The order information for the Start and Favorites menus is kept in the registry. To alphabetize, this batch program exports the current settings to a file and then simply deletes the appropriate keys from the registry. Without an order specified in the registry, Windows alphabetizes the lists. As you add or move menu items, Windows re-creates the order information in the registry.

This batch program relies on the availability of Reg.exe, a command-line utility for viewing and modifying the registry. Reg.exe is one of the support tools included on the Windows 2000 Professional CD. To install all the support tools, run \Support \Tools\Setup.exe from the CD. If you want to install only Reg.exe, you can extract it from \Support\Tools\Support.cab and copy it to a folder that's in your application search path.

In the Alphabetize.bat listing that follows, we've included line numbers for reference. Note that you can't use line numbers in an actual batch file.

```
 1  @echo off
 2  rem Alphabetizes Favorites and/or Start menu
 3  setlocal
 4  if not exist "%appdata%\expert companion\" md "%appdata%\Expert
       Companion\"
 5
 6  if "%1" == "" goto usage
 7  if "%1" == "/?" goto usage
 8  if /i %1 == help goto usage
 9  set type=%1
10  set action=%2
11  if "%2" == "" set action=sort
12
13  set startmenu=false
14  set favorites=false
15  goto %type%
16  :STARTMENU
17  set startmenu=true
18  goto %action%
19  :FAVORITES
20  set favorites=true
21  goto %action%
22  :BOTH
23  set startmenu=true
24  set favorites=true
25  goto %action%
26
27  :SORT
28  :SORTFAVORITES
29  if not %favorites% == true goto sortstartmenu
30  reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\
    MenuOrder\Favorites" "%AppData%\Expert Companion\Favorites.reg" > nul
31  reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\
       Explorer\MenuOrder\Favorites" /f > nul
32  if %errorlevel% equ 0 echo Favorites alphabetized.
33
34  :SORTSTARTMENU
35  if not %startmenu% == true goto :eof
```

```
36 reg export "HKCU\Software\Microsoft\Windows\CurrentVersion
     \Explorer\MenuOrder\Start Menu" "%AppData%\Expert Companion\Start
     Menu.reg" > nul
37 reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\
     Explorer\MenuOrder\Start Menu" /f > nul
38 if %errorlevel% equ 0 echo Start Menu alphabetized.
39 goto :eof
40
41 :UNDO
42 :UNDOFAVORITES
43 if not %favorites% == true goto undostartmenu
44 if not exist "%appdata%\expert companion\favorites.reg" goto noundofile
45 reg import "%appdata%\expert companion\favorites.reg" > nul
46 echo Favorites order restored.
47
48 :UNDOSTARTMENU
49 if not %startmenu% == true goto :eof
50 if not exist "%appdata%\expert companion\start menu.reg"
     goto noundofile
51 reg import "%appdata%\expert companion\start menu.reg" > nul
52 echo Start menu order restored.
53 goto :eof
54
55 :NOUNDOFILE
56 echo No file exists to restore.
57 goto :eof
58
59 :USAGE
60 echo.
61 echo Usage:
62 echo    Alphabetize StartMenu^|Favorites^|Both [Undo]
63 echo.
64 echo Example:
65 echo    Alphabetize Favorites
66 echo.
67 echo    Add Undo to restore previous settings.
```

Lines 1 through 3 take care of some basic setup functions. They identify what this batch program does and turn echoing off. The Setlocal command specifies that environment variables created or changed by this batch program should be "local" to this batch program and should not affect other programs. *For more information, see "Using Local Environment Variables," page 625.*

Line 4 creates a folder under the Application Data folder called Expert Companion. Because the Md (make directory) command displays an error if the folder already exists, we use If Not Exist so that the Md command is executed only if the folder does not exist.

The second section of the batch program, lines 6 through 11, checks for command-line parameters. The %1 that appears in several of these lines represents the first argument on the command line. %2 represents the second, and so on up to %9. If you type the command *alphabetize a*, for example, the command interpreter sees this as the first line in this section of the batch program:

```
if "a"=="" goto usage
```

The test for equality would not be True, so the Goto statement would not be executed. But if you type *alphabetize* (without any arguments), the command interpreter would see

```
if ""=="" goto usage
```

and the Goto statement would be executed.

Notice that %1 is surrounded by quotation marks. This isn't a requirement. We could just as easily have written *%1$==$*. All we're doing is making sure that the command interpreter always sees something on both sides of the equal signs. Without a character there, it sees the line as

```
if == goto usage
```

The result would be a syntax error, causing the batch program to terminate. The quotation marks are a readable way to be sure neither side is ever empty.

The first line of this section, therefore, is for the case when no command-line parameters are used, and it sends the command processor to the Usage label (line 59), where the program displays instructions for using Alphabetize.

Lines 7 and 8 do the same thing: they answer calls for help. Because the comparison in an If statement requires an exact match, in line 8 we used the /I switch, which causes the If statement to ignore case. This switch is available only if command extensions are enabled. The /I switch overcomes a major limitation of earlier versions of MS-DOS and Windows, in which you'd need to set up several If statements to test for capitalization variants of the word *help*. For example, you might test for *help*, *HELP*, and *Help*—and you still wouldn't catch every possible form.

If the command line includes parameters that are not requests for help, lines 9 through 11 come into play. The Set commands assign the command-line parameters to environment variables that we can use later in the batch program. If the second command-line parameter is blank ("%2"==""), the action is assumed to be Sort and is set to that value.

Replaceable Parameters

Besides %1 through %9, you should be aware of two other useful replaceable parameters: %* and %0.

%* represents *all* the command-line arguments. One useful place for this parameter is in a For...In...Do statement. For example, you could enhance CleanRecent.bat (the batch program described in the preceding section) by changing its For statement to read

```
for %%t in (%*) do del "%userprofile%"\recent\*.%%t.lnk
```

You would then type the extensions you want to delete (separated by spaces) on the command line. You could type any number of extensions.

%0 represents the command name (in other words, the name of the batch file).

In lines 13 through 25, we set a group of environment variables that are used to tell the remainder of the batch program what to do.

Lines 13 and 14 set the environment variables StartMenu and Favorites to their default value of False. The Goto %Type% command (line 15) sends processing to the label that matches the Type variable set earlier. Because labels are not case sensitive, it doesn't matter if the user types *both, Both,* or some other variant. The rest of this section sets the StartMenu and Favorites variables to True if they are to be processed. They remain set to False if they are not to be processed. The Goto %Action% commands (lines 18, 21, and 25) send processing to the proper section of the batch program: to the Sort label (line 27) or the Undo label (line 41).

Now we are ready to start the actual work. Lines 27 through 39 sort the menus, and lines 41 through 57 restore the old menu arrangements.

The Sort section starts by checking that the value of the variable Favorites is True, in line 29. If it is not, the processing of Favorites is skipped. Next, the Reg Export command (line 30) creates a file that contains the current Favorites order. The environment variable AppData is used to locate the Expert Companion folder that was created at the beginning of the batch program. After the backup file is made, the Reg Delete command (line 31) removes all the Favorites order information from the registry. The /F switch does this without confirmation, and > Nul eliminates the completion message.

Reg sets the error level value to 0 upon successful completion or to 1 if an error occurs. The If statement in line 32 echoes a message of success if the error level is 0. This form of the If statement works only with Windows 2000; if you want to create a program for use on computers running earlier versions of Windows, you could instead use the more traditional form:

```
if not errorlevel 1 echo Operation successful.
```

The SortStartMenu section (lines 34 through 39) performs the same process on the Start menu. Lines 35 and 39 demonstrate another new feature of Windows 2000: the Goto :EOF command. This special label, which must include the colon, causes the command processor to jump to the end of the batch program—in other words, to end execution. With MS-DOS and earlier versions of Windows, you must create a label at the end of the file and use it as the target of the Goto command to achieve the same result.

The Undo section of the batch program, lines 41 through 57, restores the original menu order. Again, the first check is to be sure that the Favorites are supposed to be processed (line 43). Then the If Not Exist command in line 44 checks to be sure that a backup file exists. If the file doesn't exist, the NoUndoFile section (lines 55 through 57) displays a message to that effect.

The Reg Import command (line 45) does the actual work. It imports the contents of the backup file to the registry, restoring the previous order.

The UndoStartMenu section (lines 48 through 53) performs the same process on the Start menu.

It's a good idea to make batch programs self-documenting. The Usage section, lines 59 through 67, does just that. This section consists of a series of Echo commands that display the correct usage of this batch program. Note the use of the Echo command followed by a dot, which displays a blank line for a nicer display. (If you use Echo alone, it reports the state of the echoing function—on or off.)

The interesting thing about line 62 is the use of the escape symbol (^) to indicate that the pipe symbol (|) should be treated as a character and not interpreted as a pipe symbol. Without the escape symbol, the command interpreter would try to pipe the Echo command and the first few words to whatever follows the pipe symbol, which would cause a syntax error. You must use the escape symbol any time you want to echo a pipe symbol (|), a greater-than sign (>), a less-than sign (<), an ampersand (&), or a caret (^).

Although this batch program illustrates some advanced techniques of batch processing, it also demonstrates some limitations.

If you misspell the first parameter, which should be Favorites, StartMenu, or Both, the batch program will fail. For example, if you type *alphabetize favorits*, the batch program displays this message:

```
The system cannot find the batch label specified - favorits
```

There is no way to trap for this error or to change the message to something more meaningful.

Likewise, if you happen to type one of the options for the first parameter as the second parameter, the batch program goes into an endless loop. For example, if you type *alphabetize favorites both*, the batch program appears to hang. It is actually very busy jumping back and forth between various labels, but the only way to stop it is to press Ctrl+Break.

These limitations are typical of complex batch programs. Batch programs provide a quick way to do simple tasks, but other tools (such as Windows Script Host) are better for more complex tasks.

A final word about debugging batch programs: You usually have to do some experimenting to get your batch programs to work exactly the way you want. You can write the batch program in one Command Prompt window and test it in another. To see exactly what the command interpreter sees, change the first line to

```
rem @echo off
```

This "comments out" the Echo Off command so that each line echoes to the screen with parameters and environment variables filled in before it is executed. In our sample file, you'd probably also want to temporarily remove the redirection to Nul from each command so that you could see all the output.

Using Other Batch Program Tricks

We wrap up our discussion of batch programs with a handful of other techniques you can use in your batch programs.

A Refreshing Pause

The Pause command always puts up the same boring message: "Press any key to continue." You might prefer to instruct your users to type, strike, hit, depress, or otherwise activate a key. You can use the Echo command to display your own message and then get rid of the unwanted Pause message by redirecting it to the Nul device. You might even wax poetic:

```
echo  If the going gets too tough,
echo     Hit Control+C to stop this stuff.
echo  But if you'd like to see the rest of me,
echo     Continue on! Press any key.
pause > NUL
```

Using Pushd and Popd to Change to a Different Folder

A common sequence of events in a batch program is move to a specific folder, do some work there, and then return to the original folder. The problem is that your batch program can be run from any folder. If you don't know where you are, you can't go back. Pushd and Popd to the rescue.

The Pushd command saves the current folder and sets a new one. The Popd command restores the original. Normally, you need these commands only in batch programs, but an example from the command line shows how they work:

```
C:\bat>pushd \data
C:\data>pushd sales
C:\data\sales>popd
C:\data>popd
C:\bat>
```

You can probably figure out intuitively what's going on here, but if you're not a programmer, you might wonder what "push" and "pop" in the command names mean. *Push* means to put something onto a *stack*. It might be a stack of plates or a stack of computers, but in this case we mean a stack of folder names. *Pop* means to take the top item—the only one you can get at—off the stack.

In the example, we first push the Bat folder onto the stack. If we popped now, we'd get the Bat folder back. Instead we push another folder, Data. We have to pop it off the stack before we can get at the Bat folder. Of course, in a batch program we'd be doing some work in each folder before we pushed another one or popped to restore the old one.

Note

The online help for Pushd says that the *path* parameter is optional, but don't believe it. If you don't supply a folder path to the Pushd command, the Popd command won't restore it.

Using Local Environment Variables

In many cases, a batch program needs to change a standard environment variable, such as Path. But changing this critical variable without restoring it when you are finished could cause problems for other programs. If you're writing the batch program for your own use, it's not difficult to restore modified variables, although it gets tiresome after a while. But if you're writing a batch program to be run by others, you probably won't even know what settings to restore.

Windows 2000 addresses this problem with the Setlocal and Endlocal commands. Setlocal makes any further settings or changes to environment variables local to the current batch program. Endlocal returns handling of environment variables back to normal mode—any further changes remain after the batch program terminates.

You might want to use a batch program to modify environment variables for either of two reasons. First, this might be the primary purpose of the batch program, as it is in the following short batch program (call it Addpath.bat), which adds a folder to the end of the search path:

```
@echo off
set Path=%Path%;%1
```

But more often, you will use environment variables to save values or change program behavior within the batch program. The simple rule is to use Setlocal at the start of the batch program and Endlocal at the end. Even if your batch program sets only a temporary environment variable, you want to be sure that the variable is cleared on termination. Actually, the Endlocal command is usually unnecessary. If you use Setlocal, the system automatically performs the equivalent of an Endlocal statement when the batch program terminates. However, using Setlocal and Endlocal in pairs makes your batch programs more consistent and easier to understand. For example:

```
Setlocal

rem Set new path
set Path=D:\BIN
rem Do something with the new path
.
.
.
endlocal
rem Path goes back to its original value after EndLocal
```

Chapter 38

Using Windows Script Host

In This Chapter

Finding Scripting Resources 628
Wscript vs. Cscript 628
Choosing a Scripting Language 629
Using the Script File Format 631
Debugging Scripts 632
Introducing Objects 637
Example Scripts 640

Microsoft Windows Script Host (WSH) provides a way to perform more sophisticated tasks than the simple jobs that batch programs are able to handle. You can control virtually any component of Microsoft Windows and of many Windows-based programs with Windows Script Host scripts.

WSH scripts work much the same way batch programs do. You can type a script name at a command prompt or simply double-click the file name in Windows Explorer. Batch programs rely on Cmd.exe, a command interpreter that executes programs written in the batch language described in Chapter 37, "Using Batch Programs." Windows Script Host has two nearly equivalent programs, Wscript.exe and Cscript.exe, that, with the help of a language interpreter dynamic-link library such as Vbscript.dll, execute scripts written in VBScript or other scripting languages.

The *content* of WSH script files, however, is much different from that of batch programs. With WSH, the files can be written in several different languages, including VBScript (a form of Microsoft Visual Basic) and JScript (a form of JavaScript). Windows Script Host is, in fact, just what its name says: a host for script languages. VBScript and JScript interpreters come with Windows 2000; interpreters for Perl and other languages are available elsewhere.

Because WSH scripts can access ActiveX controls, they provide great flexibility. Several objects are provided with Windows Script Host that allow you basic control of Windows and your computer. By using ActiveX, you can control many of the programs on your computer. For example, you can create a WSH script to display a chart in Microsoft Excel.

As an introduction, here's the WSH "Hello World" script. It's as short as it can get in any programming language:

```
WScript.Echo "Hello World"
```

Using a plain-text editor such as Notepad, put this line in a file with a .vbs extension (Hello.vbs, for example), and you have a working WSH script. Simply double-click the file name in Windows Explorer to run your script.

Finding Scripting Resources

You won't learn how to write a script in this chapter. You must know a scripting language, or else use these resources to learn one. (If you know Visual Basic, you already know a scripting language.) We hope to show you some of what you can do with Windows Script Host and help you find the widely scattered information you need to use it effectively.

One of the biggest hurdles to learning to use WSH is finding the information you need. The scripting language, VBScript or JScript, is separate from the objects you use in your scripts, and each piece has separate documentation. You must find the reference guide for both the scripting language you choose and the objects you use. Throughout this chapter, we tell you where to find the relevant documentation, most of which is available on Microsoft's Web site. Microsoft has an entire subsite for scripting at *msdn.microsoft.com/scripting*. Browsing this site can be confusing, however. The site describes the use of the scripting languages and their associated objects, but it also provides information for software developers who want to add scripting capabilities to their programs—which is another topic altogether.

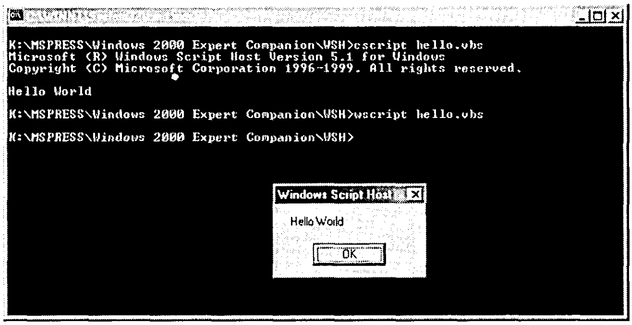
Wscript vs. Cscript

Windows 2000 actually includes two programs that run WSH scripts. Cscript.exe is the command-line version, and Wscript.exe is the GUI version. Although this sounds like a big distinction, for most scripts the differences are pretty small. Try running Hello.vbs with each program to see the difference. At the command prompt, type these two lines:

```
cscript hello.vbs
wscript hello.vbs
```

Figure 38-1 shows the results. Cscript displays the words "Hello World" in a Command Prompt window. Wscript displays a small dialog box with the message "Hello

World" and an OK button. With Cscript, you use command-line parameters to change the properties of a script file. Wscript, in contrast, provides a dialog box to set the properties. Type *wscript* at a command prompt to display the properties dialog box.



```
K:\MSPRESS\Windows 2000 Expert Companion\WSH>cscript hello.vbs
Microsoft (R) Windows Script Host Version 5.1 for Windows
Copyright (C) Microsoft Corporation 1996-1999. All rights reserved.

Hello World

K:\MSPRESS\Windows 2000 Expert Companion\WSH>wscript hello.vbs

K:\MSPRESS\Windows 2000 Expert Companion\WSH>
```

Figure 38-1
Cscript.exe, the console version, displays its result in a Command Prompt window, whereas Wscript.exe pops up a dialog box.

You can change the association so that Cscript is the default by typing the following at a command prompt:

```
cscript //h:cscript
```

Note that Cscript and Wscript command-line options use two slashes. This differentiates them from command-line options for the script being executed, which use a single slash. To see all the command-line options, type *cscript //?* (or *wscript //?*) at a command prompt.

Choosing a Scripting Language

Windows Script Host doesn't care whether you use VBScript, JScript, or some other scripting language. All the objects are available to any language, and in most situations, you can choose to use the language with which you are most comfortable. In this book, we use mostly VBScript but also a little JScript. As you will see later, you can actually mix languages in the same program.

Here is a short script, called Folders.vbs, that shows some of the elements of a script written in VBScript:

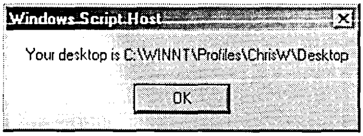
```
Option Explicit

Dim objWSShell
Dim strMsg
Dim intCtr

Set objWSShell = WScript.CreateObject("WScript.Shell")
WScript.Echo "Your desktop is " & objWSShell.SpecialFolders("Desktop") _
    & vbNewLine
```

```
strMsg = "All your special folders are:" & vbNewLine
For intCtr = 0 To objWSShell.SpecialFolders.Count - 1
  strMsg = strMsg & objWSShell.SpecialFolders.Item(intCtr) & vbNewLine
Next
WScript.Echo strMsg
```

Note You can find all the example scripts from this chapter on the companion CD.

The script starts with an Option Explicit statement, which tells the VBScript interpreter to require you to use a Dim statement for every variable in the script. This helps to prevent errors from misspelled variable names and is accepted as good programming practice.

The Set statement creates a WScript Shell object, which is used to access the special folders. One of the properties of the Shell object is the SpecialFolders object. The SpecialFolders object lets you retrieve the path and file name of any of the special folders on your system. For example, this script retrieves the Desktop folder, as shown in Figure 38-2.

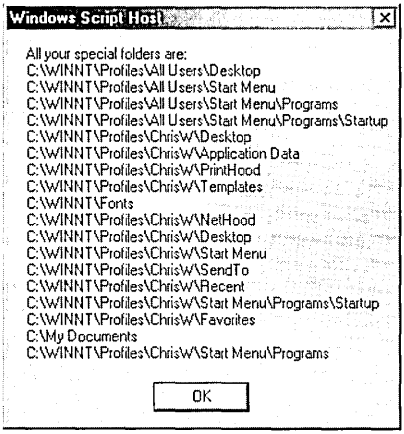


Your desktop is C:\WINNT\Profiles\ChrisW\Desktop

Figure 38-2
Folders.vbs initially displays the location of your Desktop folder.

The next section of the script, the For...Next loop, displays all the special folders. This section demonstrates a technique that makes scripts work well with both Wscript and Cscript. Instead of putting a WScript.Echo statement inside the loop, we add each result to the strMsg string and then display this string after the loop is finished. When run with Cscript, the results are the same. However, when run with Wscript, accumulating the results into a string and using one WScript.Echo statement means that one dialog box is displayed for the entire loop, rather than one dialog box for each special folder. See Figure 38-3.

VBScript is a major subset of Visual Basic. If you know Visual Basic, there is little that you can't do in VBScript. One of the biggest differences is that VBScript has only Variant variables. You simply use Dim and the variable name; you can't add a variable type because they are all the same. You can find documentation of VBScript at *msdn.microsoft.com/scripting/vbscript/techinfo/vbsdocs.htm.*



```
All your special folders are:
C:\WINNT\Profiles\All Users\Desktop
C:\WINNT\Profiles\All Users\Start Menu
C:\WINNT\Profiles\All Users\Start Menu\Programs
C:\WINNT\Profiles\All Users\Start Menu\Programs\Startup
C:\WINNT\Profiles\ChrisW\Desktop
C:\WINNT\Profiles\ChrisW\Application Data
C:\WINNT\Profiles\ChrisW\PrintHood
C:\WINNT\Profiles\ChrisW\Templates
C:\WINNT\Fonts
C:\WINNT\Profiles\ChrisW\NetHood
C:\WINNT\Profiles\ChrisW\Desktop
C:\WINNT\Profiles\ChrisW\Start Menu
C:\WINNT\Profiles\ChrisW\SendTo
C:\WINNT\Profiles\ChrisW\Recent
C:\WINNT\Profiles\ChrisW\Start Menu\Programs\Startup
C:\WINNT\Profiles\ChrisW\Favorites
C:\My Documents
C:\WINNT\Profiles\ChrisW\Start Menu\Programs
```

Figure 38-3
The For...Next loop builds a string that is displayed in a single dialog box.

Using the Script File Format

For WSH scripts, you can use VBScript in files with the .vbs extension and JScript in files with the .js extension. Windows Script Host version 2, which is new in Windows 2000, adds another level of tags that provide more flexibility and power. In fact, WSH 2 files, which use the .wsf extension, are actually Extensible Markup Language (XML) files that use tags, as shown in the following example (Hello.wsf):

```
<?XML version="1.0"?>
<package>
<job id="job1">
<?job debug="true"?>
<script language="VBScript" src="MyScript.vbs"/>
<script language="VBScript">
<![CDATA[
   WScript.Echo "Hello World"
]]>
</script>
</job>
</package>
```

Table 38-1 describes the function of each of these tags, plus a few others.

Table 38-1. Useful XML Tags

Tag	Description
<?XML version="1.0"?>	Marks your code as XML 1.0–compliant. This tag is optional now but might be required by future XML tools.
<package> </package>	Encloses multiple jobs in a single file. The <package> tag is optional if you have only one pair of <job> tags.
<job id="job1"> </job>	Identifies jobs in a file. When you have multiple jobs in a file, you can run any one with this syntax: `Cscript //Job:MyFirstJob MyScripts.wsf`
<?job debug="true"?>	Allows use of the script debugger. You can add *error="true"* to this tag to allow error messages for syntax or run-time errors.
<script language= "VBScript" src = "MyScript.vbs"/>	Includes, or merges, another file into the current one when the script runs. This tag allows you to easily reuse code.
<script language= "VBScript"> </script>	Encloses a script. In a single job, you might have several scripts—even in different scripting languages.
<![CDATA[ ]]>	Indicates that the parser should treat your code as character data and not interpret the characters in it. Use this tag if you use the XML tag.
<object>	Defines objects that can be referenced by the script.
<reference>	Provides a reference to an external type library, allowing you to use defined constants from that type library.
<resource>	Isolates text or numeric data that should not be hard-coded in a script.

Debugging Scripts

To debug scripts, you first need to install Microsoft Script Debugger. Go to Start | Settings | Control Panel | Add/Remove Programs | Add/Remove Windows Components. In the Windows Components Wizard that appears, select Script Debugger in the Components list.

In addition, if you want to debug .wsf files, you must do the following:

- In the registry, change the JITDebug value in the HKCU\Software\Microsoft \Windows Script\Settings key to 1. Changing this registry entry lets you debug .wsf files in addition to .vbs and .js files. For your convenience, the companion CD contains a file called WSH_Debug.reg that makes this change for you.

- Add the line *<?job debug="true"?>* to your script file. (It goes right below the <job> tag.) Without this line, the debugger will not open.

Note After you have installed the debugger, the messages you see when you encounter a script error while you browse the Internet are different. At the bottom, the message asks, "Do you want to debug the current page?" If you click Yes, the debugger appears with the page loaded. Since you are probably looking at someone else's site, however, you probably want to click No!

You can find the documentation for Script Debugger at *msdn.microsoft.com/scripting/debugger*. Keep in mind that you can use this same debugger to debug both client and server scripts for Web pages; most of the documentation is focused on those activities. (In fact, Windows Script Host might not be mentioned in the debugger documentation at all.)

You start the debugger using command-line switches with the Cscript or Wscript commands. The //X switch starts the debugger, loads the script into the debugger, and stops at the first line of the script. The //D switch starts the debugger only when an error is encountered. It also loads the program in the debugger and stops at the line where it encountered the error.

Here's an example of debugging a very simple script, which we call Debug.vbs:

```
main()

Function main()
x = 99
WScript.echo "Hello once"
WScript.echox "Error 1 here"

End Function
```

After creating this script, at the command prompt type

```
wscript //d debug.vbs
```

The words "Hello once" should appear in a small dialog box. When you click OK, Script Debugger appears, with the error highlighted, as shown in Figure 38-4.

The debugger helps you find your error, but you can't fix errors here. As you notice at the top of the document window, the file is identified as read-only. You can open another instance of the file in the debugger and edit that file. The debugger provides an editor that is on a par with Notepad.

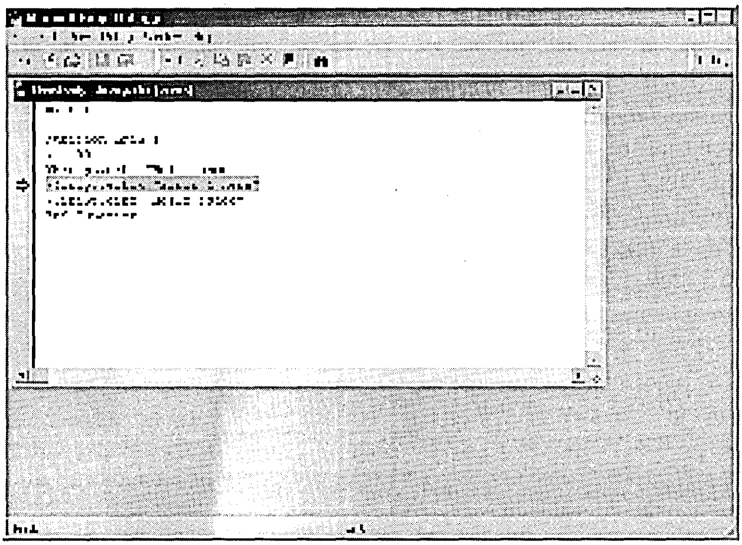
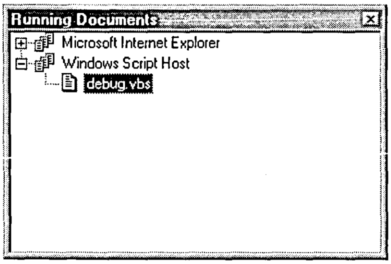


Figure 38-4
When you run a script with the //D switch, Script Debugger appears when an error is encountered and highlights the error.

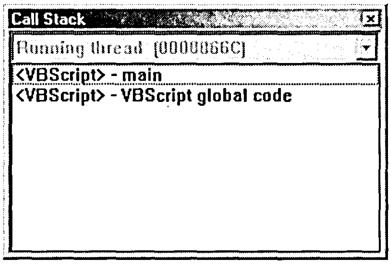
Using Other Debugger Windows

At this point, the debugger can provide some additional information, but you are effectively done with running the script. Three additional windows, all available both from the View menu and from the right side of the toolbar, allow you to see more information about your script:

- The Running Documents window shows you scripts that are currently running. Besides Windows Script Host, you are likely to see Microsoft Internet Explorer here. If you right-click a script in this window, one command appears on the menu: Break At Next Statement. This command provides a way to "invite" a script into the debugger.



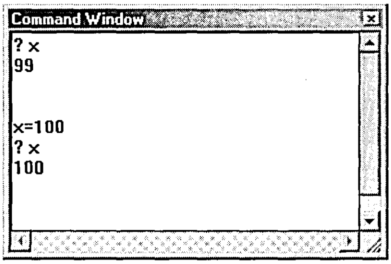
- The Call Stack window displays the call history to the current point in the current script. This can help you figure out just how you got to where you are.



Call Stack

```
Running thread [0000066C]
<VBScript> - main
<VBScript> - VBScript global code
```

- The Command window lets you view and manipulate variables in your script. In the following example, the first line "printed" the value of *x*. (A question mark is shorthand for the Visual Basic Print command.) Then the value of *x* was changed to 100 and displayed again.



Command Window

```
? x
99


x=100
? x
100
```

When you work in the Command window, you must use the same language as the currently running script. If you are running a VBScript file, for example, type a question mark followed by a space and the variable name to display a variable's value. If you are running a JScript file, simply enter the name of the variable. You can also view and change an object's properties in the Command window.

Stepping Through Scripts

When you start the debugger using the //X command-line switch, the debugger opens with the first line of the script highlighted. You can move through the script and see how the program flow works. All the debugging information is available so that you can check the value of variables and object properties and see how they are changed by the operation of the script.

The Debug toolbar—one of three toolbars in Script Debugger—has the tools you use to step through a script. Table 38-2 describes the buttons on the Debug toolbar.

Table 38-2. Script Debugger's Debug Toolbar

Button	Name	Description
	Run	Executes the script until it hits a breakpoint, an error, or comes to the end of the script
	Stop Debugging	Runs the script outside the debugger
	Break At Next Statement	Activates an open server script in the debugger; not useful for WSH files
	Step Into functions	Advances the script by one statement; steps into and subroutines
	Step Over	Advances the script by one statement; executes but does not display functions and subroutines
	Step Out	Advances the script until it exits the current function or subroutine
	Toggle Breakpoint	Inserts or removes a breakpoint at the line containing the insertion point
	Clear All Breakpoints	Clears all breakpoints
	Running Documents	Displays the Running Documents window
	Call Stack	Displays the Call Stack window
	Command Window	Displays the Command window

The process is to step through the script, line by line, until you find an error. When you determine that a specific part of the script works, you can set a breakpoint at the beginning of the untested part and then click Run to get to that point quickly. When you believe that your functions and subroutines are working correctly, you can speed up debugging by clicking Step Over to execute them as one step, instead of using the Step Into button.

Introducing Objects

You can't do much with WSH without using objects. An object is a variable comprising both routines and data that is treated as a discrete entity. Some objects are built into the scripting language; others are provided by the operating system. One of the previous script examples used the WScript.Shell object to gain access to the Windows shell.

Table 38-3 describes the objects that are built into VBScript. They are documented, along with the VBScript language, at *msdn.microsoft.com/scripting/vbscript/techinfo/vbsdocs.htm.*

Table 38-3. VBScript Objects

Object	Description
Class object	Provides access to the events of a created class
Dictionary object	Stores data in key/item pairs
Drive object	Provides access to the properties of a disk drive or network share
Drives collection	Collection of all available Drive objects
Err object	Provides information about run-time errors
File object	Provides access to all the properties of a file
Files collection	Collection of all File objects within a folder
FileSystemObject	Provides access to your computer's file system object
Folder object	Provides access to all the properties of a folder
Folders collection	Collection of all Folder objects contained within a Folder object
Match object	Provides access to the read-only properties of a regular expression match
Matches collection	Collection of regular expression Match objects
RegExp object	Provides simple regular expression support
TextStream object	Facilitates sequential access to a file

Windows Script Host provides the objects shown in Table 38-4. They are documented, along with Windows Script Host, at *msdn.microsoft.com/scripting/windowshost/docs/reference/default.htm.*

Table 38-4. Windows Script Host Objects

Object	Description
Wscript object	Exposes properties that specify the path of the running scripting host (Wscript.exe or Cscript.exe), its arguments, and the working mode (interactive or batch); also provides methods to create and read objects
WshArguments object	Returns a pointer to the collection of command-line parameters
WshEnvironment object	Retrieves system environment variables
WshNetwork object	Maps the network, making it easy to connect and disconnect remote drives and printers
WshShell object	Starts new processes, creates shortcuts, and provides the Environment collection to handle environment variables such as SystemRoot, Path, and Prompt
WshShortcut object	Creates an object reference to a shortcut
WshSpecialFolders object	Accesses the Windows shell folders such as the Desktop folder, the Start Menu folder, and the My Documents folder
WshUrlShortcut object	Creates an object reference to a URL shortcut

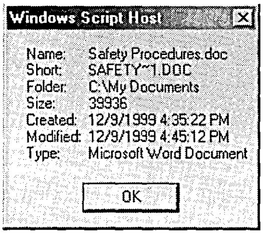
Windows Management Instrumentation (WMI) provides many more objects that you can use to manage your Windows environment. The WMI scripting interface is documented at *msdn.microsoft.com/library/psdk/wmisdk/scintro_67e1.htm*. Click the "show toc" button at the top to add the table of contents panel to this page.

Using the File System Object

One of the objects you will probably use often is FileSystemObject. This object gives you access to the files and folders on your computer. The following example, called FileProp.vbs, shows how to use this object; Figure 38-5 shows the result.

```
' Displays properties of file on command line

   Option Explicit
   Dim strArg, objFileSys, objFile, strMsg

   If WScript.Arguments.Count < 1 Then
      WScript.Echo "Usage: FileProp <filename>" & vbNewLine & _
                   "Or drag and drop a file on this file."
      WScript.Quit (1)
   End If
```

```
Set objFileSys = CreateObject("Scripting.FileSystemObject")

strArg = objFileSys.GetAbsolutePathName(WScript.Arguments(0))

Set objFile = objFileSys.GetFile(strArg)

strMsg = "Name:    " & vbTab & objFile.Name & vbNewLine
strMsg = strMsg & "Short:   " & vbTab
strMsg = strMsg & objFile.ShortName & vbNewLine
strMsg = strMsg & "Folder:  " & vbTab
strMsg = strMsg & objFile.ParentFolder & vbNewLine
strMsg = strMsg & "Size:    " & vbTab
strMsg = strMsg & objFile.Size & vbNewLine
strMsg = strMsg & "Created: " & vbTab
strMsg = strMsg & objFile.DateCreated & vbNewLine
strMsg = strMsg & "Modified:" & vbTab
strMsg = strMsg & objFile.DateLastModified & vbNewLine
strMsg = strMsg & "Type:    " & vbTab
strMsg = strMsg & objFile.Type & vbNewLine
WScript.Echo strMsg

Set objFile = Nothing
Set objFileSys = Nothing
```



```
Name:     Safety Procedures.doc
Short:    SAFETY~1.DOC
Folder:   C:\My Documents
Size:     39936
Created:  12/9/1999 4:35:22 PM
Modified: 12/9/1999 4:45:12 PM
Type:     Microsoft Word Document
```

Figure 38-5
The FileProp.vbs script quickly displays some file properties that aren't easily viewed in Windows Explorer.

This script first checks to see whether the command line contains any parameters. If none are found, it displays a usage message and quits. The script works with drag and drop because Windows adds the name of dropped files to the command line. If you drop more than one file on this script, it displays information about only the first one.

After the error checking is out of the way, the script creates a FileSystemObject object and then uses that object to get the full path name of the file. Using the full path name, it gets a File object.

The script then builds a string by concatenating various properties of the File object. When the entire string is built, the script displays it with the Echo method of the WScript object. You can also use the MsgBox function to display strings. It allows you to specify which buttons appear, to change the title from Windows Script Host to a message you specify, and to respond to the button a user clicks. Whereas the WScript.Echo method works differently in Cscript and Wscript, the MsgBox function works the same way in both: it always displays a dialog box. To see the difference, try replacing the WScript.Echo line in the previous script with the following line:

```
MsgBox strMsg, vbOKOnly, "File Properties"
```

Finally, the script releases the FileSystemObject object and the File object by setting the variables to the built-in value Nothing, which releases the resources used by the objects. It's not important to do this in a small script such as this one because it happens anyway when the script ends, but in more involved scripts, releasing the objects when you've finished with them can reduce the resources your script requires.

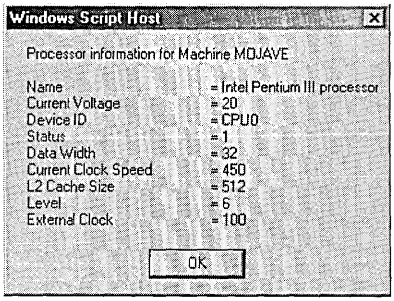
The FileSystemObject object is documented at *msdn.microsoft.com/scripting/vbscript/doc/vbsfsoTOC.htm.*

Example Scripts

In this section, we present two sample scripts that demonstrate some of the techniques you can use with Windows Script Host.

Displaying Processor Properties

The first script displays some hard-to-find information about your processor, as shown in Figure 38-6.



```
Processor information for Machine MOJAVE

Name                  = Intel Pentium III processor
Current Voltage       = 20
Device ID             = CPU0
Status                = 1
Data Width            = 32
Current Clock Speed   = 450
L2 Cache Size         = 512
Level                 = 6
External Clock        = 100
```

Figure 38-6
Processor.vbs uses WMI objects to display information about your computer's CPU.

```
'*********************************************************************
'*
'*  File:          Processor.vbs
'*
'*  Function:      Displays information about the local machine's
'*                 CPU, including name, speed, and other information.
'*
'*
'*********************************************************************

Option Explicit

GetProcProp()


'*********************************************************************
'*
'* Sub GetProcProp()
'*
'* Purpose: Gets CPU information for the local machine.
'*
'*
'* Output:  Results are displayed on screen (Cscript) or in a message
'*          box (Wscript).
'*
'*********************************************************************
Private Sub GetProcProp()

    On Error Resume Next

    Dim objService, objProcSet, objProc, objLocator, objWshNet
    Dim strWBEMClass, strServer, strNameSpace, strResults

    strWBEMClass = "Win32_Processor"
    strNameSpace = "root\cimv2"

    'Establish a connection with the server
    'Create Locator object to connect to object manager
    Set objLocator = CreateObject("WbemScripting.SWbemLocator")

    If blnErrorOccurred("occurred when creating a locator object.") _
       Then
    Exit Sub
End If

'Connect to the namespace
Set objService = objLocator.ConnectServer(, strNameSpace)
If blnErrorOccurred("occurred when connecting to server.") Then
    Exit Sub
End If

'Set the security level
objService.Security_.impersonationlevel = 3
If blnErrorOccurred("occurred when setting security.") Then
    Exit Sub
End If

'Get the processor information set
Set objProcSet = objService.InstancesOf(strWBEMClass)
    If blnErrorOccurred("Could not obtain " & _
               strWBEMClass & " instance.") Then
    Exit Sub
End If

If objProcSet.Count = 0 Then
    WScript.Echo "No processor information is available."
    Exit Sub
End If

'Get the server's name
Set objWshNet = CreateObject("WScript.Network")
strServer = objWshNet.ComputerName

strResults = "Processor information for Machine " & strServer
strResults = strResults & vbNewLine & vbNewLine

For Each objProc In objProcSet
    strResults = strResults & "Name" & vbTab & vbTab & vbTab _
         & "= " & objProc.Name & vbNewLine
    strResults = strResults & "Current Voltage" & vbTab & vbTab _
         & "= " & objProc.CurrentVoltage & vbNewLine
    strResults = strResults & "Device ID" & vbTab & vbTab _
         & "= " & objProc.DeviceID & vbNewLine
    strResults = strResults & "Status" & vbTab & vbTab & vbTab _
         & "= " & objProc.CpuStatus & vbNewLine
```

```
        strResults = strResults & "Data Width" & vbTab & vbTab _
             & "= " & objProc.DataWidth & vbNewLine
        strResults = strResults & "Current Clock Speed" & vbTab _
             & "= " & objProc.CurrentClockSpeed & vbNewLine
        strResults = strResults & "L2 Cache Size" & vbTab & vbTab _
             & "= " & objProc.L2CacheSize & vbNewLine
        strResults = strResults & "Level" & vbTab & vbTab & vbTab _
             & "= " & objProc.Level & vbNewLine
        strResults = strResults & "External Clock" & vbTab & vbTab _
             & "= " & objProc.ExtClock & vbNewLine
        WScript.Echo strResults
    Next


End Sub


'*********************************************************************
'*
'* Function blnErrorOccurred()
'*
'* Purpose: Checks for and reports errors. Displays the built-in error
'*          message plus a message saying where the error occurred.
'*
'* Input:   strIn       String saying where the error occurred.
'*
'* Output:  Displayed on screen (Cscript) or in message box (Wscript).
'*
'* Returns: False       No error occurred
'*          True        An error occurred
'*
'*
'*********************************************************************
Private Function blnErrorOccurred(ByVal strIn)
    Dim strMsg

    If Err.Number Then
        strMsg = "Error " & CStr(Err.Number) & " " & strIn
        If Err.Description <> "" Then
            strMsg = strMsg & vbNewLine & Err.Description
        End If
        WScript.Echo strMsg
        Err.Clear
        blnErrorOccurred = True
    Else
        blnErrorOccurred = False
    End If

End Function
```

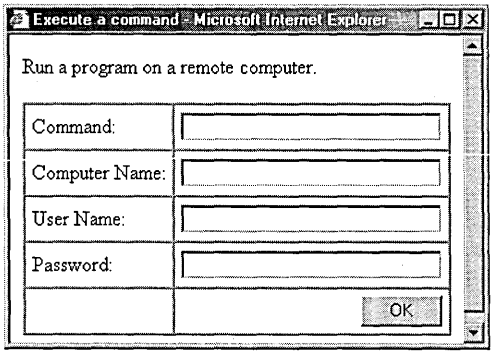
This script, named Processor.vbs, displays your processor's name, clock speed, L2 cache size, and other information. It gets this information from the Windows Management Instrumentation interface. The documentation for the WMI scripting interface is at *msdn.microsoft.com/library/psdk/wmisdk/scref_4u95.htm.* All of the GetProcProp function, down to the comment *Get the server's name,* uses the WMI interface to get the processor information.

When the processor information is retrieved from WMI, a WScript.Network object is created to get the computer's name. After that, the properties of the processor are concatenated to a string and the results are displayed. The For...Next loop adds the results for each processor in the set of processors reported by WMI. This allows the script to report the properties of more than one processor, if your computer has more than one. The For...Each construction is an easy way to step through a group of objects.

As each major step is taken in this script, the function blnErrorOccurred is called. This function checks the Err object, which contains error information, and reports any errors that occur. The blnErrorOccurred function returns True if an error has occurred or False if there is no error. The main subroutine, GetProcProp, simply exits if an error occurs.

Executing Commands on Remote Computers

The following script allows you to run a command on either a local computer or a remote computer. It uses Internet Explorer to provide a user interface for entering information, as shown in Figure 38-7. This example demonstrates how you can control any program that has a Component Object Model (COM) interface from a script.



Execute a command - Microsoft Internet Explorer

Run a program on a remote computer.

Figure 38-7
Internet Explorer provides the user interface for the Exec.wsf script.

With this script, you can run a command on your local computer by entering only the command. You can run a command on a remote computer by entering information in all four text boxes. The user name you enter must have permission to run commands on the remote computer, which usually requires administrative rights.

This script, called Exec.wsf, uses the Windows Script Host 2 script file format. It uses a <script> tag to include another script file at run time. It also uses two scripting languages, VBScript and JScript.

```
<?XML version="1.0"?>
<package>
<job id="js">
<?job debug="true" error="true"?>
<comment>
=============================================================================
Program: Exec.wsf

Executes a command on a remote computer.

=============================================================================
</comment>

<comment> FILE NAME </comment>
<resource id="strHTMLFile">exec.htm</resource>

<comment> MESSAGES </comment>
<resource id="errNoCommand">Please enter a command to execute.</resource>
<resource id="errMissingComputer">You must enter a computer name.</resource>
<resource id="errMissingName">You must enter a name.</resource>
<resource id="errMissingPassword">You must enter a password.</resource>
<resource id="errLocator">occurred when creating a locator object.</resource>
<resource id="errServer1">occurred when connecting to </resource>
<resource id="errServer2">.</resource>
<resource id="errSecurity">occurred when setting security.</resource>
<resource id="errWin32Process">occurred getting a Win32_Process class object.</resource>
<resource id="errCreateProcess1">occurred when creating process </resource>
<resource id="errCreateProcess2">.</resource>
<resource id="errNetworkObject">occurred when creating network object.</resource>

<resource id="msgError">Error </resource>
<resource id="msgSucess1">Succeeded in executing </resource>
<resource id="msgSucess2"> on </resource>
<resource id="msgSucess3">.</resource>
<resource id="msgFailure1">Failed to execute </resource>
```

```
<resource id="msgFailure2">.</resource>
<resource id="msgProcessID">Process ID = </resource>
<resource id="msgStatus">Status = </resource>

<comment> TITLE </comment>
<resource id="strWindowTitle">Execute a command</resource>

<comment> INCLUDE ERROR FUNCTION </comment>
<script language = "VBScript" src="ErrorMsg.vbs"/>

<script language="VBScript">
<![CDATA[

Option Explicit
'********************************************************************
'* Function ExecuteCommand()
'*
'* Purpose: Executes a command on local or remote computer.
'*
'* Input:   Accesses values in IE directly.
'*
'********************************************************************

Sub ExecuteCommand()
    On Error Resume Next

    Dim objService, objInstance, objLocator, objWshNet
    Dim strMsg, strNameSpace
    Dim strServer, strUserName, strCommand, strPassword
    Dim intProcessId, intStatus

    strNameSpace = "root\cimv2"
    strCommand = doc.all.txtCommand.Value
    strServer = UCase(doc.all.txtComputer.Value)
    strUserName = doc.all.txtUser.Value
    strPassword = doc.all.txtPassword.Value

    'Establish a connection with the server
    'Create Locator object to connect to object manager
    Set objLocator = CreateObject("WbemScripting.SWbemLocator")
    If blnErrorOccurred(getResource("errLocator")) Then
        Exit Sub
    End If
```

```
'Connect to the namespace
Set objService = objLocator.ConnectServer(strServer, strNameSpace, strUserName, strPassword)
If blnErrorOccurred(getResource("errServer1") & strServer & getResource("errServer2")) Then
    Exit Sub
End If

objService.Security_.impersonationlevel = 3
If blnErrorOccurred(getResource("errSecurity")) Then
    Exit Sub
End If
If strServer = "" Then
    'Get the server's name
    Set objWshNet = CreateObject("WScript.Network")
    If blnErrorOccurred(getResource("errNetworkObject")) Then
        Exit Sub
    End If
    strServer = objWshNet.ComputerName
End If
strMsg = ""
intProcessId = 0

Set objInstance = objService.Get("Win32_Process")
If blnErrorOccurred(getResource("errWin32Process")) Then
    Exit Sub
End If

If objInstance Is Nothing Then
    Exit Sub
End If

intStatus = objInstance.Create(strCommand, Null, Null, intProcessId)
If blnErrorOccurred(getResource("errCreateProcess1") & _
   strCommand & getResource("errCreateProcess2")) Then
    Exit Sub
End If

If intStatus = 0 Then
    If intProcessId < 0 Then
        '4294967296 is 0x100000000.
        intProcessId = intProcessId + 4294967296
    End If
    strMsg = getResource("msgSucess1") & strCommand & getResource("msgSucess2")
```

```
            strMsg = strMsg & strServer & getResource("msgSucess3") & vbCrLf
            strMsg = strMsg & getResource("msgProcessID") & intProcessId
        Else
           strMsg = getResource("msgFailure1") & strCommand & getResource("msgFailure2")
            strMsg = strMsg & vbCrLf & getResource("msgStatus") & intStatus
        End If
        WScript.Echo strMsg

    End Sub



    ]]>
    </script>


    <script language="JScript">
    <![CDATA[

    // Declare globals
    var ie;
    var doc;
    var ie_continue;
    var rootdir;
    var htmlfile;

    // Start execution
    main();

    /*********************************************************************
    '* Function main()
    '*
    '* Purpose: Sets up IE, loads HTML file, and waits for IE to close.
    '*
    '*********************************************************************/
    function main()
    {
        init();
        ie.Navigate(rootdir + htmlfile);

        while (ie_continue)
        {
               WScript.Sleep(100);
    }
}

/*********************************************************************
'* Function init()
'*
'* Purpose: Initialization routines.
'*
'*********************************************************************/
function init()
{

    ie  = WScript.CreateObject("InternetExplorer.Application", "ie_");

    // Set up IE's window
    ie.AddressBar = false;
    ie.FullScreen = false;
    ie.MenuBar    = false;
    ie.Resizable  = false;
    ie.StatusBar  = false;
    ie.ToolBar    = false;
    ie.Height = 270;
    ie.Width = 380;

    // Get path to HTML file
    rootdir = WScript.ScriptFullName;
    rootdir = rootdir.substring(0, rootdir.lastIndexOf("\\") + 1);
    htmlfile  = getResource("strHTMLFile");

    // Don't stop
    ie_continue = true;
}

/*********************************************************************
'* Function ie_DocumentComplete()
'*
'* Purpose: Adds window title, sets up callback function to respond to
'*          IE events.
'*
'*********************************************************************/
function ie_DocumentComplete()
{
    doc = ie.Document;
    doc.title = getResource("strWindowTitle");
    doc.all.btnOK.onclick = btnOK_OnClick;
    ie.Visible = true;
}

/*******************************************************************
'* Function btnOK_OnClick()
'*
'* Purpose: Handles the IE click event for the OK button. Checks for
'*          a command and then calls the function to execute the command.
'*
'*******************************************************************/
function btnOK_OnClick()
{
    // Check that there is at least a command to execute
    if (doc.all.txtCommand.value == ""){
           WScript.Echo (getResource("errNoCommand"));
           return;
    }
    ExecuteCommand();
}

/*******************************************************************
'* Function ie_OnQuit()
'*
'* Purpose: Handles the IE OnQuit event and ends this program.
'*
'*******************************************************************/
function ie_OnQuit()
{
    ie_continue = false;
}


]]>
</script>
</job>
</package>
```

This script uses an HTML file named Exec.htm to provide the user interface:

```
<html>
<head>
<title>Run a program on a remote computer</title>
</head>
```

```
<body>
<p>Run a program on a remote computer.</p>
<form name="frmMain">
<table border="1" cellspacing="0" cellpadding="5">
  <tr>
    <td>Command:</td>
    <td><input type="text" name="txtCommand" size="30"></td>
  </tr>
  <tr>
    <td>Computer Name:</td>
    <td><input type="text" name="txtComputer" size="30"></td>
  </tr>
  <tr>
    <td>User Name:</td>
    <td><input type="text" name="txtUser" size="30"></td>
  </tr>
  <tr>
    <td>Password:</td>
    <td><input type="password" name="txtPassword" size="30"></td>
  </tr>
  <tr>
    <td>&nbsp;</td>
    <td align="right"><input type="button" value="OK" name="btnOK"></td>
  </tr>
</table>
</form>

</body>
</html>
```

Following the comments at the top of the script are a series of <resource> tags. These tags contain the strings used in the script, which makes it easy to find the strings for editing or localization.

The first <script> tag includes the file ErrorMsg.vbs. This script contains the same error function used in the previous example, Processor.vbs. Because many scripts require error reporting, this same script can be used in many places.

The first subroutine is ExecuteCommand, and it does all the work. It is placed first in the script so that it will be available to the functions and subroutines following it in the file. This function uses the WMI interface to launch a command on a remote computer.

The remainder of this script is written in JScript. The main function starts by calling the init function, loading our form into Internet Explorer, and then simply going to sleep until the ie_continue variable becomes False.

The init function creates an InternetExplorer.Application object and sets up its window. Then it gets the path and name of the HTML file that provides our user interface, sets ie_continue to True, and returns.

Control is returned to the main function, which then loads the HTML document into Internet Explorer. The main function then sits in a loop, waiting for ie_continue to change.

It doesn't look like anything else happens in this script, because main contains no more statements. But when Internet Explorer finishes loading the HTML page, the DocumentComplete event is triggered, which calls the ie_DocumentComplete function. Note that the name of the function is created by taking the object variable name, ie, and appending an underscore and the event name.

The ie_DocumentComplete function sets up additional properties of the ie object, including the title. The line

```
doc.all.btnOK.onclick = btnOK_OnClick;
```

says to call the btnOK_OnClick function when the button named btnOK is clicked in Internet Explorer. When this is done, Internet Explorer's Visible property is set to True, and it appears on the screen.

When the OK button is clicked, the btnOK_OnClick function is called. This function checks to be sure that the Command text box contains an entry, and it displays an error message if the box is empty. If the function finds a command, it calls the ExecuteCommand function, which does the work of executing the command.

When you close the Internet Explorer window, the OnQuit event is triggered, calling the ie_OnQuit function. This functions simply sets ie_continue to False so that the main function will exit.

Part 10

Maintaining and Optimizing

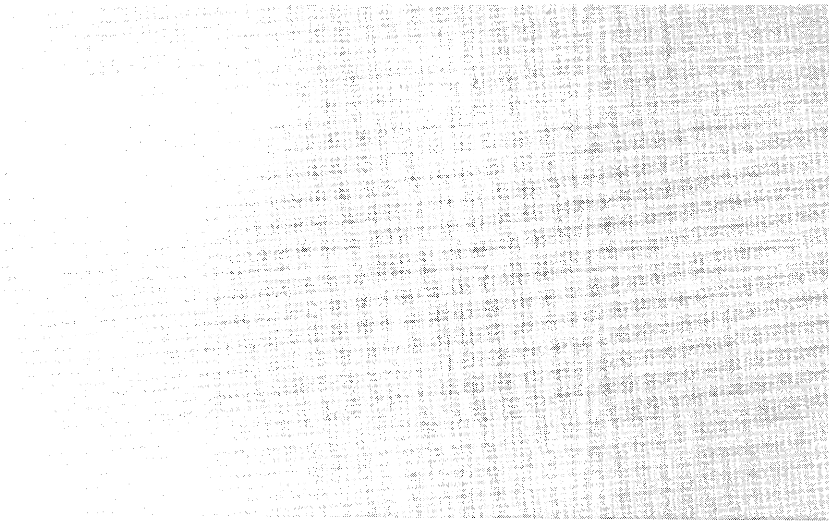
Chapter 39
Working with the Registry 655

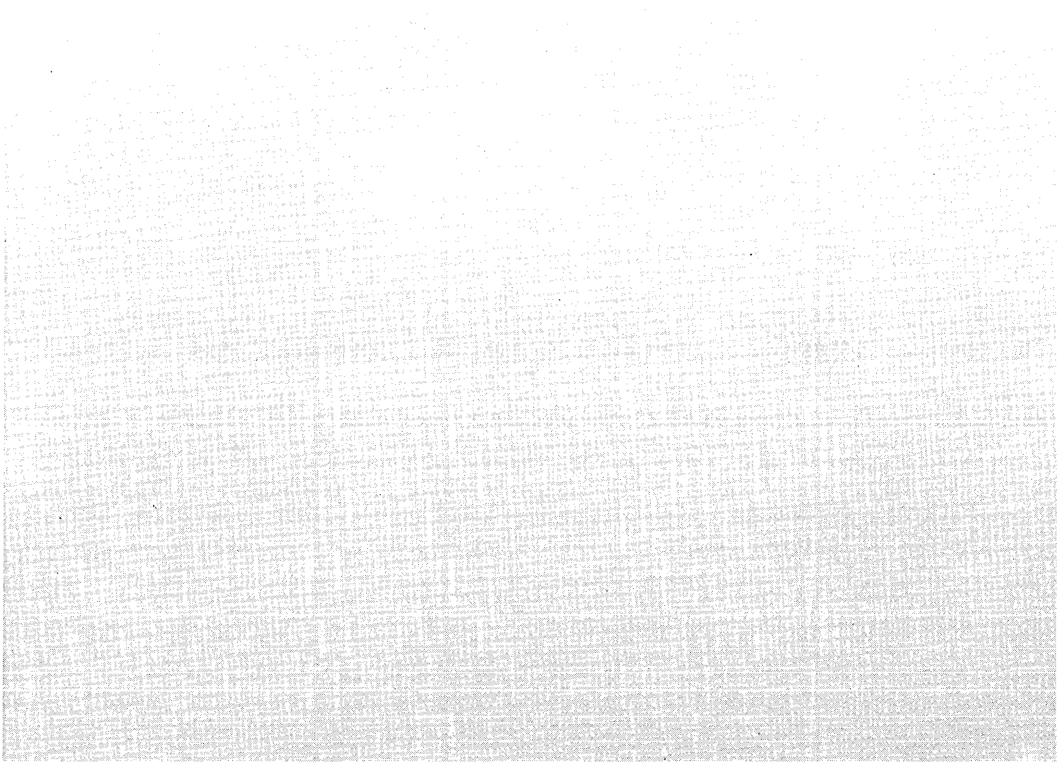
Chapter 40
Performing Routine Maintenance 669

Chapter 41
Viewing System Information 679

Chapter 42
Troubleshooting 689

Chapter 43
Monitoring System Performance 713





Chapter 39

Working with the Registry

In This Chapter

How the Registry Is Structured 656

Backing Up and Restoring the Registry 659

Regedit vs. Regedt32 660

Editing the Registry 661

Changing Registry Key Permissions 665

Working with a Remote Computer's Registry 666

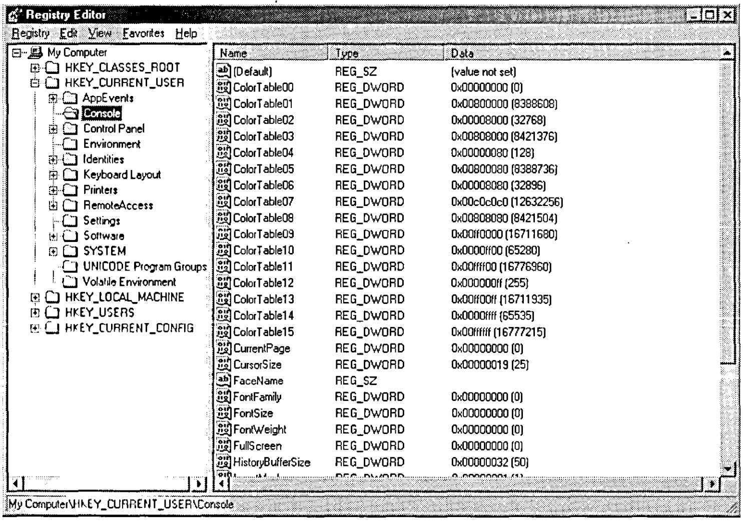
Monitoring Changes to Your Registry 666

Microsoft Windows 2000 includes two programs for browsing and editing your own registry and remote registries. Called Regedit.exe and Regedt32.exe, neither is everything you want in a registry editor. Because both programs lack undo and journaling capabilities, and because both transfer edits immediately to the registry without an intermediate save step, you have to use them with a certain degree of caution. Like the warnings that accompany nearly every consumer device these days, the cautionary messages sprinkled throughout these registry editors' help documents are, perhaps, a bit overstated. Nevertheless, it's true that certain errant registry edits (particularly in the HKLM section, which records data about your hardware configuration) can make your system inoperable. Be alert and you won't get hurt, as a certain freeway-traffic reporter in Los Angeles used to say.

This chapter presents a brief overview of the registry's organization and data types, a survey of the strengths and weaknesses of Regedit and Regedt32, and some details about the use of each registry editor. For information about some useful third-party tools for managing the registry, see the CD that accompanies this book.

How the Registry Is Structured

Figure 39-1 shows a portion of a system's registry, as seen through Regedit. As shown in the figure, the registry consists of five *root keys*, called HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, and HKEY_CURRENT_CONFIG. (The registry actually includes a sixth root key, HKEY_DYN_DATA. This one doesn't appear in the figure because Windows 2000 doesn't allow you to see it—let alone modify it!) For simplicity's sake and typographical convenience, this book, like many other registry texts, abbreviates the root key names to HKCR, HKCU, HKLM, HKU, and HKCC.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ColorTable00	REG_DWORD	0x00000000 (0)
ColorTable01	REG_DWORD	0x00800000 (8388608)
ColorTable02	REG_DWORD	0x00008000 (32768)
ColorTable03	REG_DWORD	0x00808000 (8421376)
ColorTable04	REG_DWORD	0x00000080 (128)
ColorTable05	REG_DWORD	0x00800080 (8388736)
ColorTable06	REG_DWORD	0x00008080 (32896)
ColorTable07	REG_DWORD	0x00c0c0c0 (12632256)
ColorTable08	REG_DWORD	0x00808080 (8421504)
ColorTable09	REG_DWORD	0x00ff0000 (16711680)
ColorTable10	REG_DWORD	0x0000ff00 (65280)
ColorTable11	REG_DWORD	0x00ffff00 (16776960)
ColorTable12	REG_DWORD	0x000000ff (255)
ColorTable13	REG_DWORD	0x00ff00ff (16711935)
ColorTable14	REG_DWORD	0x0000ffff (65535)
ColorTable15	REG_DWORD	0x00ffffff (16777215)
CurrentPage	REG_DWORD	0x00000000 (0)
CursorSize	REG_DWORD	0x00000019 (25)
FaceName	REG_SZ	
FontFamily	REG_DWORD	0x00000000 (0)
FontSize	REG_DWORD	0x00000000 (0)
FontWeight	REG_DWORD	0x00000000 (0)
FullScreen	REG_DWORD	0x00000000 (0)
HistoryBufferSize	REG_DWORD	0x00000032 (50)

My Computer\HKEY_CURRENT_USER\Console

Figure 39-1
The registry consists of five root keys, each of which contains many subkeys.

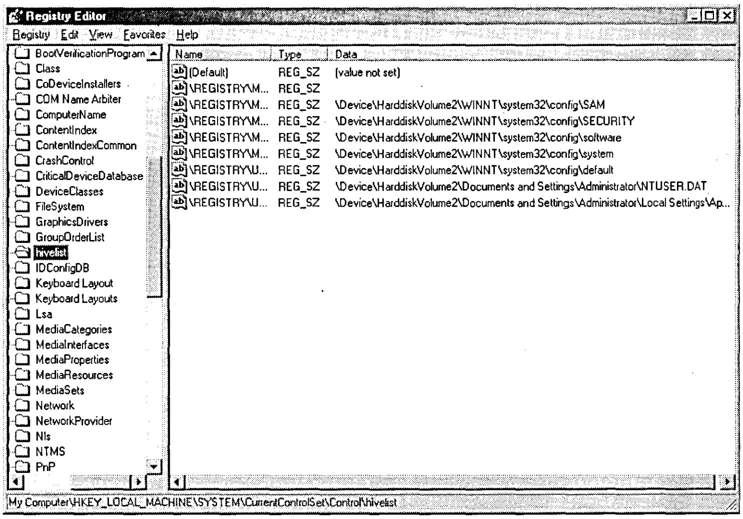
Root keys, which are also sometimes called *predefined keys*, contain subkeys. Registry editors, including Regedit and Regedt32, display this structure as an outline. In Figure 39-1, for example, HKCU has been opened to show the top-level subkeys: AppEvents, Console, Control Panel, and so on. A root key and its subkeys can be described as a path, like this: HKCU\Console. Root keys and their subkeys appear in the left pane of both Windows 2000 registry editors.

Subkeys, which we call *keys* for short, can contain subkeys of their own. Whether they do or not, they always contain at least one value. In most registry texts, and in Regedit, that value is identified as the default value. Many keys have additional values. The names, data types, and data associated with values appear in the right pane of both of the Windows 2000 registry editors. As Figure 39-1 shows, the HKCU\Console key has many values.

The default value for many keys—including HKCU\Console—is not defined. You can therefore think of an empty default value as a placeholder—a slot that could hold data but currently does not. (In Regedt32, empty default values do not appear. Default values that do contain data are identified as <No Name> instead of default.)

All values other than the default always include the following three components: name, data type, and data. As Figure 39-1 shows, the ColorTable00 value of HKCU\Console is of data type REG_DWORD. The data associated with this value is 0x00000000. (The prefix *0x* denotes a hexadecimal value. Regedit displays the decimal equivalent of hexadecimal values in parentheses.)

A key with all its subkeys and values is commonly called a *hive*. Registry documentation sometimes uses the term *hive* in a more restricted sense, to denote a root key and all its subkeys and values. Hives in this restricted sense also constitute segments of the registry that are stored on disk in separate data files. You can see where the hives on your system are located by examining the values associated with HKLM \System\CurrentControlSet\Control\HiveList. Figure 39-2 shows the HiveList key for one of the systems used for this book. Machine-specific hives are stored in %SystemRoot%\System32\Config; user-specific hives, which contain profile data, are stored in the %UserProfile% folder for each user.



Name	Type	Data
(Default)	REG_SZ	(value not set)
\REGISTRY\M...	REG_SZ	
\REGISTRY\M...	REG_SZ	\Device\HarddiskVolume2\WINNT\system32\config\SAM
\REGISTRY\M...	REG_SZ	\Device\HarddiskVolume2\WINNT\system32\config\SECURITY
\REGISTRY\M...	REG_SZ	\Device\HarddiskVolume2\WINNT\system32\config\software
\REGISTRY\M...	REG_SZ	\Device\HarddiskVolume2\WINNT\system32\config\system
\REGISTRY\U...	REG_SZ	\Device\HarddiskVolume2\WINNT\system32\config\default
\REGISTRY\U...	REG_SZ	\Device\HarddiskVolume2\Documents and Settings\Administrator\NTUSER.DAT
\REGISTRY\U...	REG_SZ	\Device\HarddiskVolume2\Documents and Settings\Administrator\Local Settings\Ap...

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist

Figure 39-2
You can find the names and locations of files that make up your registry in HKLM\System\CurrentControlSet\Control\HiveList.

If you ever need to back up or restore hive files from a command prompt, the information in HKLM\System\CurrentControlSet\Control\HiveList tells you where the files live and what they are named.

Note The registry is the work of many hands and bears no consistent approach to capitalization. With readability as our goal, we have made our own capitalization decisions for this book, and ours frequently differ from those you see in your registry editor. No matter. The registry itself is indifferent to capitalization.

Registry Data Types

The registry employs the following data types:

- **REG_SZ.** The *SZ* stands for zero-terminated string. This is a variable-length string that can contain Unicode as well as ANSI characters. Your registry editor automatically terminates the string with a 00 byte. A quick scan of the registry reveals that REG_SZ is one of the most common data types and that it's often used for numeric as well as textual data. (See, for example, the values of HKCU\Control Panel\Desktop.) The default values of most keys, where defined, are of type REG_SZ.
- **REG_DWORD.** A REG_DWORD is a "double word"—that is, a 32-bit numeric value. Although this data type can hold any integer from 0 to 2^{32}, the registry often uses it for simple Boolean values (0 or 1) because it lacks a Boolean data type.
- **REG_MULTI_SZ.** This type is simply a group of zero-terminated strings assigned to a single value. The REG_MULTI_SZ type is sufficiently uncommon that the designers of Regedit failed to provide a good multistring editor. If you need to create or modify values of this type, use Regedt32.
- **REG_EXPAND_SZ.** This data type is a zero-terminated string containing an environment variable, such as %SystemRoot%. If you need to create a key containing a variable name, use this data type, not REG_SZ.
- **REG_BINARY.** As its name suggests, the REG_BINARY type contains binary data—0s and 1s. For this data type, as for REG_MULTI_SZ, Regedt32 is a better editor than Regedit.
- **REG_LINK.** The REG_LINK data type is a pointer to another section of the registry. For example, the HKCU root key consists of REG_LINKs to a specific user's data stored under HKU. When a user logs on, HKCU is mapped to point to the appropriate user-specific information in HKU. The REG_LINK type allows programs that need information about the current user's preferences or history to get that information from a single source, HKCU, without having to know who's logged on. You can't create REG_LINK values through Regedit or Regedt32. It can be done only through the registry application programming interfaces (APIs).
- **REG_NONE.** The rare REG_NONE type is used only in unusual circumstances in which the presence or absence of a value is significant but the value's data is not.

- **REG_FULL_RESOURCE_DESCRIPTOR, REG_RESOURCE_LIST, and REG_RESOURCE_REQUIREMENTS_LIST.** These three data types provide information about the resources used or required by various components of your system. You'll probably never want to edit any of these values, but if you want to see what they look like, use Regedt32 and explore HKLM.

Backing Up and Restoring the Registry

Because the files that store registry hives are always open while Windows 2000 is running, you can't use simple copy procedures for backing up and restoring. You can, however, use Ntbackup.exe, the backup utility supplied with Windows 2000. To back up your registry with Ntbackup, choose the option to back up System State data. Ntbackup will back up your registry, your COM+ Class Registration database, and your boot files.

You can also back up the hive files listed at HKLM\System\CurrentControlSet\Control\HiveList by first booting into another operating system, such as MS-DOS. If your hives are stored on an NTFS volume, however, you need a tool that allows you to access that volume from your alternative operating system. You can find one for MS-DOS at *www.sysinternals.com/ntfspro.htm.*

Note *Microsoft Windows 2000 Professional Resource Kit* (Microsoft Press, 2000) includes Regback.exe and Regrest.exe, tools that let you back up your registry files while Windows 2000 is running. It also offers several other registry-management tools, including command-line (character-mode) utilities for searching and replacing registry keys, editing registry contents, and dumping registry contents to the standard output device (or a file). The Resource Kit tools work with local as well as remote registries.

Backing Up and Restoring Particular Hives

Regedit's Export Registry command (on the Registry menu) lets you save the current key, along with all its subkeys, values, and data, in a plain-ASCII file that can be restored to the registry via the Import Registry command (also on the Registry menu). These commands provide the undo or journaling capability that Regedit otherwise lacks. Before you make changes to a hive, you can save that hive to disk. If you repent, you can import the saved file to return the registry to its former condition.

Regedt32 also allows you to save and restore selected hives, by means of the Registry | Save Key command and the Registry | Restore command. There's a crucial difference, however, between the files created by Regedit's Export Registry and Regedt32's Save Key: a file created by Regedit records the key from which it was saved, whereas a file created by Regedt32 does not. When you restore a file exported by Regedit, the data automatically returns to the part of the registry from which it was saved. When you restore a file exported by Regedt32, the program displays a confirmation prompt to warn you that you're about to overwrite the current registry key. Be careful! It's your responsibility to verify that you've selected the right key to overwrite. Because a mistaken selection can wreak considerable damage to your registry, you might want to avoid using Regedt32 for simple undo-protection backup purposes.

Note Regedit's export files have the extension .reg. You can also restore such a file to the registry by right-clicking it in Windows Explorer and choosing Merge from the shortcut menu—or simply by double-clicking the file, assuming that its default action has not been changed. Application vendors typically use .reg files to add their data to your registry on setup, and, as we'll see, you can use .reg files to edit your own and others' registries as well.

Regedt32 has an additional command, Registry | Load Hive, that restores a saved hive without overwriting current registry data. The incoming information becomes a subkey to the selected key. This procedure provides a convenient way to duplicate a section of the registry—for example, to copy data from one user's section of HKU to another's. The Load Hive command is available only in HKU and HKLM.

Regedit vs. Regedt32

Each editor has strengths and weaknesses relative to the other. Unless you opt for a third-party program that has the best features of both, you'll probably find yourself switching between the two, using Regedit for certain tasks and Regedt32 for others. Incidentally, the Setup program for Windows 2000 doesn't create shortcuts for either editor on the Start menu, but it does install both editors. You can run either by typing its name (no path required) on a command line.

Here's a capsule summary of the differences between Microsoft's two registry editors:

- **User interface.** Regedt32 uses a multiple-document interface, conveniently displaying each root key in a separate window. Unfortunately, instead of using the current Windows standard for outline controls, it emulates the look and feel of the Windows 3.1 File Manager, requiring you to double-click outline entries to reveal their subentries. Moreover, determining exactly where you are in the registry is sometimes a challenge with Regedt32 because the program lacks a status bar. And, unlike Regedit, Regedt32 does not save your selection when you quit, so if you want to return to some deeply nested registry outpost at your next session, you either have to use the Find command or double-click your way back.

  In contrast, Regedit uses standard outline controls, displays your current position on its status bar, and keeps track of your selection when you quit. It's a cleaner, simpler design, and it doesn't make you feel like you're living in 1992.

- **Searching for keys, values, and data.** Regedit's Edit | Find command (shortcut Ctrl+F) lets you search through values and data as well as keys. It's more versatile than Regedt32's View | Find Key command (no shortcut), which looks only at key names. When you've entered a search string in Regedit, you can repeat the search by pressing F3.
- **Editing.** Regedit is fine for editing REG_SZ, REG_EXPAND_SZ, and REG_DWORD data. Because it presents all other data types as hexadecimal values, you'll probably feel more comfortable using Regedt32 for many editing tasks.
- **Risk-free browsing.** Regedt32 offers a read-only mode (Options | Read Only Mode) that's ideal for casual registry exploration. Regedit provides no such convenience.
- **Security.** Regedit won't help you if you need to change the permissions associated with a registry key. Use Regedt32's Security | Permissions command instead. *(See "Changing Registry Key Permissions, " page 665.)*

Editing the Registry

Now let's look at procedures for making specific kinds of changes to your registry.

Changing Data

In either registry editor, you can change the data associated with a value by double-clicking the value in the right pane. This action pops up an editor dialog box, where you can enter a new value. Note the following points:

- For data types other than REG_SZ, REG_EXPAND_SZ, and REG_DWORD, you'll probably prefer Regedt32 to Regedit. Regedt32's dialog boxes provide more options (the ability to work with binary data, either in binary or hex, for example), and only Regedt32 allows you to edit REG_MULTI_SZ data as strings.
- To add data to an empty default value, you must use Regedit. Regedt32 provides no way of doing this.

Adding or Deleting Keys

To add a key in Regedit, select the new key's parent key, choose Edit | New, and then choose Key from the cascading submenu. The new key arrives as a generically named outline entry, exactly the way a new folder does in Windows Explorer. Simply type to supply a new name. To delete a key, select it and press the Delete key.

To add a key in Regedt32, choose Edit | Add Key. The dialog box that appears has a Name field and a Class field. Don't waste any time trying to figure out what the Class field is for; it appears to have no purpose whatsoever. To delete a key, select it and press Delete.

Adding or Deleting Values

To add a value in Regedit, select the parent key and choose Edit | New. From the cascading submenu, choose String Value, Binary Value, or DWORD Value. (If you want an EXPAND_SZ or MULTI_SZ, use Regedt32, not Regedit.) The new value arrives in the right pane with a generic name. Type over the generic name, double-click, and add data to taste.

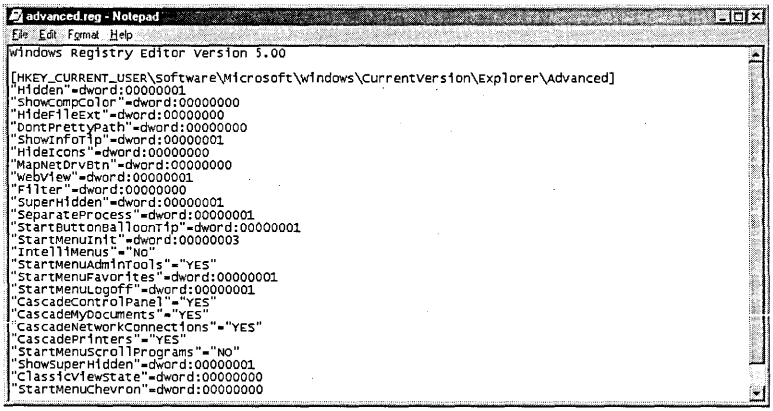
To add a value in Regedt32, choose Edit | Add Value. In the dialog box, supply a name and choose a data type from the drop-down list. Double-click the resulting value to supply data.

To delete a value in either program, select it and press Delete.

Using .Reg Files to Edit the Registry

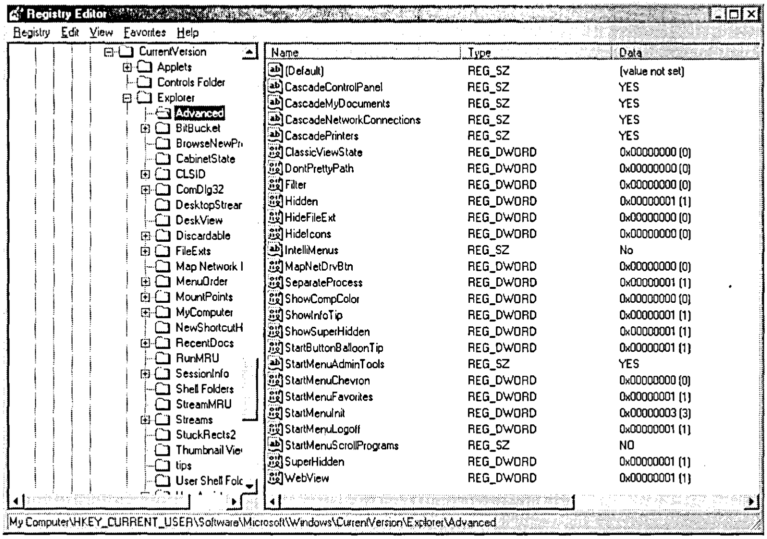
The .reg files created by Regedit's Export Registry command are plain ASCII, suitable for reading and modification in Notepad or any other plain-text editor. *(See "Backing Up and Restoring Particular Hives," page 659.)* Thus, you have an alternative way to edit your registry: you can export a hive, change it offline, and merge it back into the registry. Or you can add new keys, values, and data to the registry by creating a .reg file from scratch and merging it. A .reg file is particularly useful if you need to make the same changes to the registry of several different computers. You can make and test your changes on one machine, save the relevant part of the registry as a .reg file, and then transport the file to the other machines that require it.

Figure 39-3 shows an example of a .reg file. In this case, the file was generated from the HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced key, shown in Figure 39-4.



```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"Hidden"=dword:00000001
"ShowCompColor"=dword:00000000
"HideFileExt"=dword:00000000
"DontPrettyPath"=dword:00000000
"ShowInfoTip"=dword:00000001
"HideIcons"=dword:00000000
"MapNetDrvBtn"=dword:00000000
"WebView"=dword:00000001
"Filter"=dword:00000000
"SuperHidden"=dword:00000001
"SeparateProcess"=dword:00000001
"StartButtonBalloonTip"=dword:00000001
"StartMenuInit"=dword:00000003
"IntelliMenus"="No"
"StartMenuAdminTools"="YES"
"StartMenuFavorites"=dword:00000001
"StartMenuLogoff"=dword:00000001
"CascadeControlPanel"="YES"
"CascadeMyDocuments"="YES"
"CascadeNetworkConnections"="YES"
"CascadePrinters"="YES"
"StartMenuScrollPrograms"="NO"
"ShowSuperHidden"=dword:00000001
"ClassicViewState"=dword:00000000
"StartMenuChevron"=dword:00000000
```

Figure 39-3
A .reg file is a plain-text file suitable for offline editing. This one was generated by the key shown in Figure 39-4.



Name	Type	Data
(Default)	REG_SZ	(value not set)
CascadeControlPanel	REG_SZ	YES
CascadeMyDocuments	REG_SZ	YES
CascadeNetworkConnections	REG_SZ	YES
CascadePrinters	REG_SZ	YES
ClassicViewState	REG_DWORD	0x00000000 (0)
DontPrettyPath	REG_DWORD	0x00000000 (0)
Filter	REG_DWORD	0x00000000 (0)
Hidden	REG_DWORD	0x00000001 (1)
HideFileExt	REG_DWORD	0x00000000 (0)
HideIcons	REG_DWORD	0x00000000 (0)
IntelliMenus	REG_SZ	No
MapNetDrvBtn	REG_DWORD	0x00000000 (0)
SeparateProcess	REG_DWORD	0x00000001 (1)
ShowCompColor	REG_DWORD	0x00000000 (0)
ShowInfoTip	REG_DWORD	0x00000001 (1)
ShowSuperHidden	REG_DWORD	0x00000001 (1)
StartButtonBalloonTip	REG_DWORD	0x00000001 (1)
StartMenuAdminTools	REG_SZ	YES
StartMenuChevron	REG_DWORD	0x00000000 (0)
StartMenuFavorites	REG_DWORD	0x00000001 (1)
StartMenuInit	REG_DWORD	0x00000003 (3)
StartMenuLogoff	REG_DWORD	0x00000001 (1)
StartMenuScrollPrograms	REG_SZ	NO
SuperHidden	REG_DWORD	0x00000001 (1)
WebView	REG_DWORD	0x00000001 (1)

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

Figure 39-4
This key's name, values, and data are recorded in the .reg file shown in Figure 39-3.

As you examine the examples shown in the two illustrations, note the following:

- **Header line.** The file begins with the line Windows Registry Editor Version 5.00. When you merge a .reg file into the registry, Regedit uses this line to verify that the file contains registry data. Version 5 (the version of Regedit shipped with Windows 2000) generates Unicode text files. If you want to share registry data with a system running Windows NT 4 or Windows 9x, choose the Windows 9x/NT4 option in Regedit's Export Registry File dialog box. Otherwise, the Windows 9x or Windows NT version of Regedit will choke on the file's Unicode characters. To create a .reg file from scratch that's suitable for import into Windows 9x or Windows NT 4, use the header REGEDIT4 instead of Windows Registry Editor Version 5.00.
- **Key names.** Key names are delimited by brackets and must include the full path from root key to current subkey. The root key name must not be abbreviated. (Don't use HKCU, for example.) Figure 39-3 shows only one key name, but you can have as many as you please.
- **The default value.** Undefined default values do not appear in .reg files. Defined default values are identified by the special character @. Thus, a key whose default REG_SZ value was defined as MyApp would appear in a .reg file this way:

  ```
  "@"="MyApp"
  ```
- **Value names.** Value names must be enclosed in quotation marks, whether or not they include space characters. Follow the value name with an equal sign.

Notice that the value names shown in Figure 39-3 do not appear in the same order as in Figure 39-4. Don't ask why. (We didn't make this one up; this is how Regedit saved it.) Regedit displays your keys in alphabetical order, no matter how you enter them.

- **Data types.** REG_SZ values don't get a data-type identifier or a colon. The data follows directly after the equal sign. Other data types are identified as follows:

Data Type	Identifier
REG_DWORD	dword
REG_BINARY	hex
REG_EXPAND_SZ	hex(2)
REG_MULTI_SZ	hex(7)
REG_RESOURCE_LIST	hex(8)
REG_FULL_RESOURCE _DESCRIPTOR	hex(9)
REG_RESOURCE_ REQUIREMENTS_LIST	hex(a)
REG_NONE	hex(0)

A colon separates the identifier from the data. Thus, for example, a REG_DWORD value of 00000000 looks like this:

```
"Keyname"=dword:00000000
```

- **REG_SZ values.** Ordinary string values must be enclosed in quotation marks. A backslash character within a string must be written as two backslashes. Thus, for example, the path d:\lotus\123\addins is written like so:

```
"d:\\lotus\\123\\addins\\"
```

- **REG_DWORD values.** Dword values are written as eight hexadecimal digits, without spaces or commas. Do not use the *0x* prefix.
- **All other data types.** All other data types, including REG_EXPAND_SZ and REG_MULTI_SZ, appear as comma-delimited lists of hexadecimal bytes (two hex digits, a comma, two more hex digits, and so on). The following is an example of a REG_MULTI_SZ value:

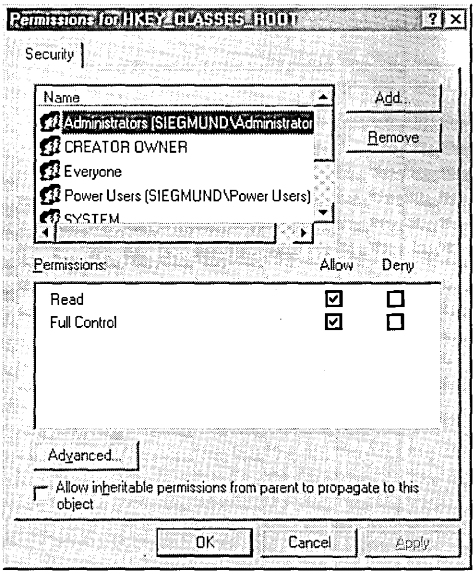
```
"Addins"=hex(7):64,00,3a,00,5c,00,6c,00,6f,00,74,00,75,00,73,00,5c,00,31,\
00,32,00,33,00,5c,00,61,00,64,00,64,00,69,00,6e,00,73,00,5c,00,64,00,71,\
00,61,00,75,00,69,00,2e,00,31,00,32,00,61,00,00,00,00,00,00,00
```

- **Line-continuation characters.** You can use the backslash as a line-continuation character. The REG_MULTI_SZ value just shown, for example, is all one stream of bytes. We've added backslashes and broken the lines for readability, and you can do the same in your .reg files.
- **Line spacing.** You can add blank lines for readability. Regedit ignores them.

Changing Registry Key Permissions

By default, administrators and the System account have full control over all registry keys. The Creator/Owner of a key has full control over that key. (For example, a user typically has full control over HKCU while that user is logged on.) In other registry contexts, a user's default permissions allow Read access but nothing more. If you attempt to change a registry key for which you have Read access only, your registry editor presents the appropriate editing dialog box but rejects your edit.

To change permissions for a key, log on as an administrator and use Regedt32's Security | Permissions command. The Permissions dialog box, shown in Figure 39-5, works the same way as similar dialog boxes in other parts of Windows 2000.



Permissions for HKEY_CLASSES_ROOT

Name
- Administrators (SIEGMUND\Administrator
- CREATOR OWNER
- Everyone
- Power Users (SIEGMUND\Power Users)
- SYSTEM

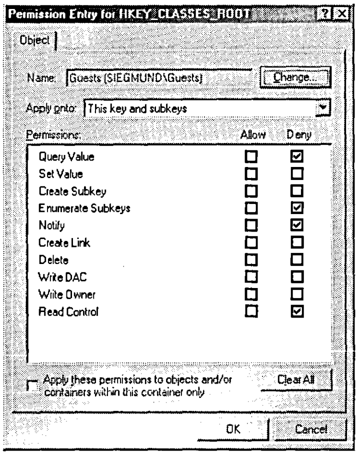
Permissions:	Allow	Deny
Read	☑	☐
Full Control	☑	☐

☐ Allow inheritable permissions from parent to propagate to this object

Figure 39-5
By default, administrators and the System account have full control over all registry keys. In most contexts, other users have Read access only.

Use the Add button to add a user or group to the Name list. For example, if you want to deny Read access to guest logons, click Add, select Guests in the ensuing Name list, and then click Add followed by OK. This returns you to the dialog box shown in Figure 39-5, where you can select Guests in the Name list and then select Deny in the Read row.

To set or deny something more specific than Read or Full Control, click the Advanced button in the dialog box shown in Figure 39-5. The Permissions tab of the Access Control Settings dialog box that appears specifically lists all the actions that each user and group can or cannot perform. To modify one of these settings, select it and click View/Edit. In the next dialog box that appears, shown in Figure 39-6, you can make the appropriate adjustments.



Name: Guests (SIEGMUND\Guests)

Apply onto: This key and subkeys

Permissions:	Allow	Deny
Query Value	□	☑
Set Value	□	□
Create Subkey	□	□
Enumerate Subkeys	□	☑
Notify	□	☑
Create Link	□	□
Delete	□	□
Write DAC	□	□
Write Owner	□	□
Read Control	□	☑

□ Apply these permissions to objects and/or containers within this container only

Figure 39-6
You can set permissions at a more granular level than Read or Full Control.

Permissions for a key propagate, by default, to all that key's subkeys that currently exist and all that might be created in the future. To turn this propagation off for a key, select the key, choose Security | Permissions, and clear the check box at the bottom of the Permissions dialog box.

Working with a Remote Computer's Registry

To work with a remote registry in Regedt32, choose Registry | Select Computer and specify the remote computer's network name. To do the same in Regedit, choose Registry | Connect Network Registry. Regedt32 permits you to work only with the remote computer's HKLM and HKU keys. In Regedit, you can also work with the remote computer's HKCR.

Monitoring Changes to Your Registry

Windows 2000 doesn't provide a registry monitoring tool, but third-party products that serve this function are available. (The excellent Regmon, for example, is included on the companion CD or you can download it from *www.sysinternals.com/regmon.htm.*) If you don't have a monitoring program, you can still take "before and after" shots of your registry to determine what changes have occurred. You might want to do this before installing a new application if you're concerned about what that application's setup routine might do to your registry.

You can use Regedit's Registry | Export Registry File command to dump your entire registry to a .reg file. (Choose All in the Export Range section of the Export Registry File dialog box.) This generates a gigantic disk file, of course, so if you're concerned only about changes in a particular section of the registry, you can save a little time and disk space by dumping only that section.

At any rate, after you've taken your "before" shot and "after" shot, you can use a file-comparison program to find out what changes have occurred. The Command Prompt program Fc.exe does a fast and efficient job of comparing large text files. Be sure to use the /U (Unicode) switch. You might also want to redirect output to a text file for easier inspection:

```
fc /u before.reg after.reg >regcomp.txt
```

If you prefer a graphical approach to file comparison, you can use the Windiff utility, one of the support tools supplied on your Windows 2000 Professional distribution CD. But Fc gets you the information you need a lot more quickly than Windiff.

Chapter 40

Performing Routine Maintenance

In This Chapter

Freeing Up Disk Space 669

Optimizing Disk Performance with Disk Defragmenter 672

Checking Disks for File-System and Media Errors 675

Using Windows Update to Maintain Driver and System Files 676

Backing Up 677

Keeping an Up-to-Date Emergency Repair Disk 678

Just as you perform regularly scheduled maintenance on your car, so should you take some simple periodic maintenance steps to keep your Microsoft Windows 2000 system running smoothly. In particular, it's wise to do the following on a regular basis:

- Make sure that you always have enough space on your hard disk, by getting rid of files you no longer need and compressing files if necessary.
- Defragment your hard disks to optimize file access.
- Check your disks for file-system and media errors.
- Visit the Windows Update Web site to make sure that you're using the latest versions of your device drivers and system files.
- Update your emergency repair disk (ERD).

Freeing Up Disk Space

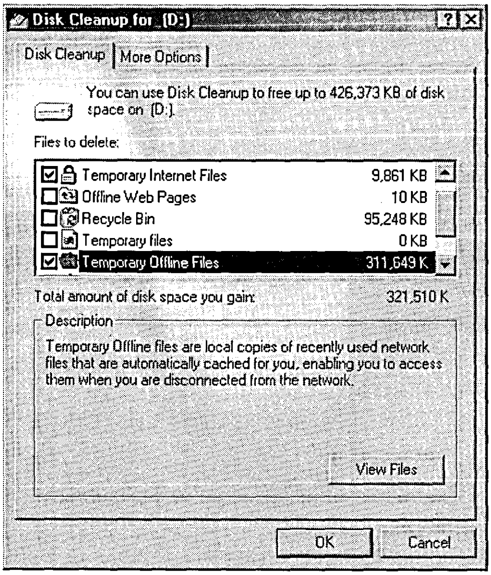
Like freeway lanes, hard disks have a way of filling to overcapacity, no matter how many you have. The very cheapness of disk storage encourages consumption; and Windows itself is a most extravagant consumer. It's important to keep an eye on your available space, because if you run too low on storage, Windows won't have enough room for its paging (swap) file. At that point, you start seeing ominous messages and degraded performance.

To pare back on disk-space consumption, you can do any or all of the following:

- Uninstall programs you don't need.
- Uninstall Windows components you don't need.
- Delete documents you don't need.
- Use the on-the-fly file compression available on NTFS volumes.

Cleaning Up with Disk Cleanup

The simplest way to perform most of these steps is with Disk Cleanup, a tool that you can run by choosing Start | Programs | Accessories | System Tools | Disk Cleanup. (Alternatively, right-click a disk in Windows Explorer, choose Properties from the shortcut menu, and click Disk Cleanup on the General tab of the properties dialog box.) Figure 40-1 shows an example of the work that Disk Cleanup can perform.



You can use Disk Cleanup to free up to 426,373 KB of disk space on (D:).

Files to delete:

☑ Temporary Internet Files	9,861 KB
□ Offline Web Pages	10 KB
□ Recycle Bin	95,248 KB
□ Temporary files	0 KB
☑ Temporary Offline Files	311,649 K

Total amount of disk space you gain: 321,510 K

Description

Temporary Offline files are local copies of recently used network files that are automatically cached for you, enabling you to access them when you are disconnected from the network.

Figure 40-1
Disk Cleanup can get the cobwebs off your system.

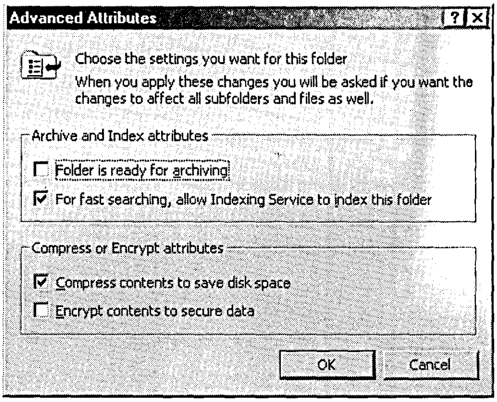
As the figure shows, Disk Cleanup can eliminate files in various categories. When you select a file category, the utility describes that category in the space below the category list. For most categories, you can click a View Files button to see the files in question in Windows Explorer.

The More Options tab in the Disk Cleanup dialog box provides two more buttons—one for removing Windows components, the other for removing other programs.

Clicking these buttons takes you to sections of Control Panel | Add/Remove Programs that were described in Chapter 9. *(See "Changing or Removing Programs," page 148; and "Adding and Removing Windows Components," page 149.)* Note that many of the Windows components that were on the list of removable items in previous versions of Windows are no longer there by default. Chapter 9, however, describes a way to restore those items to the list so that you can delete them.

Using NTFS File Compression

One of the many advantages of the NTFS file system is that it offers on-the-fly compression. All you have to do is set an attribute for an NTFS file, and Windows 2000 compresses it, decompressing it automatically when you open it. To compress a file or folder, right-click it in Windows Explorer, choose Properties from the shortcut menu, and click Advanced. In the Advanced Attributes dialog box, shown in Figure 40-2, select Compress Contents To Save Disk Space.



Advanced Attributes

Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☐ Folder is ready for archiving

☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes

☑ Compress contents to save disk space

☐ Encrypt contents to secure data

Figure 40-2
You can compress any or all of your NTFS files and folders by setting an attribute in this dialog box.

To compress an entire volume at once, right-click the drive in Windows Explorer and follow the procedure just described. You'll be asked to confirm that you really want to do this for every file in the volume. When you say yes, the system starts a process that might take hours to complete. But you need to do this only one time. (You can continue working while Windows 2000 is busy compressing your NTFS files. If the system wants to compress an open file, you'll be notified. At that point, you can close the file in question and click a Retry button, or you can click Ignore or Ignore All.)

Note the following about compressed NTFS files:

- Encryption, which is also enabled via an attribute setting, is incompatible with compression. For reasons that are not clear, the NTFS file system can compress a file or encrypt it, but it can't do both. *(For information about encryption, see "Encrypting Folders and Files," page 557.)*

- If you create a new file in a compressed folder, the new file is compressed.
- If you copy a file into a compressed folder, the file is compressed.
- If you move a file from a different NTFS volume into a compressed folder, the file is compressed.
- If you move a file from the same NTFS volume into a compressed folder, the file retains whatever compression setting it had originally.
- The amount of compression you get depends on the contents of the file. But in any case, the compression offered via NTFS is not as great as you would get from a third-party product such as WinZip. In return for less dramatic compression, NTFS offers the convenience of on-the-fly compression and decompression.

If you use compression, you might also want to take advantage of an option in Windows Explorer that displays compressed files and folders in an alternative color. That way, you can see at a glance which files and folders are compressed. To use this feature, choose Tools | Folder Options in Windows Explorer. Go to the View tab and select Display Compressed Files And Folders With Alternate Color.

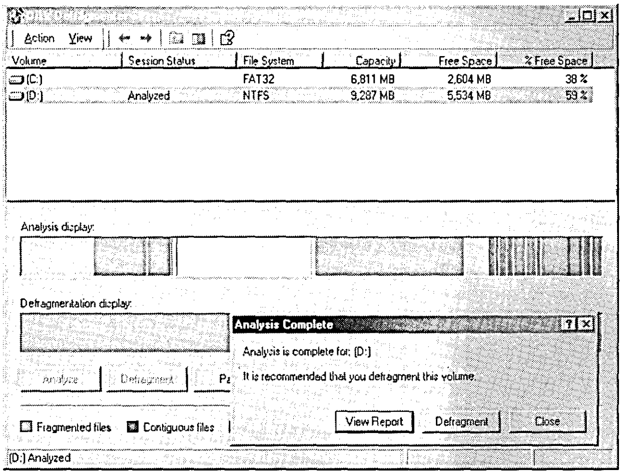
Optimizing Disk Performance with Disk Defragmenter

On a freshly formatted disk, files are stored in contiguous clusters. As files are deleted and new ones of differing sizes are created, this tidy arrangement of contiguously stored files breaks down, and files that were once all one piece become split into many noncontiguous pieces. The resulting fragmentation adversely affects disk performance because it takes more movement of the read/write head to open or save a file. The Disk Defragmenter utility improves performance by rearranging files into contiguous clusters.

To run Disk Defragmenter, choose Start | Programs | Accessories | System Tools | Disk Defragmenter. Alternatively, do any of the following:

- Right-click a drive in Windows Explorer, choose Properties from the shortcut menu, click the Tools tab, and then click Defragment Now.
- Run Dfrg.msc from a command prompt.
- Right-click My Computer, choose Manage from the shortcut menu, open Storage in the console tree of Computer Management, and select Disk Defragmenter.

Disk defragmentation can be a time-consuming process, so it's probably not worth the bother on a disk that's not very fragmented. To determine whether it would be worthwhile to defragment a disk, select it in the top half of Disk Defragmenter's window and click Analyze. As Figure 40-3 shows, Disk Defragmenter presents its recommendation. You can click View Report to get more details. (See Figure 40-4.)



Volume	Session Status	File System	Capacity	Free Space	% Free Space
(C:)		FAT32	6,811 MB	2,604 MB	38 %
(D:)	Analyzed	NTFS	9,287 MB	5,534 MB	59 %

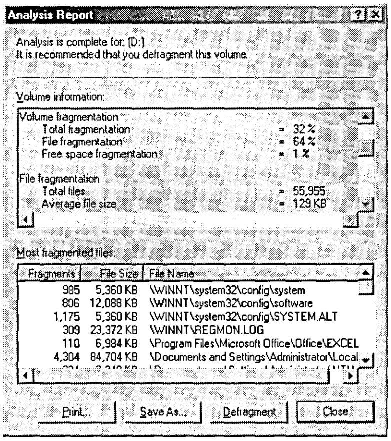
Analysis Complete

Analysis is complete for: (D:)

It is recommended that you defragment this volume.

(D:) Analyzed

Figure 40-3
Disk Defragmenter can analyze your disk to determine whether defragmentation is warranted.



Analysis Report

Analysis is complete for: (D:)
It is recommended that you defragment this volume.

Volume information:

```
Volume fragmentation
     Total fragmentation                 = 32 %
     File fragmentation                  = 64 %
     Free space fragmentation            = 1 %

File fragmentation
     Total files                         = 55,955
     Average file size                   = 129 KB
```

Most fragmented files:

Fragments	File Size	File Name
985	5,360 KB	\WINNT\system32\config\system
806	12,088 KB	\WINNT\system32\config\software
1,175	5,360 KB	\WINNT\system32\config\SYSTEM.ALT
309	23,372 KB	\WINNT\REGMON.LOG
110	6,984 KB	\Program Files\Microsoft Office\Office\EXCEL
4,304	84,704 KB	\Documents and Settings\Administrator\Local

Figure 40-4
Clicking the View Report button lets you see what percentage of your files are fragmented and which files are most widely scattered.

In the Analysis Report dialog box, you can click Save As to dump the analysis to a text file, Print to generate a printed report, or Defragment to begin the optimization process.

Disk Defragmenter does not move the following items:

- The \Recycled and \Recycler folders (the repositories for your Recycle Bin on FAT and NTFS volumes, respectively)
- The files Safeboot.fs, Safeboot.csv, Safeboot.rsv, and Bootsect.dos (if they exist)
- The NTFS Master File Table (MFT)

- The NTFS Master File Table Mirror (MFTMirr)
- The paging file (Pagefile.sys)

The MFT, which the operating system must consult each time it accesses any file on an NTFS volume, is originally stored in contiguous clusters. Because severe fragmentation of the MFT would have a particularly adverse effect on disk performance, the operating system allocates enough space for this critical system file to allow expansion as you add documents and programs to your hard disk. Nevertheless, the MFT can become fragmented. (If you create a large number of small files, the number of entries in the MFT can cause the MFT to exceed the space originally allocated for it; if you create a lot of large files, those files might need some of the space originally allocated to the MFT, resulting in fragmentation of the MFT as files are subsequently added and deleted.) You can find out whether and to what degree your own MFT is fragmented by scrolling the upper portion of Disk Defragmenter's Analysis Report. (See Figure 40-4.)

As Microsoft Knowledge Base article Q174619 (included on the CD accompanying this book) explains, you can increase the ratio of MFT allocation to total disk space for all NTFS volumes on your system by adding the REG_DWORD value NtfsMftZoneReservation to the registry key HKLM\System\CurrentControlSet \Control\FileSystem (or editing this value if it already exists). Acceptable values are 1, 2, 3, and 4, with higher numbers resulting in larger MFT allocations. (Microsoft does not say exactly what the allocation ratios are.)

Note, however, that to be effective this registry change must be made at the time a disk is formatted. If your MFT is already in pieces, a registry fix will not reassemble it.

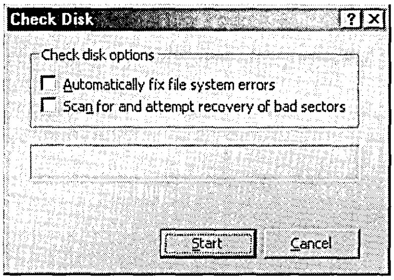
Disk Defragmenter's Analysis Report can also tell you whether your paging file is fragmented. Like the MFT, the paging file is a critical component of your system, and if it's in several pieces your system's performance will suffer. Disk Defragmenter cannot rearrange your paging file, but if yours is in fragments and you have more than one hard disk, you can work around the problem as follows:

1. Choose Start | Settings | Control Panel | System.
2. On the Advanced tab of the System Properties dialog box, click Performance Options.
3. Click Change.
4. Change both the minimum and maximum size of your current paging file to 0, and create a new paging file on a different disk.
5. Reboot your computer to make the new settings take effect.
6. Defragment the drive on which you originally had your paging file.
7. Repeat steps 1 through 4, re-creating a paging file on the original disk.
8. Reboot again.

Alternatively, you can look for a third-party defragmentation tool that offers boot-time defragmentation of your paging file. One candidate is Diskeeper, from Executive Software (*www.executive.com*), the company that supplies the defragmenter included with Windows 2000. (Diskeeper is a more feature-rich version of the Windows 2000 Disk Defragmenter.) Diskeeper can perform boot-time defragmentation of both the MFT and the paging file. Unlike the native Disk Defragmenter, it can also be set to run on a schedule, and you can use it to defragment disks on remote as well as local computers.

Checking Disks for File-System and Media Errors

To check a disk for file-system and media errors, you can right-click the disk in Windows Explorer, choose Properties from the shortcut menu, click the Tools tab, and then click the Check Now button. The Check Disk dialog box that appears provides a graphical interface for the Command Prompt command Chkdsk.



Check Disk
Check disk options
□ Automatically fix file system errors
□ Scan for and attempt recovery of bad sectors
Start
Cancel

Choosing Automatically Fix File System Errors in this dialog box is equivalent to running Chkdsk with the /F switch. Choosing Scan For And Attempt Recovery Of Bad Sectors is equivalent to running Chkdsk with /R. Choosing this second option implicitly chooses the first as well; that is, if you check for media errors (bad sectors), the command also checks the file system.

Both of these options require that the system be granted exclusive control of the disk that you want to check. If you have any open files or processes that require access to the disk, you are notified that the requested checkup cannot be carried out. You then have the option of having the system check your disk the next time you start your computer. If you accept, Windows 2000 opens a character-mode window and performs the desired check at your next startup, before the logon screen appears. If the disk in question is your boot disk, the system makes a second restart after completing the checkup.

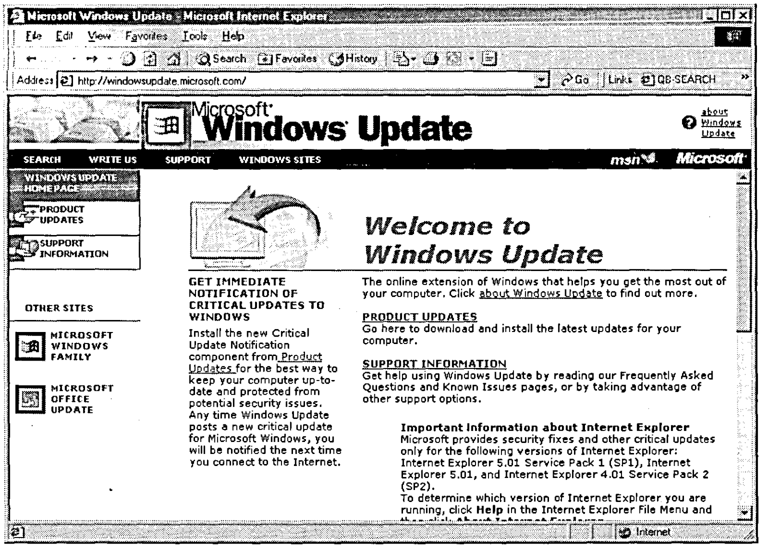
Unfortunately, although the graphical interface might be more pleasant to look at than the command line, you can't operate it through the Windows 2000 Scheduled Tasks facility. Therefore, to perform file-system and media checks automatically at regular intervals (a good maintenance practice), you need to create a batch program that executes Chkdsk.exe and then create a scheduled task to execute the batch program.

(For information about creating batch programs, see Chapter 37, "Using Batch Programs." For information about creating scheduled tasks, see Chapter 8, "Running Programs.")

Chkdsk has some additional options not provided by the graphical interface. To see an explanation of these options, open a Command Prompt window and type *chkdsk /?*.

Using Windows Update to Maintain Driver and System Files

As we mentioned in Chapter 16, "Using Device Manager and Hardware Profiles," it's a good practice to visit the Windows Update site periodically. Shown in Figure 40-5, the Windows Update site can keep you informed as newer drivers and Windows components become available for your system. Among other things, the Windows Update site offers a Critical Update Notification component. If you download it, this component automatically notifies you whenever Microsoft posts a new critical component for Windows 2000. But the Critical Update Notification component doesn't check for new device drivers, so you should still visit the Windows Update site from time to time, even if you have installed the notification component. To get to Windows Update, click the Windows Update command at the top of your Start menu (if it's there), or send your browser to *windowsupdate.microsoft.com.*



Welcome to Windows Update

GET IMMEDIATE NOTIFICATION OF CRITICAL UPDATES TO WINDOWS

Install the new Critical Update Notification component from Product Updates for the best way to keep your computer up-to-date and protected from potential security issues. Any time Windows Update posts a new critical update for Microsoft Windows, you will be notified the next time you connect to the Internet.

The online extension of Windows that helps you get the most out of your computer. Click about Windows Update to find out more.

PRODUCT UPDATES

Go here to download and install the latest updates for your computer.

SUPPORT INFORMATION

Get help using Windows Update by reading our Frequently Asked Questions and Known Issues pages, or by taking advantage of other support options.

Important Information about Internet Explorer

Microsoft provides security fixes and other critical updates only for the following versions of Internet Explorer: Internet Explorer 5.01 Service Pack 1 (SP1), Internet Explorer 5.01, and Internet Explorer 4.01 Service Pack 2 (SP2).

To determine which version of Internet Explorer you are running, click **Help** in the Internet Explorer File Menu and

Figure 40-5

The Windows Update site can notify you when new device drivers or Windows components are available for your system.

Windows Update also provides a link to a comparable update site for Microsoft Office, *officeupdate.microsoft.com.*

Backing Up

Although backing up is more akin to buying insurance than to getting an oil change or a tune-up, we would be remiss if our maintenance chapter did not at least mention the improved backup program that comes with Windows 2000 Professional. Ntbackup.exe, which you can run by choosing Start | Programs | Accessories | System Tools | Backup (alternatively, right-click a drive in Windows Explorer, choose Properties, click the Tools tab, and click Backup Now), now includes a scheduling feature. In other words, unlike the version shipped with Windows NT 4, the current backup program allows you to execute backup routines as scheduled tasks. Thus, while you're setting up other routine maintenance procedures, you can go ahead and establish a scheduled sequence of backups as well.

Ntbackup offers five types of backup:

- A *normal* backup backs up all selected files and clears their archive attributes (so that subsequent differential or incremental backups don't copy these files—unless, of course, the files have changed since their normal backup).
- An *incremental* backup copies selected files that have changed since the most recent normal or incremental backup and clears these files' archive attributes.
- A *differential* backup copies selected files that have changed since the most recent normal or incremental backup but does not clear the files' archive attributes. Subsequent differential backups continue to copy all files that have changed since the most recent normal or incremental backup.
- A *copy* backup copies all selected files but does not clear archive attributes. A copy backup is useful as a way of archiving particular files without affecting your overall backup routine.
- A *daily* backup copies all selected files that have changed on the current day, without clearing the files' archive attributes. It's a way of backing up a particular day's work without affecting the overall backup routine.

When you set up a backup task in Ntbackup, you have the option of including your system state data in the backup. Unless space limitations make it impossible, you should avail yourself of this option. When you back up your system state data, Ntbackup copies your registry, your COM+ Class Registration database, and your boot and system files to the backup medium. It also copies your registry to the folder %SystemRoot%\Repair\Regback. In the event of some kind of registry disaster—corruption or deletion of registry files, for example—you might be able to restore your registry from these Regback files, even if your backup medium became inaccessible. (Our more introductory book, *Running Microsoft Windows 2000 Professional* [Microsoft Press, 2000], provides a complete description of Ntbackup; see Chapter 29, "Protecting Your Data with Backup," in that volume.)

Keeping an Up-to-Date Emergency Repair Disk

One of the functions that Ntbackup can perform is the creation of an emergency repair disk (ERD). An ERD is a floppy disk containing data that might enable Windows 2000 to get your system running again if it fails to start in the normal way. (Recovery via ERD is one of the catastrophic recovery processes described in Chapter 42, "Troubleshooting.") You should update your ERD regularly, as one of your routine maintenance procedures. That way, if the need ever arises, you'll have a reasonably current recovery disk at your disposal.

To create an ERD, run Ntbackup (Start | Programs | Accessories | System Tools | Backup). On the Welcome tab, click Emergency Repair Disk.

Like Ntbackup's System State option, the process of creating an ERD also creates a registry backup in %SystemRoot%\Repair\Regback. (The files are too large to fit on the floppy disk.) If your registry is damaged, the ERD recovery process can make use of this backup. *(See "Using the Emergency Repair Disk," page 711.)*

Chapter 41

Viewing System Information

In This Chapter

Browsing Your System 680

Exporting System Information 684

Opening and Closing Saved System Information Files 684

Running System Information from a Command Prompt 685

Microsoft Windows 2000 includes a Microsoft Management Console snap-in called System Information that provides a read-only window into an array of details about the hardware and software components of your system. You can use this snap-in to satisfy your curiosity, to print or save a system inventory, or as a means of tracking down problems. You can save a record of your system components in text or binary format. The binary output, which can be read into another user's copy of System Information, is an ideal way to send a snapshot of your system to a product support specialist or other interested party. System Information's Tools menu also provides access to several potentially useful troubleshooting utilities.

To run System Information, do any of the following:

- Choose Start | Programs | Accessories | System Tools | System Information
- At a command prompt, type *"%commonprogramfiles%\microsoft shared\msinfo\msinfo32.exe"*
- At a command prompt, type *"%commonprogramfiles%\microsoft shared\msinfo\msinfo32.msc"*
- Launch either Msinfo32.exe or Msinfo32.msc from Windows Explorer

You can also get to System Information by right-clicking My Computer and choosing Manage. System Information is one of several snap-ins included in Computer Management.

Note that because System Information is a read-only tool, you don't have to be logged on as an administrator to use it. By default, all users have Read & Execute privileges.

Msinfo32.exe is an application whose function is to launch Msinfo32.msc, the MMC snap-in. Presumably, the reason the .exe exists is to provide additional switches (more than MMC itself provides) for command-line execution. *(See "Running System Information from a Command Prompt," page 685.)*

If you use Microsoft applications, it's possible that you also have other versions of Msinfo32.exe lurking on your system. These older versions are stand-alone applications and do not launch the MMC snap-in that is the subject of this chapter.

Note If you're curious about the provenance of alternative versions of Msinfo32.exe—or other applications or DLLs—visit Microsoft's DLL Help Database, at *support.microsoft.com/servicedesks/fileversion/dllinfo.asp.* Type the name of the file in question and click Submit. A list of version numbers appears. Use your file's properties dialog box to find its version number. Click the version number on the DLL Help Database site to see a list of applications or operating-system versions that might have supplied the file.

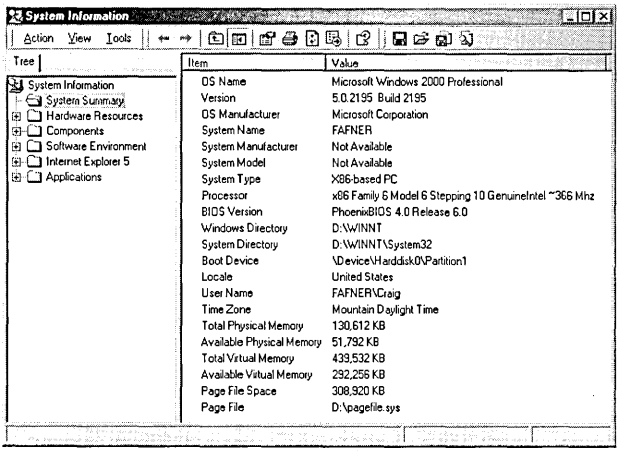
Browsing Your System

Figure 41-1 shows System Information's presentation of the System Summary item for one of the computers used to write this book. As you can see, the snap-in's console tree uses standard outline controls. You can display information for only one computer at a time. If you're perusing the local computer, the top entry in the console tree might say System Information (Local). Or it might simply say System Information. If you're working with a remote computer or if you open a saved information (.nfo) file, the name of that computer or file appears in parentheses after the words *System Information.*

To explore what System Information has to offer, simply open the outline controls and navigate. If you're investigating a local or remote computer directly (that is, you're not reading a previously saved .nfo file), you will probably have to wait a few seconds at each node of the outline while System Information refreshes its data.

Switching Between Basic and Advanced Views

Because the designers of Windows love to give you choices, System Information provides two types of views: Basic and Advanced. Unless you simply hate detail, you'll probably want to switch to Advanced view. Fortunately, your setting is



Item	Value
OS Name	Microsoft Windows 2000 Professional
Version	5.0.2195 Build 2195
OS Manufacturer	Microsoft Corporation
System Name	FAFNER
System Manufacturer	Not Available
System Model	Not Available
System Type	X86-based PC
Processor	x86 Family 6 Model 6 Stepping 10 GenuineIntel ~366 Mhz
BIOS Version	PhoenixBIOS 4.0 Release 6.0
Windows Directory	D:\WINNT
System Directory	D:\WINNT\System32
Boot Device	\Device\Harddisk0\Partition1
Locale	United States
User Name	FAFNER\Craig
Time Zone	Mountain Daylight Time
Total Physical Memory	130,612 KB
Available Physical Memory	51,792 KB
Total Virtual Memory	439,532 KB
Available Vitual Memory	292,256 KB
Page File Space	308,920 KB
Page File	D:\pagefile.sys

Figure 41-1
Browsing your system is a matter of navigating standard outline controls.

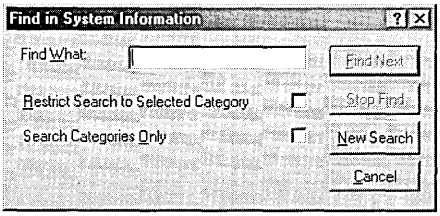
persistent. You need to switch only once, and then forevermore System Information will tell all that it knows.

To switch from Basic to Advanced view (or vice versa), simply open the View menu and select the desired view.

Searching for Information Items

The Action I Find command lets you search for either information categories or data in the details pane. If you're working with a saved System Information file, you'll find the command's performance more than satisfactory. On the other hand, if you're looking at "live" data—the current state of your own computer, for example—the Find command will prove maddeningly slow. That's because System Information caches nothing. As it traverses the console tree outline in search of your category or data, it has to refresh the current category's data at every stop along the way.

If you're simply looking for an item in the console tree, select Search Categories Only in the Find command's dialog box:



Find What:

Restrict Search to Selected Category □

Search Categories Only □

If you're looking for data and you know what category it belongs to, select that category first and then select Restrict Search To Selected Category in the command's dialog box. Note, however, that System Information still refreshes the category before performing the search. If the category is one that takes a long time to refresh (Running

Tasks, for example), you can probably hunt for the data (using your eyeballs) faster than the snap-in can.

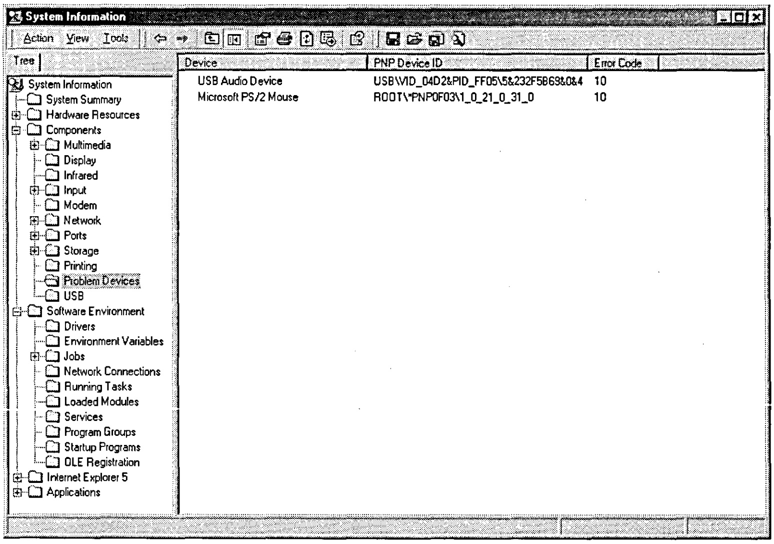
Manipulating the Details Pane

The available columns in the details pane vary, depending on the current information category (the console tree item). By default, System Information always displays all the columns available for a particular item, but for some items more columns are displayed in Advanced view than in Basic view. You can hide, display, or rearrange columns by choosing View | Choose Columns.

To change the sorting order of any item in the details pane, click once or twice on the heading of the column by which you want to sort. (The first click generates an ascending sort; the second, a descending sort.) For example, to see which loaded modules are the largest, choose Software Environment\Loaded Modules in the console tree, and then click the Size column heading twice.

Interpreting Problem Device Error Codes

The Components\Problem Devices category lists troubled components by their device names and Plug and Play IDs. (See Figure 41-2.) A third column reports the same error codes that you see if you investigate these devices in Device Manager. *(See Chapter 16, "Using Device Manager and Hardware Profiles.")* For an explanation of what the error codes mean, consult Microsoft Knowledge Base (KB) article Q125174, included on the CD that accompanies this book.



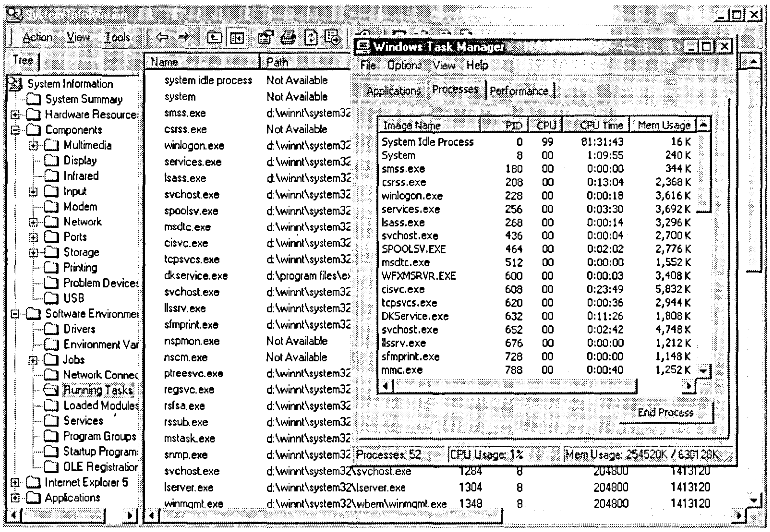
Device	PNP Device ID	Error Code
USB Audio Device	USB\VID_04D2&PID_FF05\5&232F5B69&0&4	10
Microsoft PS/2 Mouse	ROOT*PNP0F03\1_0_21_0_31_0	10

Figure 41-2
Like Device Manager, System Information can call your attention to devices that are not functioning properly.

Finding Out What's Running

Like Windows Task Manager (press Shift+Ctrl+Esc, or press Ctrl+Alt+Delete and click Task Manager), System Information can tell you the name of each process that's currently running. (See Figure 41-3.) System Information and Task Manager provide slightly different data, however:

- To see the full path and file name of each running process, use System Information.
- To find out the version number and file date for each running process, use System Information.
- To determine which process is using the most CPU cycles, check the CPU column in Windows Task Manager.
- To find out how much memory each process is using, use Windows Task Manager.
- To determine which application called each process, use Windows Task Manager. Right-click an application name on the Applications tab, and then choose Go To Process from the shortcut menu.
- To refresh the Running Processes display in System Information, choose Action | Refresh. The display in Windows Task Manager is refreshed automatically when processes begin or end.



Name	Path				
system idle process	Not Available				
system	Not Available				
smss.exe	d:\winnt\system32				
csrss.exe	Not Available				
winlogon.exe	d:\winnt\system32				
services.exe	d:\winnt\system32				
lsass.exe	d:\winnt\system32				
svchost.exe	d:\winnt\system32				
spoolsv.exe	d:\winnt\system32				
msdtc.exe	d:\winnt\system32				
cisvc.exe	d:\winnt\system32				
tcpsvcs.exe	d:\winnt\system32				
dkservice.exe	d:\program files\e›				
svchost.exe	d:\winnt\system32				
llssrv.exe	d:\winnt\system32				
sfmprint.exe	d:\winnt\system32				
nspmon.exe	Not Available				
nscm.exe	Not Available				
ptreesvc.exe	d:\winnt\system32				
regsvc.exe	d:\winnt\system32				
rsfsa.exe	d:\winnt\system32				
rssub.exe	d:\winnt\system32				
mstask.exe	d:\winnt\system32				
snmp.exe	d:\winnt\system32				
svchost.exe	d:\winnt\system32\svchost.exe	1284	8	204800	1413120
lserver.exe	d:\winnt\system32\lserver.exe	1304	8	204800	1413120
winmgmt.exe	d:\winnt\system32\wbem\winmgmt.exe	1348	8	204800	1413120

Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	99	81:31:43	16 K
System	8	00	1:09:55	240 K
smss.exe	180	00	0:00:00	344 K
csrss.exe	208	00	0:13:04	2,368 K
winlogon.exe	228	00	0:00:18	3,616 K
services.exe	256	00	0:03:30	3,692 K
lsass.exe	268	00	0:00:14	3,296 K
svchost.exe	436	00	0:00:04	2,700 K
SPOOLSV.EXE	464	00	0:02:02	2,776 K
msdtc.exe	512	00	0:00:00	1,552 K
WFXMSRVR.EXE	600	00	0:00:03	3,408 K
cisvc.exe	608	00	0:23:49	5,832 K
tcpsvcs.exe	620	00	0:00:36	2,944 K
DKService.exe	632	00	0:11:26	1,808 K
svchost.exe	652	00	0:02:42	4,748 K
llssrv.exe	676	00	0:00:00	1,212 K
sfmprint.exe	728	00	0:00:00	1,148 K
mmc.exe	788	00	0:00:40	1,252 K

Processes: 52 CPU Usage: 1% Mem Usage: 254520K / 630128K

Figure 41-3
Like Windows Task Manager, System Information can list all running processes.

Exporting System Information

To save all your system information as a text report, select the top-level item (System Information) in the console tree and choose Action | Save As Text File.

You can also save the details pane for the current category in any of the following text formats:

- Tab-delimited
- Unicode tab-delimited
- Comma-separated values
- Unicode comma-separated values

The two formats that use comma-separated values might prove more useful if you're planning to import the information into a database or spreadsheet program (although many such programs can read tab-delimited files as well). Choose one of the Unicode formats if you're working in a language that requires it.

To export a textual representation of the current outline item, select the item, right-click, and choose Export List from the shortcut menu. In the Save As dialog box, choose a file format and file name.

Exporting Binary Data

To save a binary representation of your complete set of system information, do any of the following:

- Right-click any item in the console tree and choose Save As System Information File from the shortcut menu.
- Choose Actions | Save As System Information File.
- Choose Actions | All Tasks | Save As System Information File.

The resulting .nfo file can be opened in any copy of System Information. Thus, you can attach it to an e-mail message and send it off to a product support specialist if the need arises.

Opening and Closing Saved System Information Files

To open a saved .nfo file, choose Action | All Tasks | Open System Information File. The incoming information replaces whatever System Information is currently displaying. To close a system information file, choose Action | All Tasks | Close System Information File. System Information then displays information about the local computer.

Running System Information from a Command Prompt

System Information's command-line syntax is as follows:

```
msinfo32.exe [ /s filename | /nfo filename | /report filename ] [ /computer
computername ] [/categories +|-categoryname(s) ]
```

/S *filename* — Saves data for the specified categories as an .nfo file.

/Nfo *filename* — An alternative form of /S *filename.*

/Report *filename* — Saves data for the specified categories as a text file.

/Computer — Opens System Information and connects to the specified computer.

/Categories + — In conjunction with /Report, /S, or /Nfo, allows you to | - *categoryname(s)* generate reports containing data for selected categories only. Use the plus sign to include a category. Use the minus sign in conjunction with +All to exclude a category. For example, */categories +All – ResourcesDMA* generates a report including all categories except ResourcesDMA.

Table 41-1 lists the available category names and the data they supply. Two categories—Hardware Resources\Page Files and Components\Network\NetBindings—are available only via the command-line /Categories parameter.

Table 41-1. Category Names

To Get or Omit This Information	Use This Category Parameter
All categories	All
System summary	SystemSummary
Hardware Resources\Conflicts/Sharing	ResourcesConflicts
Hardware Resources\DMA	ResourcesDMA
Hardware Resources\Forced Hardware	ResourcesForcedHardware
Hardware Resources\IO	ResourcesIO
Hardware Resources\IRQs	ResourcesIRQs
Hardware Resources\Memory	ResourcesMemory
Hardware Resources\Page Files	ResourcesPageFile
Components\Multimedia	ComponentsMultimedia
Components\Multimedia\Audio Codecs	ComponentsMultimediaAudio
Components\Multimedia\Video Codecs	ComponentsMultimediaVideo

(continued)

Table 41-1. Category Names *(continued)*

To Get or Omit This Information	Use This Category Parameter
Components\Multimedia\CD-ROM	ComponentsMultimediaCDROM
Components\Multimedia\Sound Device	ComponentsMultimediaSound
Components\Display	ComponentsDisplay
Components\Infrared	ComponentsInfrared
Components\Input	ComponentsInput
Components\Input\Keyboard	ComponentsKeyboard
Components\Input\Pointing Device	ComponentsPointDev
Components\Modem	ComponentsModem
Components\Network	ComponentsNetwork
Components\Network\Adapter	ComponentsNetAdapter
Components\Network\Protocol	ComponentsNetworkProtocol
Components\Network\NetBindings	ComponentsNetBindings
Components\Network\WinSock	ComponentsNetworkWinSock
Components\Ports	ComponentsPorts
Components\Ports\Serial	ComponentsSerialPorts
Components\Ports\Parallel	ComponentsParallelPorts
Components\Storage	ComponentsStorage
Components\Storage\Drives	ComponentsStorageDrives
Components\Storage\SCSI	ComponentsStorageSCSI
Components\Printing	ComponentsPrinting
Components\Problem Devices	ComponentsProblemDevices
Components\USB	ComponentsUSB
Software Environment\Drivers	SWEnvDrivers
Software Environment \Environment Variables	SWEnvVars
Software Environment\Jobs	SWEnvJobs
Software Environment\Jobs\Print	SWEnvPrint
Software Environment\Network Connections	SWEnvNetConn
Software Environment\Running Tasks	SWEnvRunningTasks
Software Environment\Loaded Modules	SWEnvLoadedModules
Software Environment\Services	SWEnvServices

(continued)

Table 41-1. Category Names *(continued)*

To Get or Omit This Information	Use This Category Parameter
Software Environment\Program Groups	SWEnvProgramGroup
Software Environment\Startup Programs	SWEnvStartupPrograms
Software Environment\OLE Registration	SWEnvOLEReg
Internet Explorer 5\Summary	IESummary
Internet Explorer 5\File Versions	IEFileVersions
Internet Explorer 5\Connectivity	IEConnectivity
Internet Explorer 5\Cache	IECache
Internet Explorer 5\Cache\Summary	IECacheSummary
Internet Explorer 5\List of Objects	IECacheObjectList
Internet Explorer 5\Content	IEContent
Internet Explorer 5\Content\Summary	IEContentSummary
Internet Explorer 5\Content \Personal Certificates	IEContentPersonalCertificates
Internet Explorer 5\Content\Other People's Certificates	IEContentOtherPeopleCertificates
Internet Explorer 5\Content\Publishers	IEContentPublishers
Internet Explorer 5\Security	IESecurity

Chapter 42

Troubleshooting

In This Chapter

Preparing for Disaster 690

Troubleshooting Tools Supplied with Windows 2000 692

Using the Windows Support Tools 700

Troubleshooting Resources Available on the Internet 704

What to Do If Your System Won't Start 706

Unless you lead an extraordinarily charmed life, at some point your system is not going to behave *exactly* the way you expect or the way its designers have promised. To help you deal with adversities large and small, Microsoft Windows 2000 Professional includes an assortment of troubleshooting tools. This chapter surveys the majority of those tools.

A detailed treatment of troubleshooting techniques and strategies could fill a book by itself. This chapter's purpose is more modest: to acquaint you with the tools that you have as a user of Windows 2000 Professional (and the Internet) and to point you toward sources of additional information. This chapter also includes information on ways to resuscitate a Windows 2000 system that has stopped running.

Some of the Windows 2000 troubleshooting armamentarium has been described elsewhere in this book. For information about tracking and deciphering error events, see Chapter 5, "Monitoring System and Application Activities with Event Viewer." For details about finding and resolving device resource conflicts, see Chapter 16, "Using Device Manager and Hardware Profiles." For information about network troubleshooting, see "Using Tools for Network Troubleshooting," page 406. Also see "Checking for File-System and Media Errors," page 675.

Preparing for Disaster

Just as preparedness officials develop evacuation plans for public buildings, you should give some thought—in advance of need—to how you might recover from a major system mishap. In addition to having your data adequately backed up, here are some steps worth taking:

- Keep an up-to-date emergency repair disk (ERD) handy.
- Install Recovery Console as a boot option.
- Configure Windows 2000's stop-error behavior.

Keeping an Up-to-Date ERD Handy

As Chapter 40 mentioned, updating your ERD should be part of your regular maintenance routine. If Windows fails to start because system files are damaged or missing, your ERD might help you get up and running again. To create or update your ERD, run Ntbackup (Start | Programs | Accessories | System Tools | Backup) and choose Tools | Create An Emergency Repair Disk. If you don't regularly back up your registry (using the System State option in Ntbackup or an equivalent feature in another backup program), be sure to accept the option that backs up your registry as well. Because this option does not back up the registry to the ERD itself (it wouldn't fit on a 1.44-MB floppy), and because Windows 2000 doesn't provide an easy way to restore the registry hives that it backs up in this manner, you should not rely on the ERD for registry backup. But if you really don't use any other form of registry backup, this is better than nothing. *(For information about restoring the registry from the backup created via the ERD, see "Using the Emergency Repair Disk," page 711.)*

Installing Recovery Console as a Boot Option

Recovery Console is a highly restricted character-mode subset of Windows 2000 that lets you make certain repairs in the event that Windows 2000 itself doesn't start. It allows you to perform such tasks as stopping Windows 2000 services (useful if a corrupted service is preventing your system from starting normally) and copying files to your hard drive from floppy disks or CD-ROMs (but not from a hard disk to a removable disk). *(See "Using Recovery Console," page 708.)*

You can start Recovery Console from the Windows 2000 distribution CD (if your computer can boot from a CD) or from a set of Windows 2000 Setup disks. Alternatively, you can install Recovery Console as a boot option (making your system, in effect, a dual-boot or multiboot system). Although this step involves a few minutes of your time (and 7 MB of hard disk space), it can save you time and anguish if your hour of need should arrive.

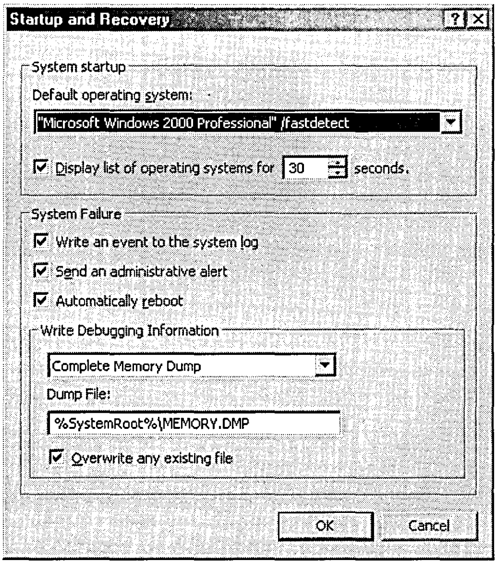
To install Recovery Console as a boot option:

1. Log on using an account with administrative privileges.
2. Insert the Windows 2000 CD. If the AutoPlay routine offers to install Windows 2000 for you, decline.
3. Choose Start | Run and type *d:\i386\winnt32.exe /cmdcons* (substituting your CD's drive letter for *d*).

After you've done this, whenever you start your system, you have the option of booting into Windows 2000 or Recovery Console (or another operating system, if your system is already set up to multiboot).

Configuring Windows 2000's Stop-Error Behavior

You have some choices about how Windows 2000 responds to a fatal error. To see what those choices are, choose Start | Settings | Control Panel | System, click the Advanced tab, and click Startup And Recovery. Figure 42-1 shows the Startup And Recovery dialog box. You must be logged on as a member of the Administrators group to make changes in this dialog box.



Startup and Recovery

System startup

Default operating system:

"Microsoft Windows 2000 Professional" /fastdetect

☑ Display list of operating systems for 30 seconds.

System Failure

☑ Write an event to the system log

☑ Send an administrative alert

☑ Automatically reboot

Write Debugging Information

Complete Memory Dump

Dump File:

%SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

Figure 42-1
In this dialog box, you can tell Windows 2000 what to do in the event of a fatal error.

The first check box in the System Failure section determines whether Windows will record the fatal error in the System log. It's hard to think of a good reason not to avail yourself of this option. (In fact, it's not even optional on Windows 2000 Server systems.) If the event is recorded, you can inspect it using Event Viewer—after you've successfully rebooted.

The Send An Administrative Alert check box, if selected, causes Windows to inform your administrator of your mishap. This might be useful if such a person exists on your network (and it isn't you).

Unless you need an immediate reboot after a stop error (for example, because critical applications depend on resources shared by your computer), you should clear the Automatically Reboot check box. Doing so gives you the opportunity to read at leisure whatever appears on the blue screen in the aftermath of the fatal error. If you leave this check box selected, you will have only a moment or two before the system attempts to reboot.

Before your system wades into the River Styx, you can have Windows record a snapshot of its memory contents. Such "last words" can help you or a support technician diagnose the terminal malady. How much of memory gets "dumped"—and where—depends on your settings in the Write Debugging Information section of the dialog box. Your choices are the following:

- **None.** Useful if you want the fastest possible reboot and don't care to perform a postmortem.
- **Small Memory Dump.** Records the smallest amount of useful information and requires about 2 MB of space on your boot volume (the volume where Windows 2000 is installed). If you choose this option, you don't have the option of overwriting existing dump files. Windows 2000 records a new file each time it goes down, leaving you with an audit trail of mini-dumps.
- **Kernel Memory Dump.** Records only the memory used by the operating-system kernel. The amount of disk space required depends on the size of your system's random access memory.
- **Complete Memory Dump.** Records a complete image of your computer's memory, requiring an extent of disk space equal to your system's memory plus 1 MB. This option obviously takes the longest, but it provides the most diagnostic information.

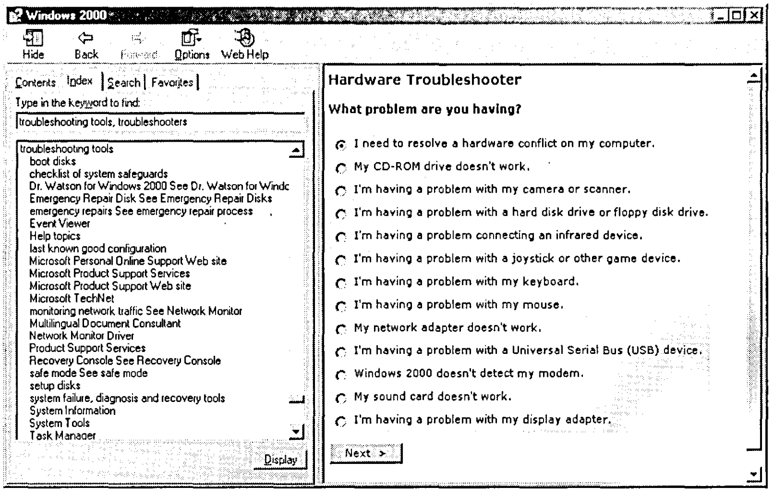
Troubleshooting Tools Supplied with Windows 2000

Now let's look at the troubleshooting utilities that come with your operating system.

The Help System Troubleshooters

The Windows 2000 Help system incorporates a set of interactive troubleshooters. These cover a gamut of topics, from Client Service for NetWare to Windows 3.x Programs. Each of these troubleshooters consists of a set of screens, all but the last of which ask you questions about the problem you're having. Given the troubleshooters' rather elementary level and your own expertise, it's not terribly likely that you'll find enlightenment at the end of this rainbow. Nevertheless, if your problem is one for which a troubleshooter is available, it would be worthwhile to try your luck with it.

To get to the Help system troubleshooters, choose Start | Help. On the Index tab, type *troubleshooters*. Then, under the heading *troubleshooters*, double-click the subentry *Windows 2000 troubleshooter list*. Figure 42-2 shows the opening screen of the hardware troubleshooter.



Type in the keyword to find:

troubleshooting tools, troubleshooters

troubleshooting tools
- boot disks
- checklist of system safeguards
- Dr. Watson for Windows 2000 See Dr. Watson for Windc
- Emergency Repair Disk See Emergency Repair Disks
- emergency repairs See emergency repair process
- Event Viewer
- Help topics
- last known good configuration
- Microsoft Personal Online Support Web site
- Microsoft Product Support Services
- Microsoft Product Support Web site
- Microsoft TechNet
- monitoring network traffic See Network Monitor
- Multilingual Document Consultant
- Network Monitor Driver
- Product Support Services
- Recovery Console See Recovery Console
- safe mode See safe mode
- setup disks
- system failure, diagnosis and recovery tools
- System Information
- System Tools
- Task Manager

Hardware Troubleshooter

What problem are you having?

● I need to resolve a hardware conflict on my computer.
○ My CD-ROM drive doesn't work.
○ I'm having a problem with my camera or scanner.
○ I'm having a problem with a hard disk drive or floppy disk drive.
○ I'm having a problem connecting an infrared device.
○ I'm having a problem with a joystick or other game device.
○ I'm having a problem with my keyboard.
○ I'm having a problem with my mouse.
○ My network adapter doesn't work.
○ I'm having a problem with a Universal Serial Bus (USB) device.
○ Windows 2000 doesn't detect my modem.
○ My sound card doesn't work.
○ I'm having a problem with my display adapter.

Figure 42-2
The Help system provides a set of elementary troubleshooting wizards.

Dr. Watson

Dr. Watson, known to your operating system as Drwtsn32.exe, is a program-error debugging utility. If an application dies, the doctor speeds to the scene and files a pathology report—a plain-text log that can help Sherlock (that's you or a support technician) diagnose the cause of the application's demise. Dr. Watson can also generate a crash dump, a binary file that can be loaded into a debugger.

The operating system's response to an application error follows this sequence:

1. The operating system checks to see whether the program generating the error has its own error handler.
2. If the application does not have its own error handler, the operating system checks to see whether the application is currently being debugged.
3. If the application is not currently being debugged, the operating system checks the Debugger and Auto values in the registry key HKLM\Software\Microsoft \Windows NT\CurrentVersion\AeDebug.
4. If Debugger specifies the command for a valid debugger and Auto is 0, the system presents a dialog box notifying you of the error. The dialog box includes

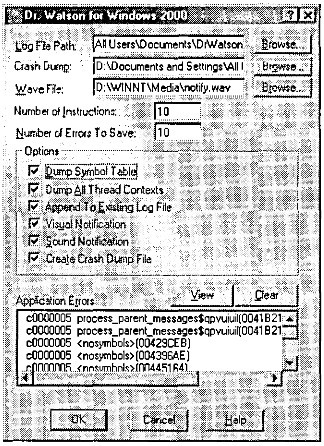
an OK button and a Cancel button. If you click OK, the offending application is terminated and nothing more happens. If you click Cancel, the debugger specified in the Debugger value is launched.

5. If Debugger specifies the command for a valid debugger and Auto is 1, the system runs the debugger directly.
6. If Debugger does not specify the command for a valid debugger, the system presents a dialog box notifying you of the error. The dialog box has only an OK button. When you click OK, the program is terminated.

When you first install Windows 2000, the Auto value is set to 1, and the Debugger value is set to launch Dr. Watson. If someone or something overrides this default (for example, if an application installs its own debugger in place of Dr. Watson), you can put Dr. Watson back on duty by typing *drwtsn32.exe –i* at a command prompt.

Setting Options for Dr. Watson

Figure 42-3 shows the dialog box in which you can set options for Dr. Watson. To arrive here, choose Start | Run and type *drwtson32* without the –I switch.



Log File Path: All Users\Documents\DrWatson

Crash Dump: D:\Documents and Settings\All I

Wave File: D:\WINNT\Media\notify.wav

Number of Instructions: 10

Number of Errors To Save: 10

Options

☑ Dump Symbol Table
☑ Dump All Thread Contexts
☑ Append To Existing Log File
☑ Visual Notification
☑ Sound Notification
☑ Create Crash Dump File

Application Errors

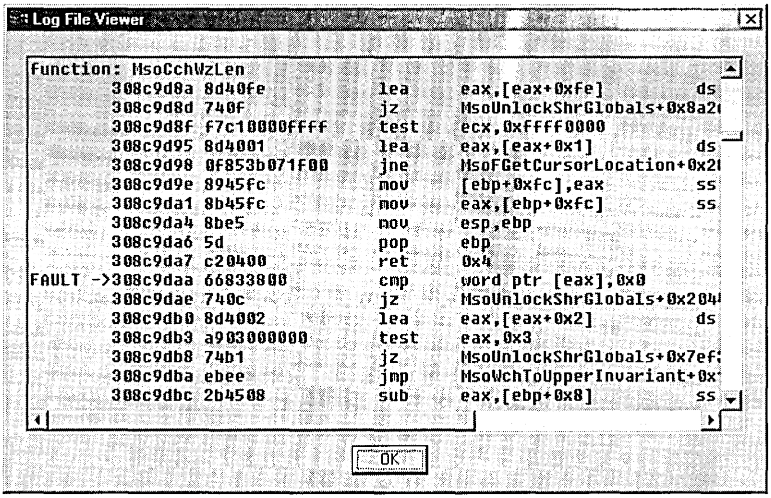
```
c0000005 process_parent_messages$qpvuiuil(0041B21
c0000005 process_parent_messages$qpvuiuil(0041B21
c0000005 <nosymbols>(00429CEB)
c0000005 <nosymbols>(004396AE)
c0000005 <nosymbols>(00445164)
```

Figure 42-3
Dr. Watson gets his orders from this dialog box.

Your options in this dialog box are as follows:

- **Log File Path.** Specifies the folder in which the ASCII error log will be recorded. The file itself is called Drwtsn32.log. The folder must be one to which all users at this machine have access.
- **Crash Dump.** Indicates the name and location of Dr. Watson's optional binary dump. The folder must be one to which all users at this machine have access.

- **Wave File.** Provides the name and location of a sound file by which Dr. Watson can announce a fatal application error.
- **Number Of Instructions.** Specifies the number of instructions, before and after the instruction at which the error occurred, that Dr. Watson will disassemble for inclusion in the log file. The default is 10. (See the following section and Figure 42-4.)
- **Number Of Errors To Save.** Specifies the maximum number of errors that Dr. Watson will record in the log file. Note that information recorded in the log is also recorded in the Application log and can be read in Event Viewer.
- **Dump Symbol Table.** If selected, causes the log file to record the name and address for each symbol used by each module running when the error occurred. This can be useful diagnostic information, but it will cause your log file to mushroom significantly.
- **Dump All Thread Contexts.** If selected, causes Dr. Watson to record state information for each thread in the offending application. If this check box is cleared, Dr. Watson records state information for only the thread that caused the error.
- **Append To Existing Log File.** Specifies whether each new error is recorded at the end of an existing log file or replaces an existing log.



```
Function: MsoCchWzLen
         308c9d8a 8d40fe          lea     eax,[eax+0xfe]           ds
         308c9d8d 740f            jz      MsoUnlockShrGlobals+0x8a2
         308c9d8f f7c10000ffff    test    ecx,0xffff0000
         308c9d95 8d4001          lea     eax,[eax+0x1]            ds
         308c9d98 0f853b071f00    jne     MsoFGetCursorLocation+0x2
         308c9d9e 8945fc          mov     [ebp+0xfc],eax           ss
         308c9da1 8b45fc          mov     eax,[ebp+0xfc]           ss
         308c9da4 8be5            mov     esp,ebp
         308c9da6 5d              pop     ebp
         308c9da7 c20400          ret     0x4
FAULT ->308c9daa 66833800        cmp     word ptr [eax],0x0
         308c9dae 740c            jz      MsoUnlockShrGlobals+0x204
         308c9db0 8d4002          lea     eax,[eax+0x2]            ds
         308c9db3 a903000000      test    eax,0x3
         308c9db8 74b1            jz      MsoUnlockShrGlobals+0x7ef
         308c9dba ebee            jmp     MsoWchToUpperInvariant+0x
         308c9dbc 2b4508          sub     eax,[ebp+0x8]            ss
```

Figure 42-4

In addition to the date, time, and process ID of a miscreant application, the log file includes a disassembly of instructions prior to and following the point at which the error occurred.

- **Visual Notification.** If selected, causes Dr. Watson to display a dialog box with an OK button when an error occurs. (The dialog box disappears if you ignore it for five minutes.)
- **Sound Notification.** If selected, causes the doctor to play a tune when summoned.
- **Create Crash Dump File.** If selected, causes Dr. Watson to record binary crash data that can be loaded into a debugger.

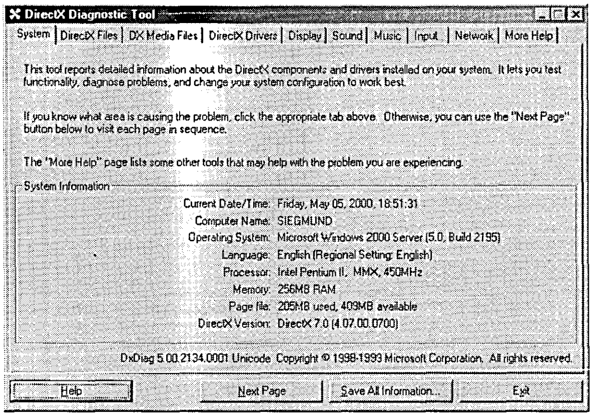
Viewing Dr. Watson's Log

The Application Errors section of the dialog box shown in Figure 42-3 lists your most recent errors. To read the log information for an error, simply select it and click the View button. Alternatively, navigate to the folder specified in the Log File Path field and open Drwtsn32.log in a text editor such as Notepad. Figure 42-4 shows a sample of the doctor's log.

You'll note that the beginning of the log file identifies the failing application only by its process identifier (PID). The log includes a table of all processes running when the misfortune occurred, however, and you can finger the offender there by its PID.

The DirectX Diagnostic Tool

The DirectX Diagnostic Tool, shown in Figure 42-5, allows you to check the functionality of your system's DirectX devices and drivers. You can step through the tool, page by page, by clicking the Next Page button. Alternatively, if you suspect that a particular DirectX component might be faulty, you can use the tabs to go straight to the relevant page. To run the DirectX Diagnostic Tool, type *dxdiag* at a command prompt.



This tool reports detailed information about the DirectX components and drivers installed on your system. It lets you test functionality, diagnose problems, and change your system configuration to work best.

If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.

The "More Help" page lists some other tools that may help with the problem you are experiencing.

System Information

Current Date/Time: Friday, May 05, 2000, 18:51:31
Computer Name: SIEGMUND
Operating System: Microsoft Windows 2000 Server (5.0, Build 2195)
Language: English (Regional Setting: English)
Processor: Intel Pentium II, MMX, 450MHz
Memory: 256MB RAM
Page file: 205MB used, 409MB available
DirectX Version: DirectX 7.0 (4.07.00.0700)

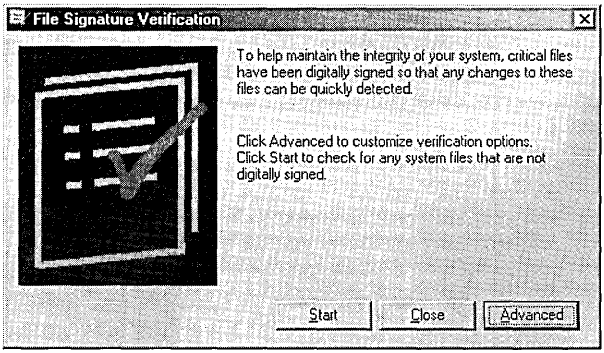
DxDiag 5.00.2134.0001 Unicode Copyright © 1998-1999 Microsoft Corporation. All rights reserved.

Figure 42-5
The DirectX Diagnostic Tool lets you check the health of your sound and display systems.

The DirectX Files, DX Media Files, and DirectX Drivers tabs list your system's DirectX files and drivers. A Notes section at the bottom of each of these tabs alerts you to potential problems. The Display, Sound, Music, Input, and Network tabs provide tests of system components. On the Display tab, for example, you can click Test DirectDraw or Test Direct3D to check out those aspects of your display system. A Save All Information button records file names, driver names, and diagnostic results in a plain-text file.

The File Signature Verification Utility

The system files supplied with Windows 2000 have been digitally signed by Microsoft. The digital signatures provide confirmation that these files have not been altered or overwritten by incompatible versions. If you suspect that an application you've installed has overwritten a digitally signed system file, you can check your hypothesis with the help of the File Signature Verification utility. To run this tool, choose Start | Run and type *sigverif*. The following dialog box appears:

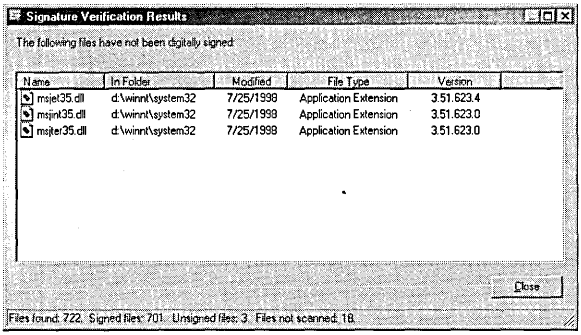


To help maintain the integrity of your system, critical files have been digitally signed so that any changes to these files can be quickly detected.

Click Advanced to customize verification options. Click Start to check for any system files that are not digitally signed.

By default, the utility checks system files only and writes its findings to the file %SystemRoot%\ Sigverif.txt, replacing any previous copy of that file. To change these defaults, click Advanced. You can choose to scan nonsystem files of any kind, to append the current results to the existing log file, and to change the name and location of the log file.

The File Signature Verification utility also reports its findings on screen, as Figure 42-6 shows. To read the complete details, however, including the names of the files that the utility was not able to scan (because those files were in use), you need to open the log file.



Signature Verification Results

The following files have not been digitally signed:

Name	In Folder	Modified	File Type	Version
msjet35.dll	d:\winnt\system32	7/25/1998	Application Extension	3.51.623.4
msjint35.dll	d:\winnt\system32	7/25/1998	Application Extension	3.51.623.0
msjter35.dll	d:\winnt\system32	7/25/1998	Application Extension	3.51.623.0

Files found: 722, Signed files: 701, Unsigned files: 3, Files not scanned: 18.

Figure 42-6
The File Signature Verification utility rounds up the usual suspects.

The Update Wizard Uninstall

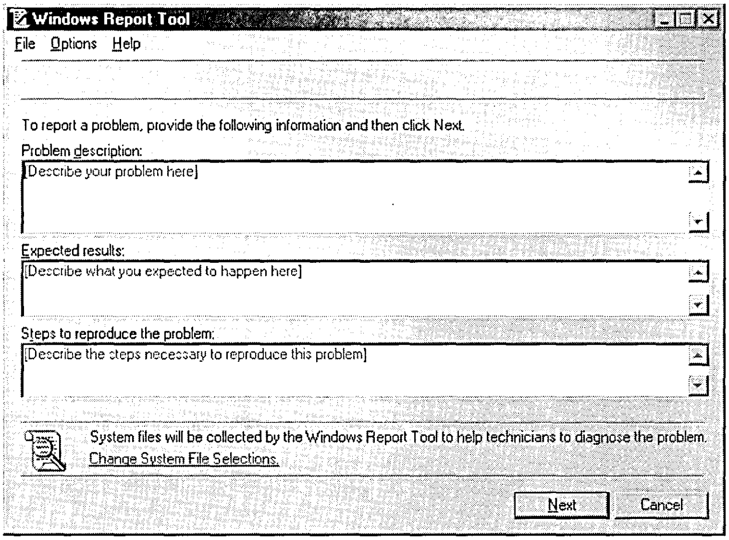
Microsoft's Windows Update site (*windowsupdate.microsoft.com*) can update your system as newer device drivers and other system components become available. *(See "Using Windows Update to Maintain Driver and System Files," page 676.)* If an updated device driver proves faulty, you can restore your prior driver with the help of the Update Wizard Uninstall tool. To get to this tool, first run System Information (%CommonProgramFiles%\Microsoft Shared\Msinfo\Msinfo32.msc). Then choose Tools | Windows | Update Wizard Uninstall.

The Windows Report Tool

The Windows Report Tool, shown in Figure 42-7, is a program that helps you communicate with a support specialist. On the program's opening screen, you can provide a verbal description of a problem, including details about what you expected to happen and what steps you took before the problem occurred. When you click Next, the program gathers information about your system. Clicking Next again saves the collected data in a report file suitable for uploading to a support specialist. To run the Windows Report Tool, type *winrep* at a command prompt.

You have some control over what information gets written to your report file and uploaded to your helper. To see your options, click the Change System File Selections link or choose Options | Collected Information. The dialog box shown in Figure 42-8 appears. Select or clear the appropriate check boxes in the Files To Copy list. Or click Add if you want to send files that do not appear in the list.

Before saving and sending your report, you'll probably also want to include some information about yourself so that the recipient will know how to get back to you. To record this data, choose Options | User Information.



To report a problem, provide the following information and then click Next.

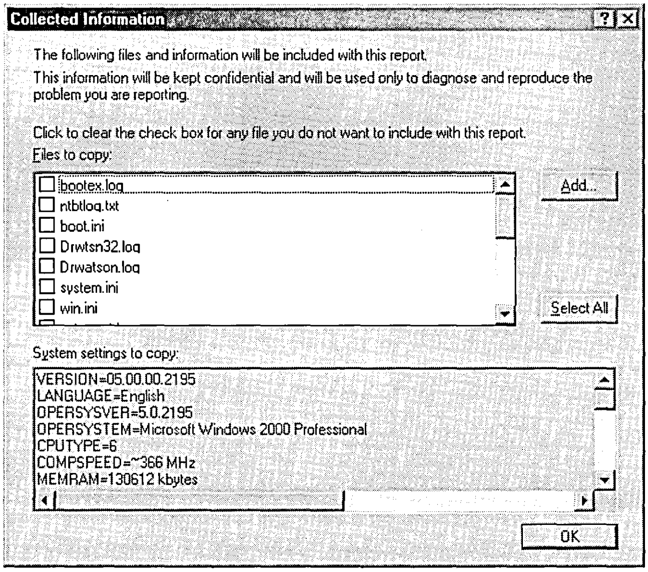
Problem description:
[Describe your problem here]

Expected results:
[Describe what you expected to happen here]

Steps to reproduce the problem:
[Describe the steps necessary to reproduce this problem]

System files will be collected by the Windows Report Tool to help technicians to diagnose the problem.
Change System File Selections.

Figure 42-7
The Windows Report Tool facilitates bug reporting and other calls for help.



The following files and information will be included with this report.
This information will be kept confidential and will be used only to diagnose and reproduce the problem you are reporting.

Click to clear the check box for any file you do not want to include with this report.
Files to copy:

☐ bootex.log
☐ ntbtlog.txt
☐ boot.ini
☐ Drwtsn32.log
☐ Drwatson.log
☐ system.ini
☐ win.ini

System settings to copy:

```
VERSION=05.00.00.2195
LANGUAGE=English
OPERSYSVER=5.0.2195
OPERSYSTEM=Microsoft Windows 2000 Professional
CPUTYPE=6
COMPSPEED=~366 MHz
MEMRAM=130612 kbytes
```

Figure 42-8
You can choose which data files to include in your report.

InoculateIT AntiVirus AVBoot

The Valueadd\3rdparty\Ca_antiv folder of your Windows 2000 Professional CD includes a program called InoculateIT AntiVirus AVBoot version 1.1, from Computer

Associates International. You can use this to check computer memory, your master boot record (MBR), and the boot sectors of all physical disks for memory-resident and boot-sector viruses. Before running AVBoot, you have to create a startup floppy disk. Insert a disk in drive A and run Makedisk.bat from the Ca_antiv folder. When you boot your computer from this floppy disk, AVBoot runs automatically.

Computer Associates recommends that you visit *support.cai.com* regularly to download the latest virus information.

Using the Windows Support Tools

Your Windows 2000 CD includes a set of tools for advanced users, some of which might prove useful to you in your time of troubleshooting need. To install these support tools, insert the Windows 2000 CD. Decline any offers to upgrade or install Windows 2000, and then navigate to \Support\Tools. Run Setup from this folder.

When installed, the support tools become accessible via Start | Programs | Windows 2000 Support Tools. To acquaint yourself with the offerings, choose Tools Help. There, you'll find an alphabetical listing and a description of each tool. Within the help text that describes a tool, you'll find a link that lets you run the tool. In many cases, this proves to be the easiest way to run the tool, because the Support Tools Setup program installs only certain of the tools on your Start menu.

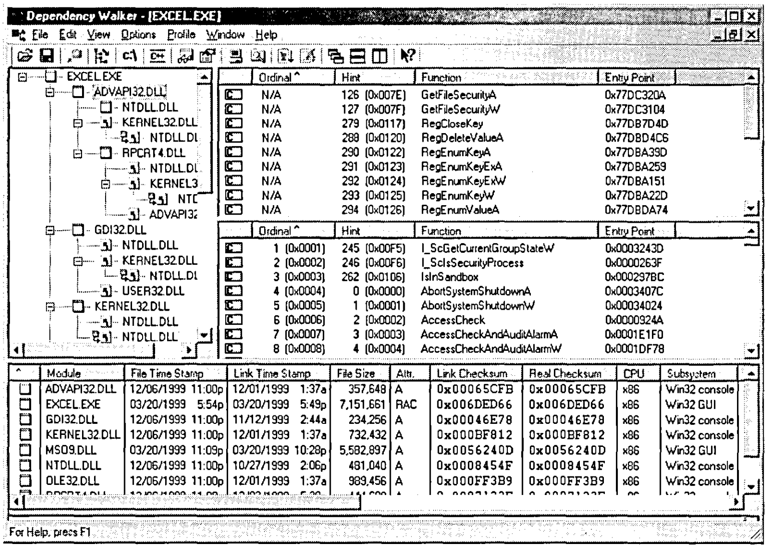
In the following paragraphs, we review some of the more useful support tools.

Dependency Walker (Depends.exe)

Dependency Walker, shown in Figure 42-9, is a graphical application that scans any 32-bit or 64-bit module (including .exe, .dll, .ocx, .sys, and other files) and presents an outline view of all dependent modules. For the end user, its most useful troubleshooting service is the ability to detect missing modules or invalid modules—.dll files, for example—required by an application.

FileVer (Filever.exe)

FileVer is a command-line (character-mode) utility that reports version information about a specified executable or .dll (or group thereof). This kind of information can be useful, for example, in helping a support technician track down which version of a hot-fix or service pack you've installed. Figure 42-10 shows a sample of FileVer's output.


Dependency Walker - [EXCEL.EXE]
File Edit View Options Profile Window Help
For Help, press F1

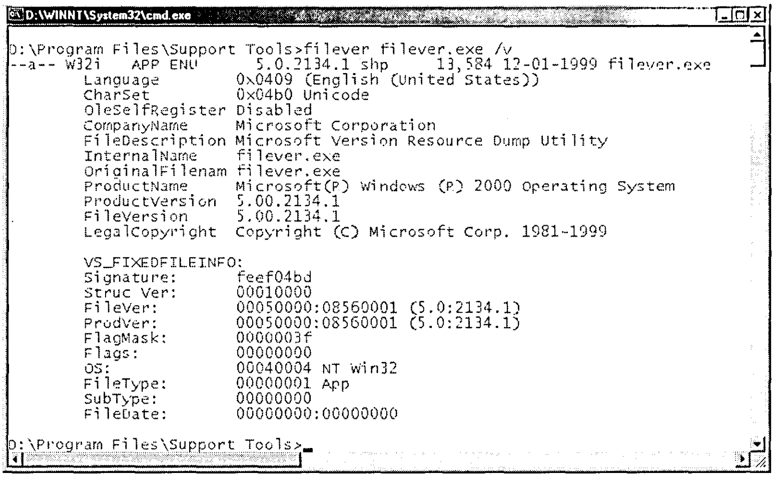
```
EXCEL.EXE
    ADVAPI32.DLL
        NTDLL.DLL
        KERNEL32.DLL
            NTDLL.DL
        RPCRT4.DLL
            NTDLL.DL
            KERNEL3
                NTC
            ADVAPI3:
    GDI32.DLL
        NTDLL.DLL
        KERNEL32.DLL
            NTDLL.DL
        USER32.DLL
    KERNEL32.DLL
        NTDLL.DLL
        NTDLL.DLL
```

	Ordinal ^	Hint	Function	Entry Point
C	N/A	126 (0x007E)	GetFileSecurityA	0x77DC320A
C	N/A	127 (0x007F)	GetFileSecurityW	0x77DC3104
C	N/A	279 (0x0117)	RegCloseKey	0x77DB7D4D
C	N/A	288 (0x0120)	RegDeleteValueA	0x77DBD4C6
C	N/A	290 (0x0122)	RegEnumKeyA	0x77DBA39D
C	N/A	291 (0x0123)	RegEnumKeyExA	0x77DBA259
C	N/A	292 (0x0124)	RegEnumKeyExW	0x77DBA151
C	N/A	293 (0x0125)	RegEnumKeyW	0x77DBA22D
C	N/A	294 (0x0126)	RegEnumValueA	0x77DBDA74

	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	245 (0x00F5)	I_ScGetCurrentGroupStateW	0x0003243D
C	2 (0x0002)	246 (0x00F6)	I_ScIsSecurityProcess	0x0000263F
C	3 (0x0003)	262 (0x0106)	IsInSandbox	0x000297BC
C	4 (0x0004)	0 (0x0000)	AbortSystemShutdownA	0x0003407C
C	5 (0x0005)	1 (0x0001)	AbortSystemShutdownW	0x00034024
C	6 (0x0006)	2 (0x0002)	AccessCheck	0x0000924A
C	7 (0x0007)	3 (0x0003)	AccessCheckAndAuditAlarmA	0x0001E1F0
C	8 (0x0008)	4 (0x0004)	AccessCheckAndAuditAlarmW	0x0001DF78

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem
□	ADVAPI32.DLL	12/06/1999 11:00p	12/01/1999 1:37a	357,648	A	0x00065CFB	0x00065CFB	x86	Win32 console
□	EXCEL.EXE	03/20/1999 5:54p	03/20/1999 5:49p	7,151,661	RAC	0x006DED66	0x006DED66	x86	Win32 GUI
□	GDI32.DLL	12/06/1999 11:00p	11/12/1999 2:44a	234,256	A	0x00046E78	0x00046E78	x86	Win32 console
□	KERNEL32.DLL	12/06/1999 11:00p	12/01/1999 1:37a	732,432	A	0x000BF812	0x000BF812	x86	Win32 console
□	MSO9.DLL	03/20/1999 11:09p	03/20/1999 10:28p	5,582,897	A	0x0056240D	0x0056240D	x86	Win32 GUI
□	NTDLL.DLL	12/06/1999 11:00p	10/27/1999 2:06p	481,040	A	0x0008454F	0x0008454F	x86	Win32 console
□	OLE32.DLL	12/06/1999 11:00p	12/01/1999 1:37a	989,456	A	0x000FF3B9	0x000FF3B9	x86	Win32 console

Figure 42-9
If an application depends on a missing or corrupted .dll file, Dependency Walker can pinpoint the problem.



```
D:\Program Files\Support Tools>filever filever.exe /v
--a-- W32i   APP ENU      5.0.2134.1 shp     13,584 12-01-1999 filever.exe
        Language        0x0409 (English (United States))
        CharSet         0x04b0 Unicode
        OleSelfRegister Disabled
        CompanyName     Microsoft Corporation
        FileDescription Microsoft Version Resource Dump Utility
        InternalName    filever.exe
        OriginalFilenam filever.exe
        ProductName     Microsoft(R) Windows (R) 2000 Operating System
        ProductVersion  5.00.2134.1
        FileVersion     5.00.2134.1
        LegalCopyright  Copyright (C) Microsoft Corp. 1981-1999

        VS_FIXEDFILEINFO:
        Signature:      feef04bd
        Struc Ver:      00010000
        FileVer:        00050000:08560001 (5.0:2134.1)
        ProdVer:        00050000:08560001 (5.0:2134.1)
        FlagMask:       0000003f
        Flags:          00000000
        OS:             00040004 NT Win32
        FileType:       00000001 App
        SubType:        00000000
        FileDate:       00000000:00000000

D:\Program Files\Support Tools>_
```

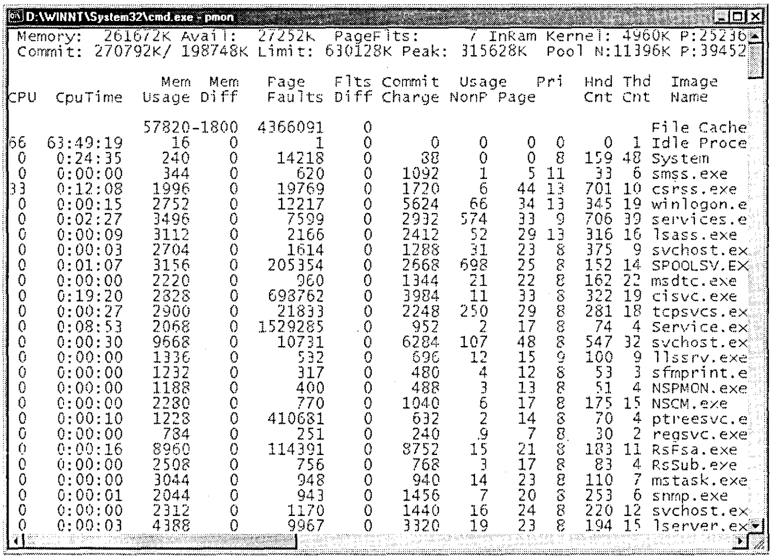
Figure 42-10
FileVer provides detailed version data about a selected executable or .dll.

Memory Profiling Tool (Memsnap.exe)

The memory profiling tool is a command-line utility that writes a snapshot of the memory resources used by all running processes to an ASCII log file. By default, the log file, named Memsnap.log, is written to the directory from which Memsnap is run. You can specify any file, however.

Process Resource Monitor (Pmon.exe)

Process Resource Monitor is a command-line utility that can help you find processes that are "leaking" memory (that is, that are not freeing up memory resources when those resources are no longer needed). The program reports memory resource usage for all running processes. Figure 42-11 shows an example of Pmon's output.



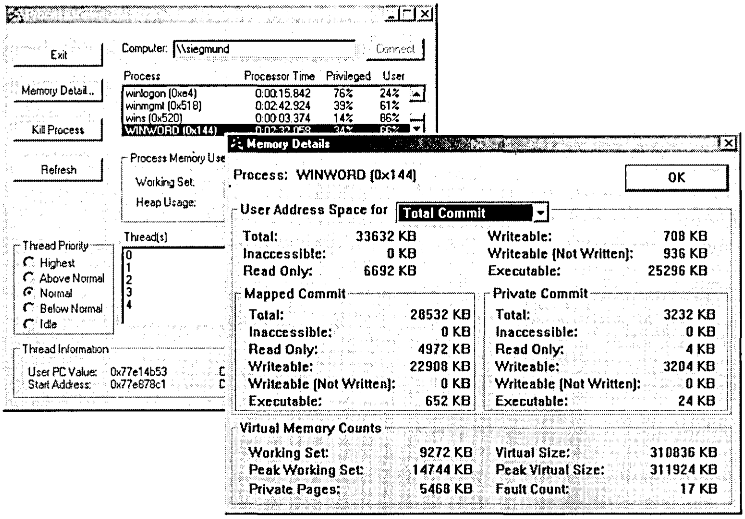
```
D:\WINNT\System32\cmd.exe - pmon
 Memory:   261672K Avail:   27252K  PageFlts:     7 InRam Kernel: 4960K P:25236
 Commit: 270792K/ 198748K Limit: 630128K Peak: 315628K  Pool N:11396K P:39452

                   Mem  Mem     Page  Flts Commit  Usage   Pri   Hnd Thd  Image
CPU  CpuTime     Usage Diff    Faults Diff Charge NonP Page      Cnt Cnt  Name

                 57820-1800   4366091    0                                File Cache
66   63:49:19       16    0         1    0      0    0    0  0     0   1  Idle Proce
 0    0:24:35      240    0     14218    0     38    0    0  8   159  48  System
 0    0:00:00      344    0       620    0   1092    1    5 11    33   6  smss.exe
33    0:12:08     1996    0     19769    0   1720    6   44 13   701  10  csrss.exe
 0    0:00:15     2752    0     12217    0   5624   66   34 13   345  19  winlogon.e
 0    0:02:27     3496    0      7599    0   2932  574   33  9   706  39  services.e
 0    0:00:09     3112    0      2166    0   2412   52   29 13   316  16  lsass.exe
 0    0:00:03     2704    0      1614    0   1288   31   23  8   375   9  svchost.ex
 0    0:01:07     3156    0    205354    0   2668  698   25  8   152  14  SPOOLSV.EX
 0    0:00:00     2220    0       960    0   1344   21   22  8   162  22  msdtc.exe
 0    0:19:20     2828    0    698762    0   3984   11   33  8   322  19  cisvc.exe
 0    0:00:27     2900    0     21833    0   2248  250   29  8   281  18  tcpsvcs.ex
 0    0:08:53     2068    0   1529285    0    952    2   17  8    74   4  Service.ex
 0    0:00:30     9668    0     10731    0   6284  107   48  8   547  32  svchost.ex
 0    0:00:00     1336    0       532    0    696   12   15  9   100   9  llssrv.exe
 0    0:00:00     1232    0       317    0    480    4   12  8    53   3  sfmprint.e
 0    0:00:00     1188    0       400    0    488    3   13  8    51   4  NSPMON.exe
 0    0:00:00     2280    0       770    0   1040    6   17  8   175  15  NSCM.exe
 0    0:00:10     1228    0    410681    0    632    2   14  8    70   4  ptreesvc.e
 0    0:00:00      784    0       251    0    240    9    7  8    30   2  regsvc.exe
 0    0:00:16     8960    0    114391    0   8752   15   21  8   183  11  RsFsa.exe
 0    0:00:00     2508    0       756    0    768    3   17  8    83   4  RsSub.exe
 0    0:00:00     3044    0       948    0    940   14   23  8   110   7  mstask.exe
 0    0:00:01     2044    0       943    0   1456    7   20  8   253   6  snmp.exe
 0    0:00:00     2312    0      1170    0   1440   16   24  8   220  12  svchost.ex
 0    0:00:03     4388    0      9967    0   3320   19   23  8   194  15  lserver.ex
```

Figure 42-11
Keeping an eye on the Commit Charge column in Pmon's display can help you pinpoint a program that leaks memory.

Monitoring the Commit numbers at the beginning of the second line of Pmon's display (above the columnar output) can help you determine whether you have a leaker. Constantly increasing numbers here suggest that a process is leaking memory. The process that is the culprit should also have increasing values in its Commit Charge column.

Process Viewer (Pviewer.exe)

Process Viewer shows information about each running process and allows you to terminate selected processes. As Figure 42-12 shows, the application includes a Memory Detail button that lets you see how any given process is using memory. The User Address Space For list in the Memory Details window lets you display total memory usage for a process or focus on a particular module used by a process.



Computer: \\siegmund

Process	Processor Time	Privileged	User
winlogon (0xe4)	0:00:15.842	76%	24%
winmgmt (0x518)	0:02:42.924	39%	61%
wins (0x520)	0:00:03.374	14%	86%
WINWORD (0x144)	0:02:32.058	34%	66%

Thread Information

User PC Value: 0x77e14b53

Start Address: 0x77e878c1

Memory Details

Process: WINWORD (0x144)

User Address Space for Total Commit

Total:	33632 KB	Writeable:	708 KB
Inaccessible:	0 KB	Writeable (Not Written):	936 KB
Read Only:	6692 KB	Executable:	25296 KB

Mapped Commit		Private Commit	
Total:	28532 KB	Total:	3232 KB
Inaccessible:	0 KB	Inaccessible:	0 KB
Read Only:	4972 KB	Read Only:	4 KB
Writeable:	22908 KB	Writeable:	3204 KB
Writeable (Not Written):	0 KB	Writeable (Not Written):	0 KB
Executable:	652 KB	Executable:	24 KB

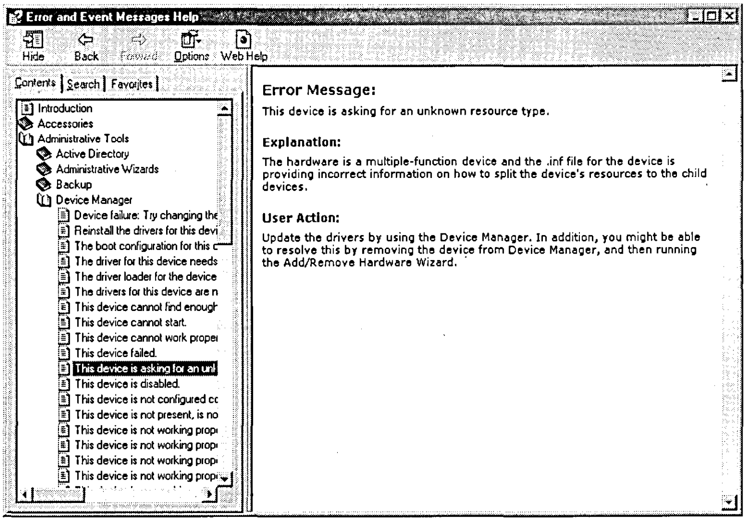
Virtual Memory Counts

Working Set:	9272 KB	Virtual Size:	310836 KB
Peak Working Set:	14744 KB	Peak Virtual Size:	311924 KB
Private Pages:	5468 KB	Fault Count:	17 KB

Figure 42-12
Process Viewer can tell you exactly how an application is using memory.

Windows 2000 Error And Event Messages Help (W2000msgs.chm)

This tool is not an application but a help file—an extremely useful help file. If you're mystified by a help message you receive in some corner of Windows 2000, try looking it up here. As Figure 42-13 shows, you can sometimes find clarity in the W2000msgs.chm document that is missing elsewhere.


Error and Event Messages Help
Hide
Back
Forward
Options
Web Help
Contents
Search
Favorites
Introduction
Accessories
Administrative Tools
Active Directory
Administrative Wizards
Backup
Device Manager
Device failure: Try changing the
Reinstall the drivers for this devi
The boot configuration for this c
The driver for this device needs
The driver loader for the device
The drivers for this device are n
This device cannot find enough
This device cannot start.
This device cannot work proper
This device failed.
This device is asking for an unl
This device is disabled.
This device is not configured cc
This device is not present, is no
This device is not working prop
This device is not working prop
This device is not working prop
This device is not working prop

Error Message:

This device is asking for an unknown resource type.

Explanation:

The hardware is a multiple-function device and the .inf file for the device is providing incorrect information on how to split the device's resources to the child devices.

User Action:

Update the drivers by using the Device Manager. In addition, you might be able to resolve this by removing the device from Device Manager, and then running the Add/Remove Hardware Wizard.

Figure 42-13
The Error And Event Messages Help file (W2000msgs.chm) can help you decrypt error messages.

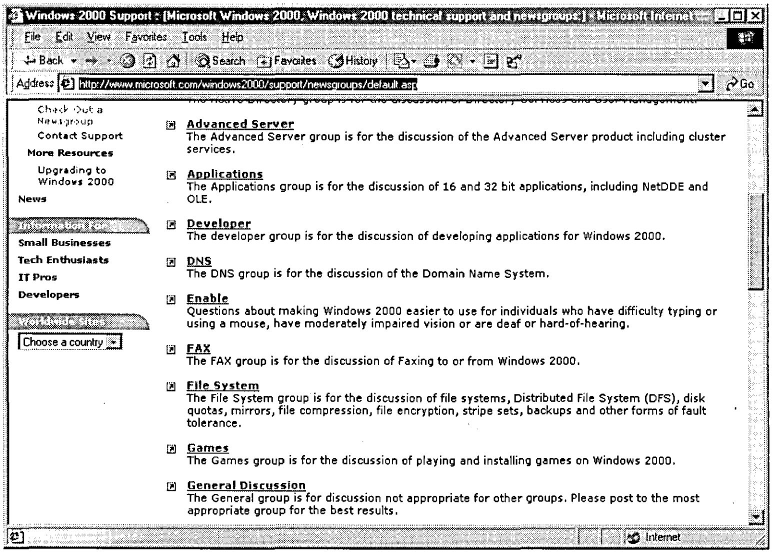
Troubleshooting Resources Available on the Internet

You can find a ton of information about Windows 2000 in the various pages that ramify from *www.microsoft.com/windows2000/default.asp,* the Windows 2000 home page. Much of what's there is from the marketing side of Microsoft, of course, but you'll find some useful troubleshooting resources as well.

Windows 2000 Newsgroups

Newsgroups can be an excellent source of troubleshooting information because they put you in touch with other highly motivated and intelligent users. Newsgroup subscribers might have solutions for problems that stump Microsoft's own product support personnel.

For a list of newsgroups focusing on Windows 2000 topics, visit *www.microsoft.com/windows2000/support/newsgroups/default.asp.* Clicking any of the links on this page launches Microsoft Outlook Express (or your default newsreader if it isn't Outlook Express) and makes it easy to subscribe to the group in question. (See Figure 42-14.) At the time of this writing, 29 newsgroups were available, on topics ranging from Active Directory to Windows Update.


Windows 2000 Support : [Microsoft Windows 2000, Windows 2000 technical support and newsgroups] - Microsoft Internet
File Edit View Favorites Tools Help
Back Search Favorites History
Go
Check Out a Newsgroup
Contact Support
More Resources
Upgrading to Windows 2000
News
Small Businesses
Tech Enthusiasts
IT Pros
Developers
Choose a country
Internet

Address: http://www.microsoft.com/windows2000/support/newsgroups/default.asp

Advanced Server
The Advanced Server group is for the discussion of the Advanced Server product including cluster services.

Applications
The Applications group is for the discussion of 16 and 32 bit applications, including NetDDE and OLE.

Developer
The developer group is for the discussion of developing applications for Windows 2000.

DNS
The DNS group is for the discussion of the Domain Name System.

Enable
Questions about making Windows 2000 easier to use for individuals who have difficulty typing or using a mouse, have moderately impaired vision or are deaf or hard-of-hearing.

FAX
The FAX group is for the discussion of Faxing to or from Windows 2000.

File System
The File System group is for the discussion of file systems, Distributed File System (DFS), disk quotas, mirrors, file compression, file encryption, stripe sets, backups and other forms of fault tolerance.

Games
The Games group is for the discussion of playing and installing games on Windows 2000.

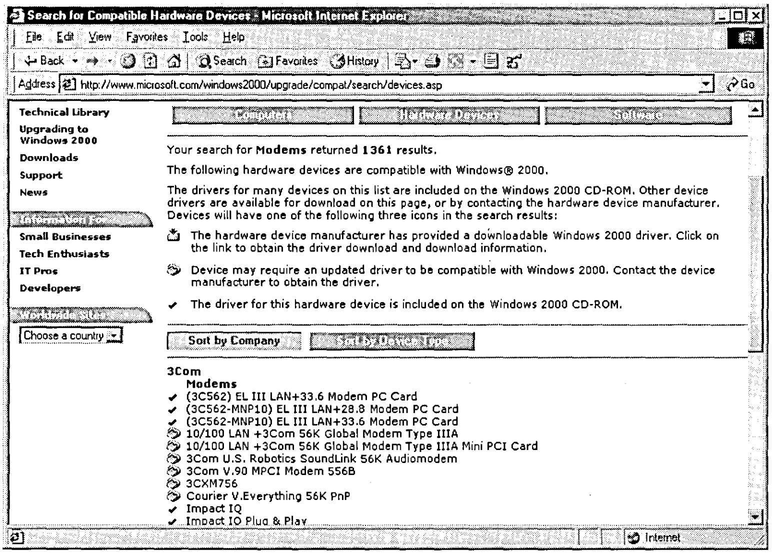
General Discussion
The General group is for discussion not appropriate for other groups. Please post to the most appropriate group for the best results.

Figure 42-14
Newsgroups offer a wealth of useful information from other users like you. This Web page provides a list of groups focusing on Windows 2000 topics.

The Hardware Compatibility List

If you install a device that doesn't work, be sure that the device is actually supported by Windows 2000. You can find out by going to *www.microsoft.com/windows2000/upgrade/compat/search/devices.asp*. Here you'll find three search fields—for company, model, and device type. To determine whether the device you already have is supported, fill out all three fields. To find out which devices in a particular class or from a certain vendor are supported, fill out just the relevant fields.

As Figure 42-15 shows, icons on the search results page divide supported devices into three categories: those for which a driver is available on the Windows 2000 CD, those for which a driver can be downloaded from the vendor's Web site, and those for which you must contact the vendor to obtain an updated (Windows 2000) driver.


Search for Compatible Hardware Devices - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.microsoft.com/windows2000/upgrade/compat/search/devices.asp
Go
Technical Library
Upgrading to Windows 2000
Downloads
Support
News
Small Businesses
Tech Enthusiasts
IT Pros
Developers
Choose a country
Computers
Hardware Devices
Software
Sort by Company
Sort by Device Type
Internet

Your search for **Modems** returned **1361** results.

The following hardware devices are compatible with Windows® 2000.

The drivers for many devices on this list are included on the Windows 2000 CD-ROM. Other device drivers are available for download on this page, or by contacting the hardware device manufacturer. Devices will have one of the following three icons in the search results:

⬇ The hardware device manufacturer has provided a downloadable Windows 2000 driver. Click on the link to obtain the driver download and download information.

↻ Device may require an updated driver to be compatible with Windows 2000. Contact the device manufacturer to obtain the driver.

✓ The driver for this hardware device is included on the Windows 2000 CD-ROM.

3Com
Modems
✓ (3C562) EL III LAN+33.6 Modem PC Card
✓ (3C562-MNP10) EL III LAN+28.8 Modem PC Card
✓ (3C562-MNP10) EL III LAN+33.6 Modem PC Card
↻ 10/100 LAN +3Com 56K Global Modem Type IIIA
↻ 10/100 LAN +3Com 56K Global Modem Type IIIA Mini PCI Card
↻ 3Com U.S. Robotics SoundLink 56K Audiomodem
↻ 3Com V.90 MPCI Modem 556B
↻ 3CXM756
↻ Courier V.Everything 56K PnP
✓ Impact IQ
✓ Impact IQ Plug & Play

Figure 42-15
This Web site provides the latest hardware compatibility information.

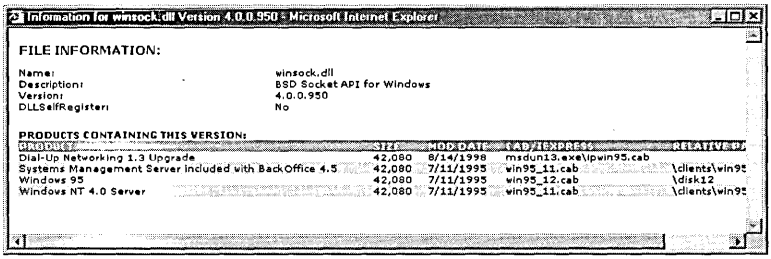
Note that the Windows 2000 CD includes a Hardware Compatibility List (\Support\Hcl.txt). The database on the Web, however, is likely to be more current.

The Microsoft Knowledge Base

The Microsoft Knowledge Base, *search.support.microsoft.com/kb*, is a comprehensive support database maintained by Microsoft's Product Support Services division. You can look here for answers regarding every product supported by the company. You can search by product, using keywords or free text. You can look for articles by their ID number (a six-digit number prefixed by the letter *Q*), look for a downloadable driver or other file, or simply search for all articles that have been added to the database during the most recent *n* days. Knowledge Base articles are often highly specific, dealing, for example, with particular hardware devices or software bugs. A number of Knowledge Base articles dealing with topics we've covered are included on the CD accompanying this book.

The DLL Help Database

If you're wondering whether a particular .dll file on the system is current—and where it came from if it's not—visit Microsoft's DLL Help Database, at *support.microsoft.com/servicedesks/fileversion/dllinfo.asp*. In the File Name search field, specify the name of the .dll you're wondering about. The database will return a list of version numbers for the specified file. Use the file's properties dialog box in Windows Explorer to determine the version number of your copy of the file. Click the link that matches the version number, and the database will return information about the file's possible sources. (See Figure 42-16.) You can look for .exe files as well as .dll files in the DLL Help Database.


Information for winsock.dll Version 4.0.0.950 - Microsoft Internet Explorer

FILE INFORMATION:

Name:	winsock.dll
Description:	BSD Socket API for Windows
Version:	4.0.0.950
DLLSelfRegister:	No

PRODUCTS CONTAINING THIS VERSION:

PRODUCT(S)	SIZE	MOD DATE	CAB/IEXPRESS	RELATIVE P
Dial-Up Networking 1.3 Upgrade	42,080	8/14/1998	msdun13.exe\ipwin95.cab	
Systems Management Server included with BackOffice 4.5	42,080	7/11/1995	win95_11.cab	\clients\win95
Windows 95	42,080	7/11/1995	win95_12.cab	\disk12
Windows NT 4.0 Server	42,080	7/11/1995	win95_11.cab	\clients\win95

Figure 42-16
You can use the DLL Help Database to find out where that old version of Winsock (or another .dll or executable) on your system came from.

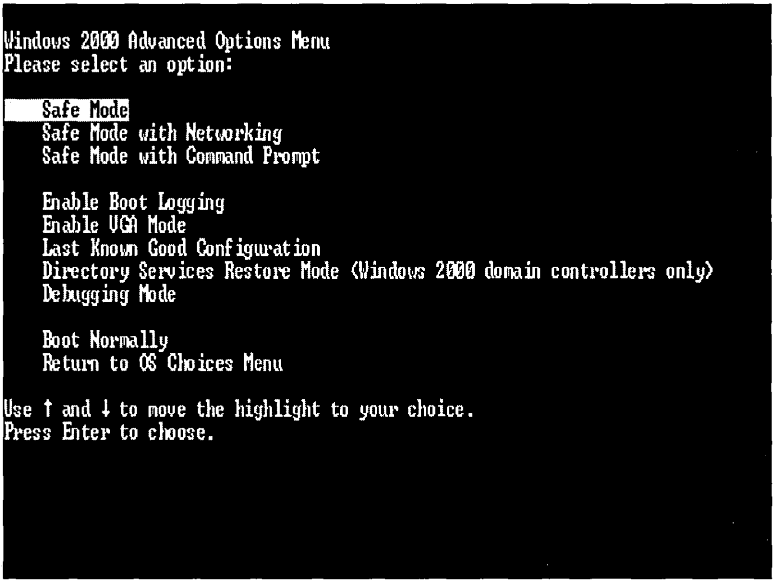
What to Do If Your System Won't Start

If your system refuses to start, you can try the following:

- Start the system in one of the three safe modes.
- Start the system with the Last Known Good Configuration option.
- Use Recovery Console.
- Use the emergency repair disk (ERD).

Starting in a Safe Mode

To start your system in one of the safe modes, press F8 immediately after your computer finishes its power-on self test (POST). The Advanced Options menu, shown in Figure 42-17, appears.



```
Windows 2000 Advanced Options Menu
Please select an option:

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable VGA Mode
    Last Known Good Configuration
    Directory Services Restore Mode (Windows 2000 domain controllers only)
    Debugging Mode

    Boot Normally
    Return to OS Choices Menu

Use ↑ and ↓ to move the highlight to your choice.
Press Enter to choose.
```

Figure 42-17
To start in safe mode, press F8 after the POST and choose one of the first three options on this menu.

Safe mode is useful if your system files are uncorrupted and you suspect a faulty device driver. The operating system starts with a minimal set of drivers and services, using the generic VGA driver at 640×480×16 colors. You get support only for your keyboard, mouse, monitor, and local storage. (The second option on the Advanced Options menu, Safe Mode With Networking, also installs your network but does not install PC Card support.) If the operating system appears to function well in this mode, you can assume that you don't have a problem with these basic services, and you can use Device Manager and Event Viewer to try to figure out where the trouble lies. If you suspect a newly installed device, use Device Manager to remove it. Then try a normal restart.

Note that the third option on the Advanced Options menu, Safe Mode With Command Prompt, is the same as the first, except that it puts you in a Cmd.exe session instead of on the desktop. To quit from here, press Ctrl+Alt+Delete and choose Shut Down. Alternatively, you can type *start explorer* to get back to the Windows desktop and then use the Start menu to shut down.

Starting with Last Known Good Configuration

The Last Known Good Configuration option on the Advanced Options menu (shown in Figure 42-17) starts your system normally (that is, not in safe mode) but restores to HKLM\System\CurrentControlSet the control set data pointed to by the LastKnownGood value of HKLM\System\Select.

Control set data includes system configuration information, such as the names of device drivers and services that should be loaded and started when Windows 2000 starts. Your system has at least two and possibly more control set subkeys of HKLM\System, identified as ControlSet001, ControlSet002, and so on. One of those ControlSet*nnn* keys is always linked to HKLM\System\CurrentControlSet. When you start successfully, the control set data used at startup is cloned, and the LastKnownGood value of HKLM\System\Select is set to point to the clone. If you make changes to your hardware, device drivers, or services, those changes are reflected in HKLM\System\CurrentControlSet (and the ControlSet*nnn* to which it is linked). To "undo" those changes, you can start with the Last Known Good Configuration option.

You should try starting with the Last Known Good Configuration option if you install a new device or driver and the system stops responding, or if you accidentally delete or disable a critical device driver. You can also try this option if you install a new video driver and your screen goes blank, although in this case starting in safe mode would also be effective, since safe mode starts your system with the generic VGA driver.

Other Advanced Options

When you start in one of the three safe modes, Windows 2000 records a log of all the drivers and services that are loaded or not loaded. The information is stored in %SystemRoot%\Ntbtlog.txt. To start normally and generate the log, choose Enable Boot Logging from the Advanced Options menu.

In the safe modes, Windows 2000 starts with the plain-vanilla generic VGA driver. To get a normal start using this driver, choose Enable VGA Mode from the Advanced Options menu.

If you choose Debugging Mode, Windows 2000 starts normally but records debugging information that can be sent through a serial cable to another computer.

Microsoft says the Directory Services Restore Mode is "not applicable for Windows 2000 Professional," but the option is there on Pro systems nonetheless. Choosing it causes Windows to perform a character-mode disk check before launching in a mode that resembles (but is not identical to) Safe Mode With Networking.

Using Recovery Console

Recovery Console is a character-mode miniature version of Windows 2000 that lets you perform the following tasks:

- Use, copy, rename, or replace operating-system files and folders.
- Enable or disable services or devices. (These changes take effect the next time you start Windows 2000.

- Repair the file-system boot sector or the master boot record (MBR).
- Create and format partitions.

For the sake of security, Recovery Console allows you to log on only if you can supply the password for the Administrator account to use Recovery Console. And, unless you change the AllowRemovableMedia environment variable from False to True—an option that can be enabled only via the Security Configuration And Analysis snap-in—Recovery Console does not permit you to copy files from fixed to removable media.

If you have installed Recovery Console as a boot option, you can run Recovery Console simply by turning on your system and choosing Windows 2000 Recovery Console from the menu that appears after your computer completes its power-on self test. *(For more information, see "Installing Recovery Console as a Boot Option," page 690.)* If you have not set up Recovery Console this way, you can run it as follows:

1. Start your computer with the Windows 2000 Setup floppy disks or the Windows 2000 CD (if your computer can boot from a CD).
2. At the Welcome to setup screen, press F10. Or press R to Repair, and then C to start Recovery Console.

You will be asked to specify which installation of "Windows NT" you want to log on to. If you have only one installation of Windows 2000 on your computer, you'll see a menu offering a single choice, of the form *D*:\WINNT, where *D* is a drive letter. After you make your selection, you'll be required to supply the password for the Administrator account. If you don't enter this password correctly, you'll get two more chances. After three incorrect passwords, Recovery Console quits.

After you've logged on to Recovery Console, you can type *help* to get a list of the available commands, and you can use the /? switch after a command name to learn its syntax. Although many of Recovery Console's commands have counterparts in Cmd.exe (and MS-DOS), they typically do not include the same options (switches) as Cmd, and they do not accept wildcard specifications. Also be aware that all file-management and folder-management commands work only within the system folders of the current Windows 2000 installation, removable media, the root folder of any hard disk partition, and the local installation sources. Table 42-1 lists the commands available in Recovery Console.

Table 42-1. Commands Available in Recovery Console

Command	Effect
Attrib	Sets or clears attributes for files or folders
Cd and Chdir	Changes folders
Chkdsk	Checks and, if needed, repairs or recovers a drive; marks bad sectors and recovers readable information
Cls	Clears the screen
Copy	Copies a file
Del and Delete	Deletes a file
Dir	Displays folder contents and attributes
Disable	Disables a service or driver
Diskpart	Manages the partitions on hard disk volumes
Enable	Enables a service or driver
Exit	Leaves Recovery Console and restarts the computer
Extract	Extracts a file from the driver .cab file on the installation media and copies it to the destination
Fixboot	Writes new Windows 2000 boot-sector code on the boot partition
Fixmbr	Repairs the master boot record of the system partition
Format	Formats the specified drive to the specified file system
Listsvc	Lists all available services, drivers, and their current start types
Logon	Lists all detected installations of Windows 2000 and Windows NT and requests an Administrator password for the installation you want to log on to
Map	Lists drive letters, file-system types, partition sizes, and mappings to physical devices
Md and Mkdir	Makes folders
More	Displays a text file, pausing at each screenful
Rd and Rmdir	Removes folders
Ren and Rename	Renames a file
Set	Displays or modifies four variables: AllowWildCards, AllowAllPaths, AllowRemovableMedia, NoCopyPrompt
Systemroot	Sets the current folder to the %SystemRoot% folder of the current Windows 2000 installation
Type	Displays a text file

Note the following about Recovery Console commands:

- If you copy a compressed file from the Windows 2000 CD to your hard disk, the file is automatically expanded.
- The Extract command works only if you have started your computer from the Windows 2000 CD.
- You can use the Fixboot command to repair boot-sector code. Alternatively, you can do this via the emergency repair process (the recovery measure that uses your ERD).
- Microsoft strongly recommends that you run antivirus software before trying to fix the MBR with the Fixmbr command. Using Fixmbr when a virus is present or a hardware problem exists can damage your partition tables and make partitions inaccessible.
- You can use the Set command to change environment variables only if you have enabled this option by means of the Security Configuration And Analysis snap-in.

Using the Emergency Repair Disk

The emergency repair process (the recovery measure that uses your ERD) can help you do the following:

- Repair problems with system files
- Repair problems with your startup environment, if you have a dual-boot or multiboot system
- Repair the partition boot sector on your boot volume

According to Microsoft, the emergency repair process might be able to solve some of these problems, even if you haven't created an ERD, but certain changes that you've made to your system since the initial setup (including any service packs you've installed) will not be restored.

To avail yourself of the emergency repair process:

1. Start your computer from the Windows 2000 CD (if you can boot from a CD) or from the Windows 2000 Setup disks.
2. You'll be asked whether you want to continue installing Windows 2000. Answer yes.
3. You'll be asked whether you want to do a full install or repair an existing installation. Choose the latter (by pressing R).
4. Indicate whether you want to perform a "fast repair" or a "manual repair."
5. Insert the ERD when prompted.

A fast repair requires no further decisions from you. The repair process attempts to fix your system files, the boot sector, and your startup environment. If your registry appears to be damaged, the fast repair process restores the copy of your registry that the Setup program created when you first installed Windows 2000. (If your registry does not appear to be damaged, the fast repair process does not change it.) It does not restore your own profile settings—the portion of the registry stored in the file Ntuser.dat. If that part of your registry is still in good shape, your personal settings will still be intact. The rest of the registry, however, will revert to the condition it was in the day you installed Windows 2000. If you have had the foresight to create a backup of your registry (via the System State option in Ntbackup or the equivalent in another backup program), you'll be able to use that backup to restore the registry to a more current condition.

A manual repair lets you choose whether you want to repair the system files, the boot sector, or the startup environment (or any combination of those), but it doesn't let you do anything with the registry.

Chapter 43

Monitoring System Performance

In This Chapter

Monitoring Performance and Managing Applications with Windows Task Manager 714

Monitoring and Logging Performance with the Performance Console 722

What to Monitor 735

Whether you're in charge of a single workstation or an entire network, it's always possible that the imps of electronics will suddenly start gobbling memory, blocking communication lines, causing gridlock on a hard disk, or producing pandemonium on the data bus. At such a time, you might wish you could dive into the system to take an up-close look at what's going on. You can't. But with Microsoft Windows 2000, you can check on what the computer system is doing. You can then put aside a lot of guesswork and base corrective actions on fact.

In this chapter, we look at Windows Task Manager and the Performance console, two tools that provide a wealth of information about what's going on in your system. Windows Task Manager lets you see which applications and processes are running at the current moment, along with information about how much memory each process is using, how many page faults it's experiencing (a *page fault* occurs when a process needs data that's not currently in its working set—the physical memory visible to the process), how many input/output (I/O) operations it's performing, and more. (A *process* is anything that runs in its own address space. That includes applications, services, and subsystems.)

Windows Task Manager has a dual personality. It's a useful and simple performance monitor. But, as its name implies, it's also a tool for managing whatever is running on your system, allowing you to do the following:

- Start and stop applications and processes. (You can use it, for example, to terminate applications that have stopped responding to the system.)
- Switch between running applications.
- Tile and cascade windows.
- Assign a process to a particular processor (on a multiprocessor system).
- Change the base priority class of a process.
- Activate a debugger, if you have one.

Some of the performance data points offered by Windows Task Manager are cumulative. The CPU Time and Page Faults columns on the Processes tab, for example, tell you the total amount of CPU time used and the total number of page faults caused by a process since that process began running. Information presented by the graphic component of Windows Task Manager (on the Performance tab), on the other hand, is ephemeral. If you set the update speed to Low and maximize the Performance tab on a 1600×1200 screen, you can see a CPU usage chart covering the most recent 8 minutes of your system's history. To track your system's behavior over a longer time interval, you need the far more extensive monitoring services provided by the Performance console.

With the Performance console, you can monitor a great many statistics not available via Windows Task Manager. You can also log performance data to disk files for subsequent analysis, export data to programs such as Microsoft Excel, set "alerts" that cause Windows 2000 to take specified actions when performance thresholds are crossed, and monitor remote systems as well as your local machine. With the Performance console, you can also record performance data when someone else is using your computer.

The Performance console is the successor to the Windows NT Performance Monitor. Like other Windows NT administrative tools, it has been transformed into a Microsoft Management Console (MMC) snap-in in Windows 2000.

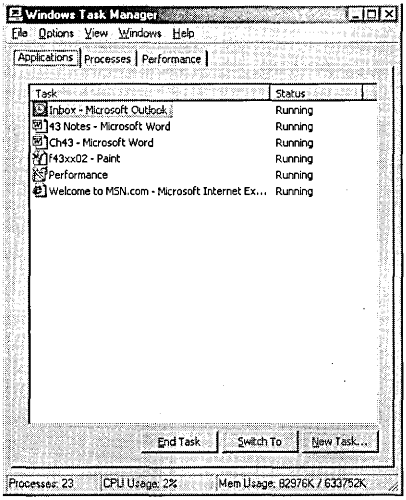
Monitoring Performance and Managing Applications with Windows Task Manager

You can start Windows Task Manager in any of the following ways:

- Right-click an unoccupied area of the taskbar and choose Task Manager from the shortcut menu.
- Press Ctrl+Shift+Esc.
- Press Ctrl+Alt+Delete, and then click Task Manager.
- Type *taskmgr* at a command prompt.

To close Windows Task Manager, you can simply press Esc.

As Figure 43-1 shows, Windows Task Manager consists of three tabs: Applications, Processes, and Performance. A status bar at the bottom of the window, visible on all three tabs, displays the number of processes that are currently running, the percentage of your CPU's processing capacity that's currently being used to execute nonidle threads, and some information about the amount of your system's memory that's currently in use. This last statistic, Mem Usage, is presented as a fraction. The numerator represents your current total *commit charge*—the amount of virtual memory in use by all running processes. (*Virtual memory* is memory backed by your paging, or swap, file.) The denominator represents your total available virtual memory. You can find more details about your current memory usage on the Performance tab.



Task	Status
Inbox - Microsoft Outlook	Running
43 Notes - Microsoft Word	Running
Ch43 - Microsoft Word	Running
f43xx02 - Paint	Running
Performance	Running
Welcome to MSN.com - Microsoft Internet Ex...	Running

Processes: 23 CPU Usage: 2% Mem Usage: 82976K / 633752K

Figure 43-1
The Applications tab in Windows' Task Manager lets you check the status of running programs.

By default, Windows Task Manager updates its data once every second. To increase the frequency to twice per second, choose View | Update Speed | High. To reduce the frequency to once every 4 seconds, choose View | Update Speed | Low. To freeze the display, choose View | Update Speed | Paused. At any frequency, you can force an immediate update by choosing View | Refresh Now.

Troubleshooting

If Windows Task Manager appears without any of the usual adornments—including the title bar, menu bar, tabs, and status bar—don't fret. It's all too easy to inadvertently switch to this lean look, and you must know the secret to return to the normal view: simply double-click anywhere in the window's background (that is, anywhere except within the list box that fills most of the window). And if you want to switch to the minimalist view, double-click anywhere between the menu bar and the status bar except within a control on the tab.

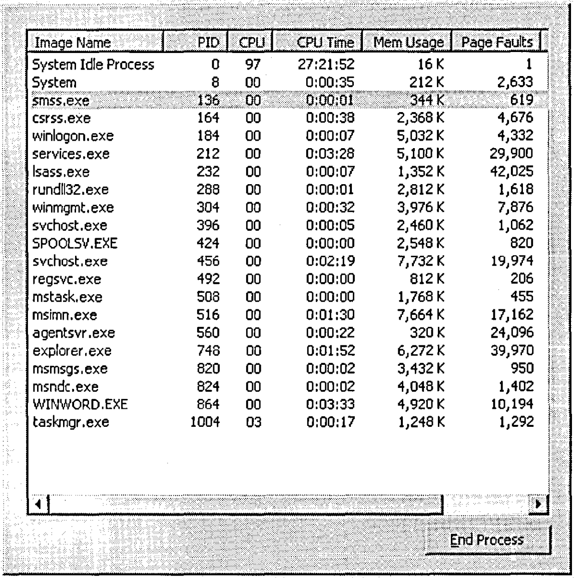


Image Name	PID	CPU	CPU Time	Mem Usage	Page Faults
System Idle Process	0	97	27:21:52	16 K	1
System	8	00	0:00:35	212 K	2,633
smss.exe	136	00	0:00:01	344 K	619
csrss.exe	164	00	0:00:38	2,368 K	4,676
winlogon.exe	184	00	0:00:07	5,032 K	4,332
services.exe	212	00	0:03:28	5,100 K	29,900
lsass.exe	232	00	0:00:07	1,352 K	42,025
rundll32.exe	288	00	0:00:01	2,812 K	1,618
winmgmt.exe	304	00	0:00:32	3,976 K	7,876
svchost.exe	396	00	0:00:05	2,460 K	1,062
SPOOLSV.EXE	424	00	0:00:00	2,548 K	820
svchost.exe	456	00	0:02:19	7,732 K	19,974
regsvc.exe	492	00	0:00:00	812 K	206
mstask.exe	508	00	0:00:00	1,768 K	455
msimn.exe	516	00	0:01:30	7,664 K	17,162
agentsvr.exe	560	00	0:00:22	320 K	24,096
explorer.exe	748	00	0:01:52	6,272 K	39,970
msmsgs.exe	820	00	0:00:02	3,432 K	950
msndc.exe	824	00	0:00:02	4,048 K	1,402
WINWORD.EXE	864	00	0:03:33	4,920 K	10,194
taskmgr.exe	1004	03	0:00:17	1,248 K	1,292

Using the Applications Tab

The Applications tab lists all running applications. The entries you see here are approximately the same as the ones presented by the Windows Alt+Tab task switcher. For example, the Applications tab shown in Figure 43-1 lists Microsoft Outlook, the Performance console (identified simply as Performance), Paint, Microsoft Internet Explorer, and so on; if these items were running on your system, you could see this same list by holding down the Alt and Tab keys. Like the Alt+Tab task switcher, the Applications tab of Windows Task Manager displays document names as well as the names of the applications that have opened those documents.

Along with the applications just cited, Figure 43-1 also shows two Microsoft Word instances—one with the file 43 Notes, another with the file Ch43. That's because Word 2000 has been designed to fool the operating system into thinking that multiple documents are actually multiple instances of the Word application itself. You would see the same two instances of Word if you pressed Alt+Tab, but an examination of the Processes tab (shown later in Figure 43-2, in the following section) would reveal that a single Winword process was responsible for both Word instances.

The correspondence between the application list presented by Windows Task Manager and the one presented by the Alt+Tab task switcher is not exact. Windows Task Manager, for example, never appears on its own Applications tab (although the process Taskmgr.exe does show up on the Processes tab).

In Details view (Windows Task Manager's default), the Applications tab includes a handy Status column. If an application locks up for any reason, the words *Not Responding* appear in this column. You can terminate the miscreant by selecting it and clicking End Task. Be aware, though, that the indication Not Responding does not necessarily mean that an application is down for the count. It simply means that Windows Task Manager cannot currently communicate with it. Before you call for the stretcher, make sure that your program isn't simply busy with some task that can't be interrupted.

When you shut down an application by clicking End Task on the Applications tab, the application goes through its normal quitting routine if it can, prompting you for confirmation or to save work if appropriate. So it's perfectly safe to shut down running programs this way. The analogous button on the Processes tab (End Process) liquidates the selected item forthwith and hence is to be avoided unless no alternative exists.

The other buttons on the Applications tab allow you to switch to a selected application and start a new task. Clicking New Task is equivalent to choosing Start | Run; the button and the command share a common most recently used (MRU) list.

To tile or cascade a group of applications using Windows Task Manager, select the applications. (Hold down Shift while selecting adjacent entries or Ctrl while selecting ones that are not adjacent.) Then select one of the window-management commands from the shortcut menu—Cascade, Tile Horizontally, or Tile Vertically.

To get information about the process that's responsible for an application, right-click it on the Applications tab and choose Go To Process from the shortcut menu. These actions transport you to the Processes tab, where you can learn the name—and many other attributes—of the process in question.

Using the Processes Tab

The Processes tab, shown in Figure 43-2, lists all currently running processes. As you can see, most of them are .exe files. You can see the same list in the System Information console. (Choose Software Environment\Running Tasks in the console tree.) But the System Information console and Windows Task Manager provide different information. System Information tells you the path, version, size, and file date of each process. Windows Task Manager provides performance data.

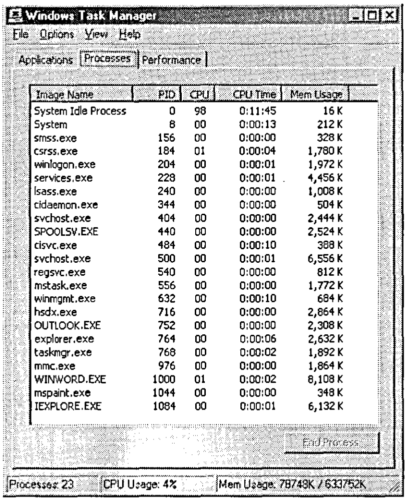


Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	98	0:11:45	16 K
System	8	00	0:00:13	212 K
smss.exe	156	00	0:00:00	328 K
csrss.exe	184	01	0:00:04	1,780 K
winlogon.exe	204	00	0:00:01	1,972 K
services.exe	228	00	0:00:01	4,456 K
lsass.exe	240	00	0:00:00	1,008 K
cidaemon.exe	344	00	0:00:00	504 K
svchost.exe	404	00	0:00:00	2,444 K
SPOOLSV.EXE	440	00	0:00:00	2,524 K
cisvc.exe	484	00	0:00:10	388 K
svchost.exe	500	00	0:00:01	6,556 K
regsvc.exe	540	00	0:00:00	812 K
mstask.exe	556	00	0:00:00	1,772 K
winmgmt.exe	632	00	0:00:10	684 K
hsdx.exe	716	00	0:00:00	2,864 K
OUTLOOK.EXE	752	00	0:00:00	2,308 K
explorer.exe	764	00	0:00:06	2,632 K
taskmgr.exe	768	00	0:00:02	1,892 K
mmc.exe	976	00	0:00:00	1,864 K
WINWORD.EXE	1000	01	0:00:02	8,108 K
mspaint.exe	1044	00	0:00:00	348 K
IEXPLORE.EXE	1084	00	0:00:01	6,132 K

Processes: 23 | CPU Usage: 4% | Mem Usage: 78748K / 633752K

Figure 43-2
The Processes tab in Windows Task Manager provides information about your processes' memory and CPU usage in addition to many other details.

For each process, Windows Task Manager includes the following information by default: Image Name (the name of the process), PID (process identifier, the number by which the process is known to the operating system), CPU (the percentage of your central processing unit's capacity that the process is currently using), CPU Time (the total amount of time that your CPU has been occupied with the process since the process began running), and Mem Usage (the size of the process's working set). If you add up the figures in the Mem Usage column, you'll notice that the total comes up quite a bit short of the Mem Usage figure that appears in Windows Task Manager's status bar. That's because the latter figure is actually the commit charge total, not the working set total.

Processes are sorted initially by their PIDs. You can sort by any other column by clicking the column heading. (Click a second time to change the sort from ascending to descending, or vice versa.) If you sort in descending order on the CPU column, you will probably find that the System Idle Process occupies most of your CPU's time. That is, on most users' systems, the CPU spends the greatest share of its day doing nothing.

Sorting on descending order by CPU can sometimes help you figure out what's going on "in the background" on your computer. If you're curious, for example, about what process is rattling your hard disk while you're just sitting there staring at your screen, check the CPU column when this happens.

The Processes tab can provide a great many statistics in addition to the ones shown by default. To add data to the tab, choose View | Select Columns. (You can also use this command to remove any of the default columns other than Image Name.) When you have displayed the columns you want, you can rearrange them by dragging column headings to the left or right.

Changing a Process's Base Priority

A process's base priority is a ranking category that governs the order in which that process's threads are scheduled for execution, relative to the threads of other processes. You can see the base priority of your processes by choosing View | Select Columns and selecting Base Priority. You can also change the base priority of a process. To do this, right-click the process's name and choose Set Priority. As Figure 43-3 shows, the six available priority settings appear on a submenu.

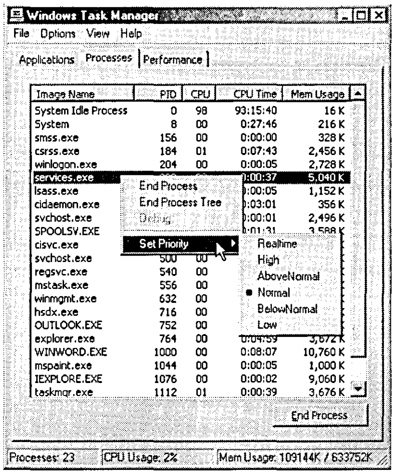


Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	98	93:15:40	16 K
System	8	00	0:27:46	216 K
smss.exe	156	00	0:00:00	328 K
csrss.exe	184	01	0:07:43	2,456 K
winlogon.exe	204	00	0:00:05	2,728 K
services.exe			:00:37	5,040 K
lsass.exe			:00:05	1,152 K
cidaemon.exe			:03:01	356 K
svchost.exe			:00:01	2,496 K
SPOOLSV.EXE			:01:31	3,588 K
cisvc.exe				
svchost.exe	500	00		
regsvc.exe	540	00		
mstask.exe	556	00		
winmgmt.exe	632	00		
hsdx.exe	716	00		
OUTLOOK.EXE	752	00		
explorer.exe	764	00	0:04:59	3,672 K
WINWORD.EXE	1000	00	0:08:07	10,760 K
mspaint.exe	1044	00	0:00:05	1,000 K
IEXPLORE.EXE	1076	00	0:00:02	9,060 K
taskmgr.exe	1112	01	0:00:39	3,676 K

Processes: 23 CPU Usage: 2% Mem Usage: 109144K / 633752K

Figure 43-3
The Set Priority command, which is available only on this shortcut menu, lets you override a process's default base priority.

Because a process's base priority is set by its program code, any changes you make via Windows Task Manager remain in effect for the current session only. If you always want to run an application at a priority level other than its default, you can create a shortcut that uses the Start command to launch the application. As you can see by typing *start /?* in a Command Prompt window, the Start command provides arguments that let you run a program at a specified priority level.

Using Windows Task Manager to Terminate a Process

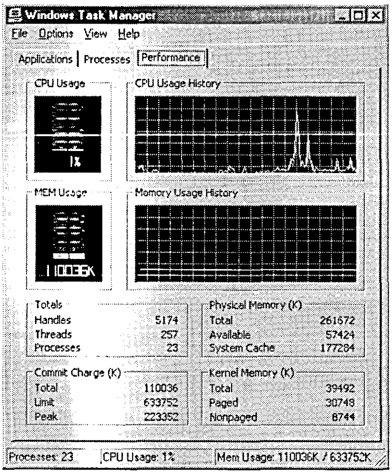
You can end any process by selecting it on the Processes tab and clicking End Process. Because this action terminates the selected process immediately, without allowing the process to go through its normal shutdown routine, Windows Task Manager presents a confirmation prompt before carrying out your order.

Changing Processor Affinity

On a multiprocessor system, you can assign a process to a particular processor by right-clicking it and choosing Set Affinity from the shortcut menu. This command does not appear on the shortcut menu on single-processor systems.

Using the Performance Tab

The Performance tab, shown in Figure 43-4, provides four graphs and some tabular data. The CPU Usage and Mem Usage graphs display the percentage of your CPU's processing capacity and your system's virtual memory capacity in use as of Windows Task Manager's most recent update. The CPU Usage History and Memory Usage History sections provide line graphs of the same performance measures over time. By default, the CPU graphs chart user-mode activities only. To include kernel-mode operations (critical operating-system components run in kernel mode), choose View | Show Kernel Times. Kernel-mode data then appears in red.



Totals
Handles 5174
Threads 257
Processes 23

Physical Memory (K)
Total 261672
Available 57424
System Cache 177284

Commit Charge (K)
Total 110036
Limit 633752
Peak 223352

Kernel Memory (K)
Total 39492
Paged 30748
Nonpaged 8744

Processes: 23 | CPU Usage: 1% | Mem Usage: 110036K / 633752K

Figure 43-4
The Performance tab lets you see at a glance how much of your system's memory is in use.

How much history the history graphs record depends on Windows Task Manager's current update speed and the width of its window. Each vertical gridline in these graphs represents one update interval. If you widen the window, you get more gridlines and see more history.

On the vertical axis, all four graphs are scaled from 0 to 100 percent. Increasing the height of the window simply expands the axis without changing its end points, making the graphs easier to read. Double-clicking anywhere within the Windows Task Manager window—on the graphs themselves or the surrounding matter—removes everything but the CPU Usage and CPU Usage History graphs, allowing you to see more detail without expanding the window itself. With the window thus altered, you can still move to the Processes and Applications tabs by pressing Ctrl+Tab. To return Windows Task Manager to its normal display, double-click again.

The remainder of the Performance tab provides some "snapshot" statistics about the current state of your computer's memory. The most useful numbers to watch here are Available Physical Memory and Peak Commit Charge.

Available Physical Memory tells you how much memory is left over after all running processes and the system cache have been serviced. (The system cache is an area of random access memory that holds frequently used data. The cache improves your system's performance by enabling processes to retrieve data from memory that would otherwise have to be fetched from disk.) A gradually dropping value for Available Physical Memory with no change in the running processes can indicate that a process is "leaking" memory. *(For more about finding leaking processes, see "Monitoring for a Memory Leak," page 736.)*

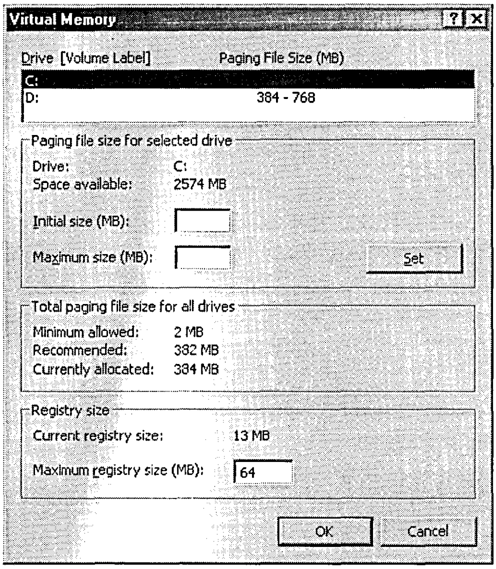
Peak Commit Charge records the maximum amount of paging-file-backed memory that your system has committed to its running applications during the time that Windows Task Manager has been running. If this figure exceeds 70 percent of the Limit Commit Charge (which is the total amount of your system's virtual memory), you should consider increasing the size of your paging file.

Adjusting the Size of Your Paging File

To change the size of your paging file, log on using an administrative account and choose Start | Settings | Control Panel | System. On the Advanced tab, click Performance Options, and then Change, to arrive at the Virtual Memory dialog box, shown in Figure 43-5. The dialog box shows the current size and location of your paging file(s).

Windows 2000 Professional, by default, creates a single paging file on the boot volume, setting that file's size to 1.5 times the amount of memory in the system and allowing the file to expand, when necessary, to twice its original size. The system depicted in Figure 43-5 has its original, default, paging file.

Using the Virtual Memory dialog box, you can adjust the minimum and maximum size of your paging file (to a limit of 4095 MB per paging file). You can also relocate the file to a different volume or create additional paging files. (You can have one on each logical volume.) Spreading your paging-file space across multiple volumes can enhance performance by allowing your system to process multiple I/O requests concurrently.



Virtual Memory

Drive [Volume Label]	Paging File Size (MB)
C:	
D:	384 - 768

Paging file size for selected drive

Drive: C:

Space available: 2574 MB

Initial size (MB):

Maximum size (MB):

Total paging file size for all drives

Minimum allowed: 2 MB

Recommended: 382 MB

Currently allocated: 384 MB

Registry size

Current registry size: 13 MB

Maximum registry size (MB): 64

Figure 43-5
You can use this dialog box to change the size or location of your paging file.

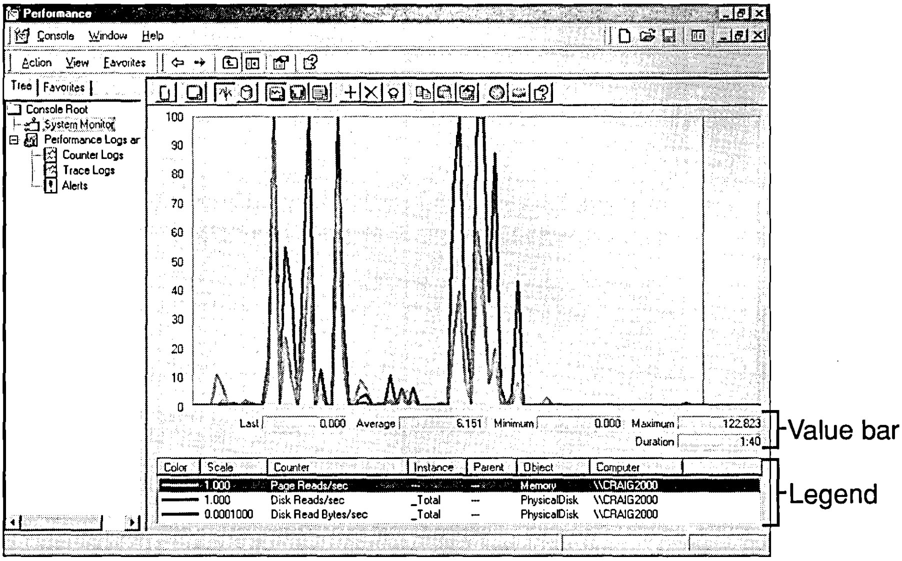
Monitoring and Logging Performance with the Performance Console

To run the Performance console, choose either Start | Programs | Administrative Tools | Performance or Start | Settings | Control Panel | Administrative Tools | Performance. Alternatively, type *perfmon.msc* at a command prompt.

The Performance console, shown in Figure 43-6, has two components: System Monitor and Performance Logs And Alerts. The latter is subdivided into Counter Logs, Trace Logs, and Alerts. System Monitor provides graphical or textual information about your system's current state and recent history. Performance Logs And Alerts lets you track your system over longer periods of time, recording data in disk files for subsequent analysis. You can use the Alerts section of Performance Logs And Alerts to indicate actions that your computer should take if performance measures meet specified thresholds.

The Performance Logs And Alerts section of the Performance console is also available as a component of the Computer Management console. In addition, you can snap it into your own MMC consoles. Adding the System Monitor component to a custom console is a little more complicated:

1. In MMC, choose Console | Add/Remove Snap-In.
2. In the Add/Remove Snap-In dialog box, click Add.



Last 0.000 Average 6.151 Minimum 0.000 Maximum 122.823
Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
———	1.000	Page Reads/sec	---	---	Memory	\\CRAIG2000
———	1.000	Disk Reads/sec	_Total	---	PhysicalDisk	\\CRAIG2000
———	0.0001000	Disk Read Bytes/sec	_Total	---	PhysicalDisk	\\CRAIG2000

Figure 43-6
The System Monitor component of the Performance console can provide graphical information about your system's current and recent status.

3. In the Add Standalone Snap-In dialog box, select ActiveX Control and click Add. This launches the Insert ActiveX Control Wizard.
4. Click Next on the wizard's first page.
5. On the wizard's second page, select System Monitor Control in the Control Type list and then click Next.
6. Click Finish to close the wizard, click Close to close the Add Standalone Snap-In dialog box, and click OK to close the Add/Remove Snap-In dialog box.

Objects, Counters, and Instances

The Performance console can track everything from relatively mundane but critical activities, such as processor time and disk access, to more exotic items, such as the number of nonpaging read bytes per second handled by the network redirector. Whatever you decide to track, you specify it to the Performance console in the form of an object and a counter.

An *object* is any portion of a computer's resources that can be assigned characteristics and manipulated as a single identifiable element. Typical objects on most computers include the processor, memory, paging file, and physical and logical disks. The complete list of objects varies from one system to another, depending on what hardware is installed, what network protocols are used, and so on.

Counters track various types of information about the objects to which they are assigned. The available counters vary from object to object. For the Processor object, for example, the available counters include % Interrupt Time, % Processor Time, Interrupts/sec, and several others.

Some counters report instantaneous values. Others report the average of the current value and the value at the previous sampling interval. Still others report the difference between the current value and the previous value. If you're uncertain about what a particular counter represents, click Explain in the Add Counters dialog box.

Some objects have multiple *instances.* A computer with multiple processors, for example, has an instance of the Processor object for each processor. The Process object has an instance for each process that's running. The PhysicalDisk object has an instance for each physical disk installed on the computer, and so on. Objects that have multiple instances typically include an instance that supplies information about the total of all the individual instances. So, for example, you could track a counter (such as IO Data Bytes/sec) for a particular running process or for the total of all running processes.

In this book, we use the following syntax to designate the combination of an object, a counter, and an instance:

object(instance)\counter

The IO Data Bytes/sec counter of the Process object for the instance *explorer,* for example, would be written like so:

Process(explorer)\IO Bytes/sec

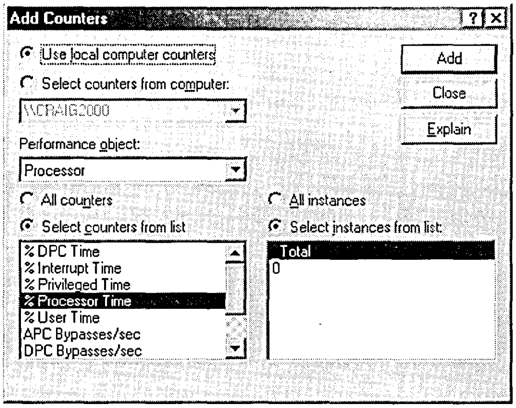
You will also see this syntax in the help file associated with the Performance console, in other Microsoft documents about performance monitoring (for example, in the *Microsoft Windows 2000 Professional Resource Kit* [Microsoft Press, 2000]), and (we presume) in other books about Windows 2000. (When the discussion concerns the monitoring of remote computers, you will see this syntax prefixed by a computer name and two backslash characters.) It's also the syntax used by the registry. In the Performance console itself, of course, you use ordinary dialog box lists to specify the combination of object, instance, and counter that you want to monitor.

Monitoring Current and Recent Information with System Monitor

In its Chart view, System Monitor shows the current state of one or more counters, along with a certain amount of very recent history. (At the default sampling interval of 1 second, the duration of a System Monitor chart is 1 minute and 40 seconds.) Alternative views show the current state of counters as a histogram or a textual report. To switch between Chart, Histogram, and Report views, use the View Chart, View Histogram, and View Report buttons on the toolbar. Alternatively, right-click anywhere on the chart, choose Properties from the shortcut menu, and select the view you want on the General tab of the System Monitor Properties dialog box.

Adding Counters

In any view, System Monitor's details pane is initially blank, waiting for you to select one or more of its myriad available performance measures. (A red vertical bar appears at the left side of the chart. If you do not see this bar, click the View Current Activity tool on System Monitor's toolbar.) To make your selection, click the Add button on the toolbar or right-click the chart and choose Add Counters from the shortcut menu. The Add Counters dialog box, shown in Figure 43-7, appears.



Add Counters

● Use local computer counters

○ Select counters from computer: \\CRAIG2000

Performance object: Processor

○ All counters

● Select counters from list

- % DPC Time
- % Interrupt Time
- % Privileged Time
- % Processor Time
- % User Time
- APC Bypasses/sec
- DPC Bypasses/sec

○ All instances

● Select instances from list:

- Total
- 0

Figure 43-7
To tell System Monitor what you want to monitor, select an object, a counter, and an instance from the lists in this dialog box.

To monitor your own computer, choose Use Local Computer Counters. To monitor a remote computer, choose Select Counters From Computer, and then select the name of the computer you want to watch.

To specify what you want to monitor, begin by selecting an object from the Performance Object list. The remaining two lists in the dialog box then show the counters and instances available for the selected object. You can select counters and instances singly, or you can make multiple selections. (Hold down the Shift key to select adjacent items or the Ctrl key to select ones that are not adjacent.) You can also use the All Counters and All Instances option buttons to select all the items in a list.

If you're not sure what a particular counter counts (more than a remote possibility, given the number of available counters), select it in the counters list and then click Explain. A paragraph of descriptive prose will descend from the bottom of the dialog box.

After you've selected a combination of object, counter, and instance, you can click Add to add the combination to your chart, histogram, or report and keep the dialog box open. Or you can simply click Close to add it and close the dialog box. You can add as many counters as you like to your chart, histogram, or report. Note, however, that a chart with many counters can be difficult to read. If you need to track a large number of performance measures at one time, consider using multiple instances of the Performance console and putting some of the counters on the second or subsequent instance.

Changing the Chart's Display Characteristics

System Monitor's Chart and Histogram views plot all counters against a single vertical axis scaled, by default, from 0 to 100. A default scaling factor is applied to each counter so that counters with large values (such as PhysicalDisk(_Total)\Disk Read Bytes/sec, which measures the number of bytes per second read from all physical disks and might reach the high hundreds of thousands or more) can coexist meaningfully in a chart with low-value counters (such as PhysicalDisk(_Total)\Disk Reads/sec, which measures the number of read operations per second).

It's quite possible that, in order to make a chart intelligible, you will need to adjust its scale or the scaling factor for one or more counters (or both the scale and one or more scaling factors). In particular, you will need to make some kind of adjustment if System Monitor represents one or more of your counters as a horizontal line along the top edge of the chart. That's System Monitor's way of saying that your data, given its current scaling factor, exceeds the highest value of the vertical axis.

Changing the Vertical Axis Scale

To change the scale, right-click the chart or histogram and choose Properties from the shortcut menu. On the Graph tab of the System Monitor Properties dialog box, type values in the Maximum and Minimum fields. Note that because all of System Monitor's many counters return positive values exclusively, you cannot set the minimum scale point to less than 0.

Changing a Counter's Scaling Factor

To change the scaling factor for a counter, go to the Data tab of the System Monitor Properties dialog box, select the counter, and then adjust the value of the Scale field. The default scaling factor is called Default, which tells you nothing about the value that System Monitor has chosen to use. To see what the default value actually is, check the Scale column in the chart's legend. For help in deciding what scaling factor might be appropriate, check the Minimum and Maximum values in the Value bar—the numeric fields that appear directly below the chart, above the legend. *(See Figure 43-6, on page 723.)*

Note, however, that the Value bar displays information only about the counter that's currently selected in the legend. Therefore, when adjusting the scaling factor for a particular counter, it's a good idea to select it in the legend *before* you open the System Monitor Properties dialog box.

Changing Colors, Fonts, and Titles

Other options on the various tabs of the System Monitor Properties dialog box let you change colors and fonts for your chart or histogram, add a main title or a vertical-axis title, and change the fonts and colors used for chart elements. You can also use Width, Color, and Style lists on the Data tab to modify the appearance of selected counters. Be aware, though, that the Style options are available only for the default line width. If you choose a nondefault width, you get the default (solid) line style.

Emphasizing a Particular Line

With several counters displayed on the same chart, it can sometimes be hard to tell which is which. If you double-click a line on the chart, System Monitor selects the associated counter in the legend. But when lines are close together, it can be difficult to be sure that you've double-clicked the right one. The Highlight tool on the toolbar (the tool that looks like a light bulb) can help. When you click the Highlight tool, System Monitor displays the current chart line in a bold width and contrasting color. With highlighting on, you can move up and down through the legend and see at a glance which chart line belongs to which legend entry.

Changing the Sampling Interval

By default, System Monitor samples counters at 1-second intervals. System Monitor always adjusts its display to show 100 sampling intervals, so at any resolution or window size the default-sampled chart shows 1 minute and 40 seconds' worth of data. You can alter the sampling interval by going to the General tab of the System Monitor Properties dialog box. Integers from 1 to 3888000 (1 second to 45 days) are accepted.

To freeze the current chart (stop sampling), clear the Update Automatically check box on the General tab of the System Monitor Properties dialog box. Alternatively, click the Freeze Display tool on the toolbar.

Printing a System Monitor Chart

Although System Monitor has no Print command, you can generate a printed image of the current chart. The easiest way to do this is to right-click the chart, choose Save As from the shortcut menu, and supply a file name. System Monitor saves your chart—its current appearance and counter list but not its other property settings—as an .htm file. You can then use your Web browser to display and print the file.

Alternatively, you can get printed output from System Monitor by importing the System Monitor control into another suitable application (such as Microsoft Word or Microsoft Excel) and then using that application's printing capability. *(See the next section, "Using the System Monitor Control.")* Or you can use the Counter Logs section of the Performance console to record performance data in a tab-separated or comma-separated log file and then import the resulting file into Excel or another spreadsheet program. *(See "Recording Performance Data with Counter and Trace Logs," page 728.)* When you have the performance numbers on a worksheet, you can use the spreadsheet program's charting facility to graph the data you're interested in.

Using the System Monitor Control

System Monitor is an ActiveX control stored in the file Sysmon.ocx. You can embed this control in many applications, including Word and Excel. When embedded, the System Monitor control functions exactly as it does in the context of the Performance console.

To insert the System Monitor control in a Word or Excel document:

1. Display the Control Toolbox toolbar. (Right-click any visible toolbar and select Control Toolbox.)
2. Click the More Controls tool.
3. Size and position the object that appears. (In Excel, you need to drag out a rectangle on the worksheet to have the object appear. Once it is visible on your worksheet, you can make further adjustments to its size and position.)
4. Click the Exit Design Mode tool.

In design mode, the System Monitor control appears without its toolbar. Handles appear around the object's perimeter (you might have to select it to make the handles visible), allowing you to size and position it. When you leave design mode, the System Monitor control's toolbar appears. Now you can use the toolbar and the shortcut menus to add counters, format the resulting chart, and so on.

Saving and Reusing System Monitor Settings

To copy the current chart's properties to the clipboard, use the Copy Properties tool on System Monitor's toolbar. To paste properties from the clipboard, use the Paste Counter List tool. These tools, which have no keyboard shortcuts or menu equivalents, let you replicate a chart in a separate instance of System Monitor. Alternatively, you can use them to restore the current state of a chart after making changes to it—provided, of course, that you haven't cleared the clipboard in the meantime. Note that the Paste Counter List tool pastes all properties stored on the clipboard, not just the counter list.

Because the .htm file created by System Monitor's Save As command *(see "Printing a System Monitor Chart," page 727)* records the current chart's counter list as well as its appearance, you can use this file as a way of transferring settings from System Monitor to a counter log or alert. *(See "Creating a Counter Log from System Monitor Settings," page 732.)*

Recording Performance Data with Counter and Trace Logs

System Monitor provides a graphical representation of the current (and recent) state of your system. But when you want to record performance data over time and preserve the numbers for analysis, you need a log. Logging is the way to create, in a disk file, a historical performance record for a computer or network you are monitoring.

By logging activity over time, for example, you can establish a baseline for the system and determine when and where performance bottlenecks occur. Or you can monitor system performance before and after a significant change, such as a hardware upgrade or a reassignment of files, folders, or users to other machines in an attempt to ease the load on a busy server.

The Performance console offers two types of logs: counter logs and trace logs. *Counter logs*, like System Monitor, sample your system at prescribed intervals. Counter logs can use any of the performance counters available in System Monitor. You can study the resulting log file, or a specified portion of it, by displaying it in System Monitor. Alternatively, if you save the log data in a tab-delimited or comma-delimited text file, you can subsequently import the numbers into a spreadsheet or database program.

Trace logs differ dramatically from counter logs. A *trace log* records an essentially continuous stream of performance data. To use a trace log, you must specify a data provider, and you can record data only for those performance measures that are made available by the provider. You can use the built-in Windows 2000 system provider or a third-party provider. An additional program—not supplied by Windows 2000—is required to parse a trace log into human-readable form.

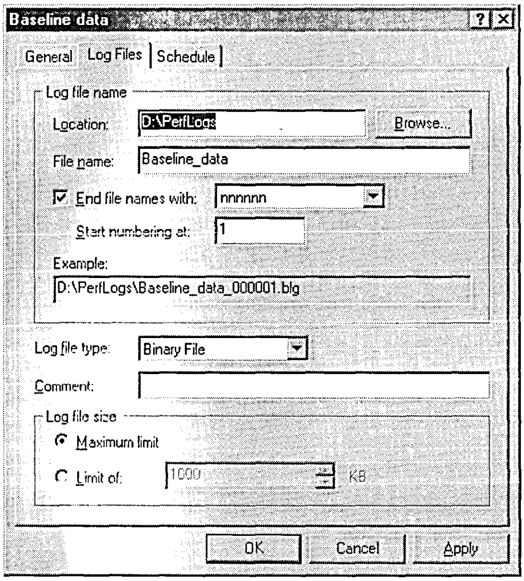
Creating a New Counter Log

To create a counter log, select Performance Logs And Alerts\Counter Logs in the console tree. Then right-click an empty place in the details pane and choose New Log Settings from the shortcut menu. In the New Log Settings dialog box, supply a name for your log and click OK. The name you enter here is the one that will appear in the Name field of the details pane, not the file name under which your data will be saved. You can enter something descriptive if you like, but you also have the ability to attach a comment (which will appear in the Comment field of the details pane), so you might want to save the description for the Comment field. (Note: to create a counter log, you must have full access to the registry key HKLM\System\CurrentControlSet \Services\SysmonLog\Log Queries.)

After supplying a name for your log, you arrive at the General tab of the new log's properties dialog box. Near the top of this dialog box, you'll find the file name and path that the Performance console proposes to use for your new log. You're not obliged to use these defaults, but before you can change them you must specify which performance counters you want to monitor. Click Add to do this. You'll find yourself in the Add Counters dialog box, which looks and functions exactly like its counterpart in System Monitor.

After you've specified the counter you want and have returned to the General tab, be sure to set the two sampling-interval controls, Interval and Units, to appropriate values. You can accept the default sampling interval of 15 seconds or override it with anything from 1 second to 45 days. The shorter your sampling interval, the more data is logged and the larger the resulting log file becomes. For the purpose of gathering baseline performance data, the 15-second default is a good value to try, but if you let the log run for a long time, you might want to keep an eye on the size of the log file. Note, however, that on the Log Files tab of the properties dialog box, which you'll come to next, you can specify a maximum size for the log file.

On the Log Files tab, shown in Figure 43-8, you can change your log's file name and path, add an automatic suffix to the file name, add a comment that will appear in the Comment field of the details pane, choose a file type, and specify a maximum file size.



Log file name

Location: D:\PerfLogs

File name: Baseline_data

☑ End file names with: nnnnnn

Start numbering at: 1

Example:
D:\PerfLogs\Baseline_data_000001.blg

Log file type: Binary File

Comment:

Log file size

● Maximum limit

○ Limit of: 1000 KB

Figure 43-8
The Performance console can add an automatic suffix, based on incremental numbering or the current date, to your log's file name.

Using File Name Suffixes

Unless you clear the End File Names With check box, the Performance console adds a suffix to your file name, using either an incremental numbering system or the current date in your choice of six date formats. These suffixes make it easy for you to create multiple iterations of a particular log. For example, if you create a log called Baseline and use the numeric suffix option with numbering starting at 1, the Performance console appends 00001 to the initial iteration of the log. If you stop and restart the log, a new file is created with the suffix 00002. Only one entry for the log appears in the details pane of the console, with the Log File Name field showing the current iteration only. But, of course, all the previous iterations are preserved and available for inspection.

Note that if you use one of the date suffix options and then stop and restart the log on the day it was created, your second iteration overwrites your first.

Choosing a File Type

The Performance console offers four log-file types:

- Binary File
- Binary Circular File
- Text File–CSV
- Text File–TSV

Chapter 43

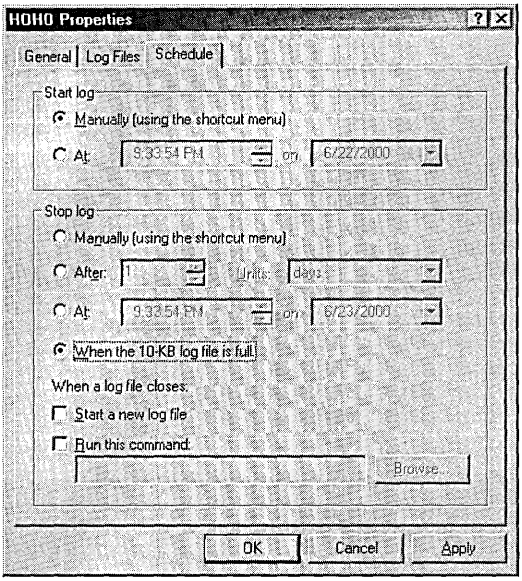
The formats of the binary and circular binary types are identical. What makes the latter circular is that if the file reaches its specified maximum size, the Performance console begins overwriting data at the beginning of the file with current data. The CSV text-file type uses commas to delimit values, and the TSV type uses tabs. Both types can be imported easily into a spreadsheet program such as Microsoft Excel. If you're planning to import into a database program, you might need to use CSV in preference to TSV.

Specifying a Maximum File Size

If you select the somewhat ambiguously named Maximum Limit option button in the Log File Size section of the dialog box, the Performance console lets the log file grow until your disk space is exhausted. To limit the file to a particular size, select Limit Of and specify a maximum size in kilobytes. On the Schedule tab, you can tell the Performance console what you want it to do if the log file reaches its maximum size. Note that you must select the When The *nn*-KB Log File Is Full option button on the Schedule tab, or the Performance console will allow the log file to grow beyond its maximum size.

Starting, Stopping, and Scheduling Logging Activity

On the Schedule tab, shown in Figure 43-9, you can tell the Performance console when you want your log to run and when you want it to stop. By default, logs are started and stopped manually. That is, they do nothing until you right-click the log name in the details pane and choose Start from the shortcut menu. And they continue to run until you holler "Stop!" by right-clicking again and choosing Stop from the shortcut menu. You can put either the starting or the stopping, or both, on a schedule by choosing options in the Start Log and Stop Log sections of this dialog box.



Start log

● Manually (using the shortcut menu)

○ At: 9:33:54 PM on 6/22/2000

Stop log

○ Manually (using the shortcut menu)

○ After: 1 Units: days

○ At: 9:33:54 PM on 6/23/2000

● When the 10-KB log file is full.

When a log file closes:

□ Start a new log file

□ Run this command:

Figure 43-9
You can use the Schedule tab to tell the Performance console when to begin and end the log.

Once started, a log continues to run when the current user logs off. It also continues to run when someone else logs on. (Because of an apparent bug, the log might not appear to be running under a different user account when you examine it in the Performance console. But if you check the log file itself, you'll see that it is.) If you shut down and restart your computer, a log that has been set to stop manually will not resume. (That is, the Performance console will regard your shutting down as a Stop command.) A log that's running on a schedule and that uses an incremental naming option will resume when the operating system restarts, but it will log to the next incremental file.

If you have specified a maximum file size on the Log Files tab, you'll want to select the When The *nn*-KB Log File Is Full option button. Then you can use the two check boxes directly below to tell the Performance console what to do if the log file should reach its maximum size. Select Start A New Log File if you're using an incremental naming system and want to continue logging in the next incremental file. Select Run This Command and specify a program name if you want the Performance console to execute a script or program when your file becomes full.

Creating a Counter Log from System Monitor Settings

You can easily create a counter log based on the performance counters currently used in System Monitor. Simply right-click in System Monitor, choose Save As from the shortcut menu, and supply a file name. Your settings will be saved as an .htm file.

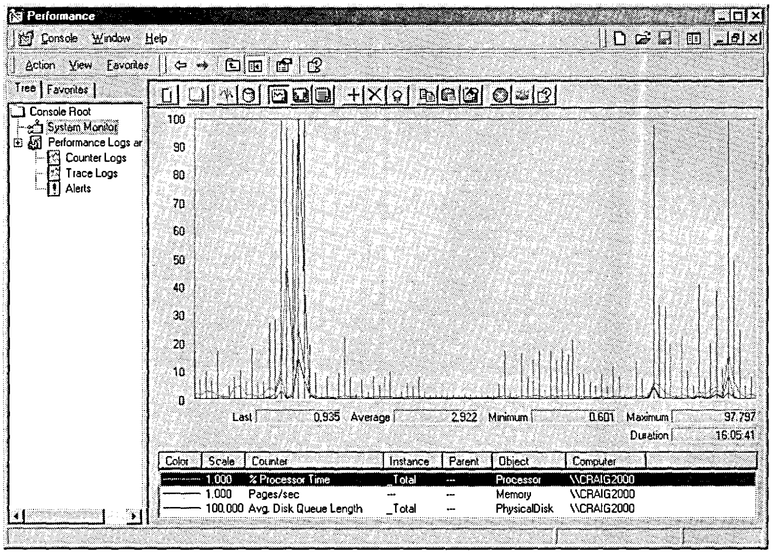
Then, in Counter Logs, right-click in the details pane and choose New Log Settings From from the shortcut menu. Specify the name of your .htm file and then a name for the new log. These steps take you to the properties dialog box for your new log, where you can take care of file-naming and scheduling details.

Viewing Counter Log Data in System Monitor

After you've created a log, you can view its data in System Monitor. You can look at either binary or text data this way, and you don't have to stop the log to look at it. (If you inspect a running log, System Monitor shows only as much data as the log currently contains; it doesn't update the display in real time.)

To display a log file in System Monitor, click the View Log File Data tool on System Monitor's toolbar, and then select the file in which your log data is stored. At first, the System Monitor chart will be blank unless, before you opened the log, you happened to be looking at real-time data for one or more of the counters recorded in the log. To make log counters visible (if they aren't already), click the Add tool, or right-click the chart and choose Add Counters from the shortcut menu. The Add Counters dialog box that appears is limited to the counters recorded in the log file. Make your selections, exactly as you would if you were charting real-time data, and then click Close.

System Monitor initially displays the entire time span of your log file. If this time span includes more than 100 sampling points, System Monitor divides the data into 100 equally spaced intervals and then uses high-low bars to show the maximum and minimum values that occurred during each interval. (See Figure 43-10.) It also shows, in the Duration field of the Value bar, the total time interval represented in the chart.

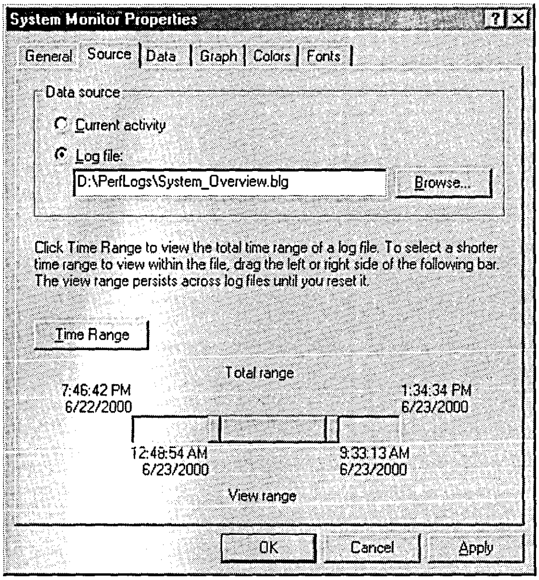


Last 0.935 Average 2.922 Minimum 0.601 Maximum 97.797
Duration 16:05:41

Color	Scale	Counter	Instance	Parent	Object	Computer
······	1.000	% Processor Time	_Total	---	Processor	\\CRAIG2000
——	1.000	Pages/sec	---	---	Memory	\\CRAIG2000
——	100.000	Avg. Disk Queue Length	_Total	---	PhysicalDisk	\\CRAIG2000

Figure 43-10
If the log data encompasses more than 100 sampling points, System Monitor groups sampling points as necessary and displays high-low bars.

To restrict the System Monitor chart to a subset of the log data, right-click the chart, choose Properties from the shortcut menu, and click the Source tab. As Figure 43-11 shows, a slider appears at the bottom of the dialog box. You can drag either end of the slider to change an end point of the time range. Or you can drag the center of the slider to the left or right to change the position of a subset without changing the subset's duration.



○ Current activity

● Log file: D:\PerfLogs\System_Overview.blg

Click Time Range to view the total time range of a log file. To select a shorter time range to view within the file, drag the left or right side of the following bar. The view range persists across log files until you reset it.

Total range: 7:46:42 PM 6/22/2000 – 1:34:34 PM 6/23/2000

View range: 12:48:54 AM 6/23/2000 – 9:33:13 AM 6/23/2000

Figure 43-11
You can use the Time Range slider to change the portion of your log data that System Monitor charts.

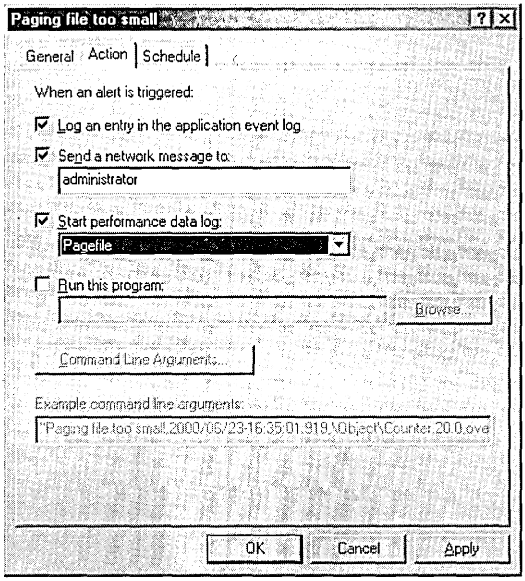
Setting Alerts

When you create an alert, you ask the Performance console to take a specified action if a particular counter crosses some threshold that you set. To do this, first select Performance Logs And Alerts\Alerts in the console tree. Then right-click in the details pane, choose New Alert Settings from the shortcut menu, and specify a name for your new alert. On the General tab of the alert's properties dialog box, supply a comment if you want one to appear in the details pane, click Add, choose one or more counters, and then click Close.

Back on the General tab again, you can set a threshold for a counter by selecting it in the Counters list and manipulating the two fields directly below the Counters list. By default, the Performance console will check your counter every 5 seconds. You can use the Interval and Units fields to adjust this sampling rate.

After you've set your counter and threshold, move on to the Action tab. There, as Figure 43-12 shows, you can have the Performance console initiate any or all of the following kinds of actions if your threshold condition is met:

- You can create an entry in the Application event log.
- You can send a message notifying a particular user.
- You can have the Performance console start a counter log.
- You can run a program (or script).



When an alert is triggered:

☑ Log an entry in the application event log

☑ Send a network message to: administrator

☑ Start performance data log: Pagefile

□ Run this program:

Example command line arguments: "Paging file too small,2000/06/23-16:35:01.919,\Object\Counter,20.0,ove

Figure 43-12
On the Action tab, specify the actions to take if the threshold is met.

If you choose to run a program, you can also have the Performance console feed that program a command string. To do this, click Command Line Arguments and fill out the ensuing dialog box.

What to Monitor

Here are a few suggestions about counters you might want to monitor. For a much more detailed account of performance counters and monitoring strategies, consult the *Microsoft Windows 2000 Professional Resource Kit* (Microsoft Press, 2000).

Establishing a Baseline for Memory Use

To establish baseline data about how your system uses memory, monitor the following counters over an extended period of time (weeks or months) of normal usage:

- Memory\Pages/sec
- Memory\Available Bytes (or Memory\Available KBytes)
- Paging File(_Total)\% Usage

Memory\Pages/sec is the number of pages (units of 4096 bytes) that are read from or written to disk to satisfy hard page faults. A *hard page fault* occurs when code or data needed by a process is not available in physical memory. Memory\Available Bytes and Memory\Available KBytes record the amount of memory available to running processes. Paging File(_Total)\% Usage records the percentage of your total paging file that's currently in use.

In your analysis of baseline data, ignore spikes. Focus on the value ranges that typify your system, not the exceptions. Then, if subsequent monitoring reveals that these counters frequently lie outside baseline ranges, you can be reasonably sure that a problem needs to be addressed.

Determining Whether Your Paging File Is Large Enough

Monitor Paging File\(_Total)\% Usage Peak. If this value, which represents the largest percentage of your paging file that your running processes actually use, exceeds 70 percent, you probably should increase the size of the paging file. You might also want to monitor Memory\% Committed Bytes In Use. This counter represents the ratio of committed memory (physical memory for which space is reserved in the paging file) to the commit limit (the total amount of memory the system can commit). Increasing the size of your paging file increases the commit limit. If Memory\%Committed Bytes In Use exceeds 85 percent, consider increasing the size of your paging file.

Monitoring for a Memory Leak

A memory leak occurs when an application allocates memory for its use but does not free the allocated memory when it no longer needs it. Symptoms of a memory leak include gradually worsening response time, a low virtual-memory message (or a message indicating that the system has automatically increased the size of your paging file), and error messages indicating that system services have been stopped. If you suspect that an application is leaking memory, monitor the following over an extended period of time while the application is running:

- **Memory\Available Bytes.** Other things being equal, this counter tends to fall during a memory leak.

- **Memory\Committed Bytes.** Other things being equal, this counter tends to rise during a leak.
- **Process(*process_name*)\Private Bytes, Process(*process_name*)\Working Set, and Process(*process_name*)\Page Faults/sec.** These all tend to rise during a leak.

Part 11

Appendixes

Appendix A
Companion CD Contents 741

Appendix B
Windows 2000 Professional CD Contents 743

Appendix A

Companion CD Contents

In This Chapter

Installing and Using Programs from the CD 742

The companion CD for this book contains supplemental information and utilities that you might find useful, including the following:

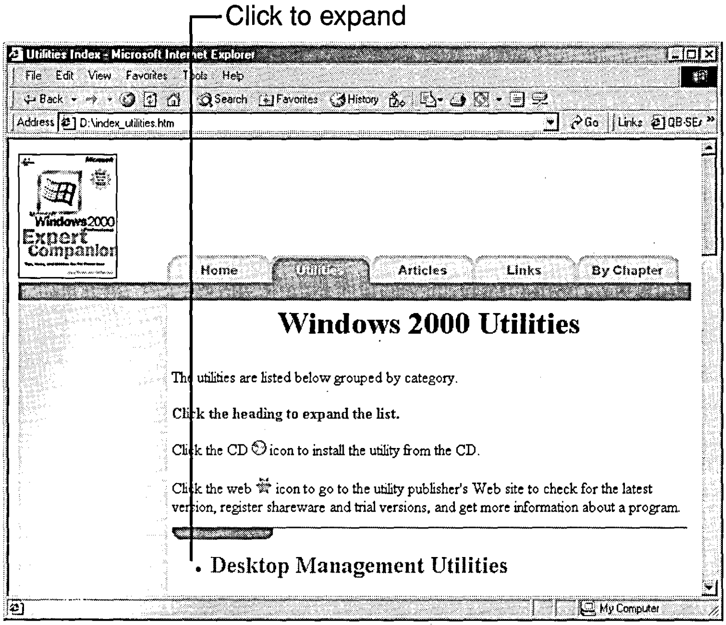
- A variety of utilities and other useful applications from Microsoft and other publishers
- Sample programs that appear elsewhere in this book
- Microsoft Knowledge Base articles that are cited in this book
- Microsoft NetMeeting Resource Kit
- Microsoft Internet Explorer Administration Kit
- Links to additional utilities from Microsoft
- Links to more information about Microsoft Windows 2000

You don't need to copy any files to your computer's hard drive or run a setup program to view the CD contents, which are set up as a Web site. Simply insert the CD in your computer's CD-ROM drive and the home page should appear in your Web browser. (If you have disabled AutoRun, open the Index.htm file in the CD's root folder.)

Note The system requirements for browsing the information on the CD are quite simple: you need a graphics-capable Web browser, such as Internet Explorer or Netscape Navigator. You can use any platform or operating system that can support your Web browser to browse the CD's content. The CD's pages include links to a number of utility programs that are on the CD. The system requirements for these utilities vary, but all are known to work on a system running Windows 2000 Professional with 96 MB of RAM.

Installing and Using Programs from the CD

The CD contains a number of programs from Microsoft and other publishers. You'll find them listed on the Utilities Index page, as shown in Figure A-1. (In addition, you'll find links to these programs on the By Chapter page.)


Click to expand

Utilities Index - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address D:\index_utilities.htm
Go Links QB-SE
Windows 2000 Expert Companion
Home
Utilities
Articles
Links
By Chapter
My Computer

Windows 2000 Utilities

The utilities are listed below grouped by category.

Click the heading to expand the list.

Click the CD icon to install the utility from the CD.

Click the web icon to go to the utility publisher's Web site to check for the latest version, register shareware and trial versions, and get more information about a program.

- Desktop Management Utilities

Figure A-1
On the Utilities Index page, click a category to display a list of programs in that category.

Some of these programs are freeware (you can use them as you see fit without payment), some are shareware (after trying the program, you're obligated to pay the publisher if you decide to continue using it), and some are limited-time trial or demonstration versions.

Along with a brief description of each utility, you'll see two icons. Clicking the CD icon starts the application's setup program. Because the CD functions like a Web site, when you click a CD icon, Microsoft Internet Explorer asks whether you want to run the program (the setup program, that is) or save the program to disk. Select the run option and click OK. Saving the program to disk just consumes disk space for a setup program you already have safely stored on CD, and it requires the extra step of launching the setup program after you save it.

The other icon by each program description is a link to the publisher's Web site. You might want to check there for additional information, a later version, or to see what other programs the publisher offers.

Appendix B

Windows 2000 Professional CD Contents

In This Chapter

Value Added Folder 744
Learning More About Files Installed from the CD 746

If you're like many experts, you comb the CD of a new operating system, looking for all the programs and other goodies that are *not* on the Start menu, hoping to find an undocumented trick to make your life easier or to amaze your friends. To give you a head start on finding such a gem, this appendix summarizes the content of the Windows 2000 Professional CD.

The Windows 2000 Professional CD-ROM includes the following folders and files in its root:

- **Bootdisk.** Contains files for creating the four-disk setup boot disk set. The disk images are stored in Cdboot1.img, Cdboot2.img, Cdboot3.img, and Cdboot4.img. Run Makeboot.exe or Makebt.32.exe to copy the disk images to floppy disks.
- **Discover.** Contains the HTML-based Discover Windows 2000 Professional tour—the one you can launch by clicking Discover Windows in the Getting Started With Windows 2000 window (Welcome.exe) that appears the first time you log on. You can launch the tour directly from this folder by opening Default.htm in Internet Explorer.
- **I386.** Contains the installation files for Windows 2000. Winnt.exe and Winnt32.exe are the 16-bit and 32-bit versions of the setup program. *(For details about setup, see Chapter 1, "Installing Microsoft Windows 2000.")* Most other files in \I386 are compressed, as indicated by the underscore (_) as the final character of the file name extension; to use any of these files you must decompress them with the Expand command.

- **\Setuptxt.** Contains Pro1.txt and Pro2.txt, the release notes for Windows 2000 Professional setup.
- **\Support.** Contains Hcl.txt, the Hardware Compatibility List (you can view an updated version at *www.microsoft.com/hcl*) and Apcompat.exe, the Application Compatibility tool. *(For details, see "Using Apcompat to Solve Compatibility Problems," page 143.)*

  The Tools subfolder contains the installation files for Windows 2000 Support Tools, an invaluable collection of miscellaneous utilities and technical information. To install Windows 2000 Support Tools, run \Support\Tools \Setup.exe. Sreadme.doc, also in the Tools subfolder, provides more information about Windows 2000 Support Tools.

  In addition, the Tools subfolder contains Deploy.cab, an archive file with tools and information for automating installation of Windows 2000. *(For details, see "Automating the Installation Process," page 14.)*
- **\Valueadd.** Contains a variety of tools from Microsoft and other publishers. Valueadd.htm ostensibly provides an overview of the contents of the subfolders, but it includes more legal disclaimer than useful information. *For more information, see the following section, "Value Added Folder."*
- **Autorun.inf.** Causes Setup.exe to run when the CD is inserted in the CD-ROM drive.
- **Cdrom_ip.5.** Identifies the Windows 2000 Professional CD as a bootable CD.
- **Cdrom_nt.5.** Identifies the Windows 2000 Professional CD as a bootable CD.
- **Read1st.txt.** Release notes for all versions of Windows 2000.
- **Readme.doc.** More extensive release notes for all versions of Windows 2000, in Microsoft Word format.
- **Setup.exe.** Program that displays a menu of options including Install Windows 2000 (runs \I386\Winnt32.exe), Install Add-On Components (runs Sysocmgr.exe, the Windows Components Wizard part of Add/Remove Programs), and Browse This CD (opens the CD root in Windows Explorer).

Value Added Folder

This section provides an overview of the contents of \Valueadd, the Value Added folder on the Windows 2000 Professional CD. In addition to the introductory Valueadd.htm file (and Banner.gif, an image file used by Valueadd.htm), \Valueadd contains two subfolders:

- **\3rdparty.** Contains a variety of applications provided by third parties (that is, someone other than Microsoft). None of these applications are developed or supported by Microsoft.

- **\Msft.** Contains a variety of applications from Microsoft. (Trivia note: For anyone who doesn't follow the roller coaster ride we call a stock market, MSFT is the ticker symbol for Microsoft Corporation.)

The following sections provide more information about the content of each subfolder. Your eyes might glaze over before you can explore all of these options on the CD. Many applications are for products or features that you've never heard of and don't need. Our goal here is to provide a quick overview that you can scan to identify the handful of programs that you might want to explore further. Most of the subfolders contain some sort of documentation—in the form of a Readme.txt file, a help file, or an HTML file.

\Valueadd\3rdparty

The 3rdparty subfolder contains the following subfolders:

- **\Ca_antiv.** Contains InoculateIT AntiVirus AVBoot V1.1, a program from Computer Associates International that detects and removes viruses when run from a bootable floppy disk.
- **\Level8\Mqc.que.** Contains Message Queuing Connector, a cross-platform application connectivity product from Level 8 Systems that you can use for implementing the Microsoft Message Queue (MSMQ) API in non-Windows operating systems.
- **\Mgmt\Agents.** Contains an HTML file with a link to information about agents that support Windows Management Instrumentation (WMI). Here's the link: *www.microsoft.com/windows2000/library/howitworks/management/wmi/agents.asp*
- **\Mgmt\Citrix\Eng.** Contains Citrix ICA clients for using a computer running any version of Windows to run applications on a Windows Terminal Server with Citrix MetaFrame.
- **\Mgmt\Inteldmi\Cimompro.** Contains a program from Smart Technology Enablers that allows an existing DMI application to run seamlessly on a WMI-enabled system.
- **\Mgmt\Inteldmi\Dmisp.** Contains a program from Smart Technology Enablers that provides the DMI service layer, a required component for either Cimompro or Wbemdmip (the other programs in the \Mgmt\Inteldmi folder).
- **\Mgmt\Inteldmi\Wbemdmip.** Contains Intel DMI to CIMON Data Provider, also from Smart Technology Enablers.
- **\Mgmt\Winstle.** Contains WinINSTALL LE, a program from VERITAS Software that allows you to package legacy setup programs for use with Windows Installer. *For more information, see "Creating MSI Files for Legacy Applications," page 151.*

- **\Security\Sdti.** Contains ACE/Agent for Windows 2000, a program from Security Dynamics Technologies that provides enterprises with the ability to add strong authentication management and encryption to their Windows 2000 environment.

\Valueadd\Msft

The Msft subfolder contains the following subfolders:

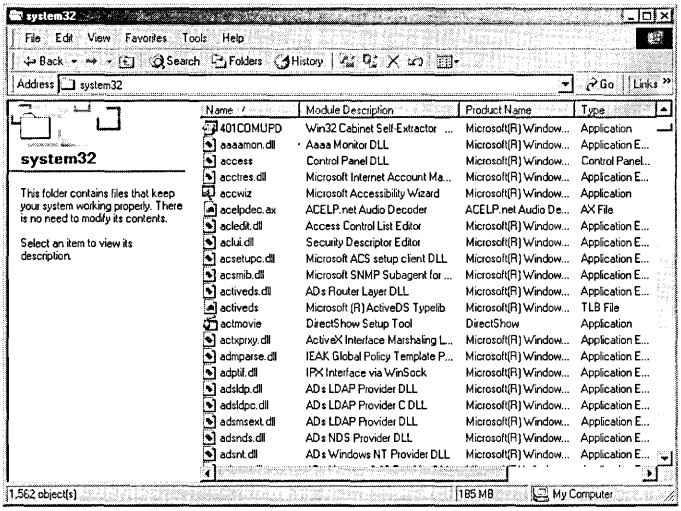
- **\Fonts.** Contains two TrueType fonts, Arial Alternative Regular and Arial Alternative Symbol.
- **\Mgmt\Adc.** Contains Active Directory Connector, which lets you synchronize Microsoft Exchange Server 5.5 mailboxes, custom recipients, and distribution lists with users, contacts, and groups in a Windows 2000 Active Directory.
- **\Mgmt\Ias.** Contains the Windows NT 4.0 Internet Authentication Service (IAS) snap-in for Microsoft Management Console, which allows you to manage IAS from Windows 2000.
- **\Mgmt\Ms_sms.** Contains the Systems Management Installation Wizard, which lets any computer become a Systems Management Server (SMS) client.
- **\Mgmt\Mstsc_hpc.** Contains the Microsoft Terminal Server Client for Windows CE, Handheld PC Edition version 3.0.
- **\Mgmt\Pba.** Contains Phone Book Administrator, a tool for managing phone books used by Microsoft Connection Manager.
- **\Mgmt\Wbemodbc.** Contains the Windows Management Instrumentation (WMI/WBEM) ODBC adapter, which provides a standard API that allows ODBC-based applications to read the data in the WMI Common Information Management (CIM) repository as if it were a relational database.
- **\Xtradocs\Script.** Contains help files that provide detailed reference information about JScript, Windows Scripting Components, VBScript, and Windows Script Host (WSH). *For more information, see Chapter 38, "Using Windows Script Host."*
- **\Xtradocs\Serk.** Contains the Microsoft FrontPage 2000 Server Extensions Resource Kit. Open Default.htm in Internet Explorer to display the documentation.

Learning More About Files Installed from the CD

And what of the myriad executable programs that are part of Windows 2000 Professional? Many are not on the Start menu and their names provide no clue as to their function. But with a little sleuthing, you can usually determine a program's purpose.

The following tips apply to all files provided with Windows 2000, but they're especially apropos to application files (.exe extension) and application extensions, or dynamic link libraries (.dll extension).

- Display the file's properties dialog box. If the file is an application, the General tab often includes a Description field that tells you everything you need. For example, the Description for one hidden gem, %SystemRoot%\System32\Dxdiag.exe, reveals its purpose: Microsoft DirectX Diagnostic Tool.
- The properties dialog box for most applications and application extensions includes a Version tab. By clicking each item in the Other Version Information box on this tab, you can learn something of a file's provenance.
- If you want to examine the Description and other potentially information-rich fields for a number of files, use Details view in Windows Explorer, choose View | Choose Columns, and display the Module Description and Product Name columns, as shown in Figure B-1.



This folder contains files that keep your system working properly. There is no need to modify its contents.

Select an item to view its description.

Name	Module Description	Product Name	Type
401COMUPD	Win32 Cabinet Self-Extractor ...	Microsoft(R) Window...	Application
aaaamon.dll	Aaaa Monitor DLL	Microsoft(R) Window...	Application E...
access	Control Panel DLL	Microsoft(R) Window...	Control Panel...
acctres.dll	Microsoft Internet Account Ma...	Microsoft(R) Window...	Application E...
accwiz	Microsoft Accessibility Wizard	Microsoft(R) Window...	Application
acelpdec.ax	ACELP.net Audio Decoder	ACELP.net Audio De...	AX File
acledit.dll	Access Control List Editor	Microsoft(R) Window...	Application E...
aclui.dll	Security Descriptor Editor	Microsoft(R) Window...	Application E...
acsetupc.dll	Microsoft ACS setup client DLL	Microsoft(R) Window...	Application E...
acsmib.dll	Microsoft SNMP Subagent for ...	Microsoft(R) Window...	Application E...
activeds.dll	ADs Router Layer DLL	Microsoft(R) Window...	Application E...
activeds	Microsoft (R) ActiveDS Typelib	Microsoft(R) Window...	TLB File
actmovie	DirectShow Setup Tool	DirectShow	Application
actxprxy.dll	ActiveX Interface Marshaling L...	Microsoft(R) Window...	Application E...
admparse.dll	IEAK Global Policy Template P...	Microsoft(R) Window...	Application E...
adptif.dll	IPX Interface via WinSock	Microsoft(R) Window...	Application E...
adsldp.dll	ADs LDAP Provider DLL	Microsoft(R) Window...	Application E...
adsldpc.dll	ADs LDAP Provider C DLL	Microsoft(R) Window...	Application E...
adsmsext.dll	ADs LDAP Provider DLL	Microsoft(R) Window...	Application E...
adsnds.dll	ADs NDS Provider DLL	Microsoft(R) Window...	Application E...
adsnt.dll	ADs Windows NT Provider DLL	Microsoft(R) Window...	Application E...

Figure B-1
Displaying the Module Description and Product Name columns allows you to see details about many files without opening their individual properties dialog boxes.

- You can also find details about the application and application extension files included with Windows, including details about exactly which version of each file is included with which Microsoft product releases, at this little-heralded Web site: *support.microsoft.com/servicedesks/fileversion/dllinfo.asp.*

Index

Numbers

- 100BaseT, peer-to-peer network connections, 362
- 10BaseT, peer-to-peer network connections, 362
- 128-bit encryption, 556
- 16-bit applications, crash prevention, 155–57
- 386 drivers, software compatibility issues, 6
- 56-bit encryption, 556

A

- Access Control Settings dialog box, 579, 581
- access control, security, 473 74
- access, auditing, 573–74
- Account Mappings dialog box, certificate mapping, 477
- accounts
  - computer, 10–11
  - domain, 293
  - local vs domain, 283–85
- ACL (access control list)
  - modifying inherited permission order, 546
  - permission editing, 545–547
  - SID (security identifier), 544, 547
  - NTFS file/folder permissions, 544–47
- ACPI (Advanced Configuration and Power Interface)
  - advantages, 258
  - battery management advantages, 258
  - Device Manager support determination, 259
  - FireWire device support, 258
  - PC card dynamic configuration support, 258
  - server support, 258
  - system compliancy process, 259
  - upgrading, 260
  - USB support, 258
  - vs APM, 257–60
- ACPI, *(continued)*
  - wake-on-LAN support, 258
  - wake-on-ring support, 258
- Action menu, common console elements, 72
- Active Directory
  - Group Policy interaction, 303
  - publish/assign application support, 146
  - publishing shared printers, 222
- active partition
  - described, 203
  - marking, 208
- ActiveX components, removing, 438
- ActiveX controls
  - adding to a console, 76–77
  - check for updates, 438
  - Microsoft NetMeeting/Web page integration, 511–12
  - snap-in requirement, 68
  - storing downloaded, 438
  - Sysmon.ocx (System Monitor), 728
- Add Counters dialog box, adding counters to System Monitor, 725–26
- Add Recovery Agent Wizard, 571
- Add Standard TCP/IP Printer Port Wizard, network printer connection, 229
- Add/Remove Programs
  - adding/removing Windows components, 149–51
  - changing/removing applications, 148–49
  - described, 147
  - new program installation, 149
  - published application availability, 146
- Address bar, MRU (most recently used) lists, 134
- Address toolbar, MRU (most recently used) lists, 134
- Adm folder, Group Policy, 301
- administrative shares, described, 373–74
- Administrative Tools folder, Adminpak.msi file, 356–57

Administrator accounts, limiting, 478–79
Administrators Group
  enabling auditing, 576
  set up auditing of files/folders, 578
  set up auditing printer access, 580
administrators, setting up new, 470
Adminpak.msi file, domain administration, 356–57
Admins Web group, 469
Adobe Systems, pdf format filters, 97
Advanced Attributes dialog box
  excluding files from catalogs, 114
  NTFS file compression, 671–72
Advanced Configuration and Power Interface (ACPI), vs APM, 257–60
Advanced Options menu
  accessing, 36
  troubleshooting options, 36–37
Advanced Power Management (APM), vs ACPI, 257–60
Advanced RISC Computing (ARC)
  Boot.ini file pathname editing, 35–36
  computer startup process, 33
Advanced Schedule Options dialog box, task property editing, 140–41
Alerter service, described, 346
alerts
  Alerter service, 346
  Performance console, 734–35
aliases, folder names, 113
Alphabetize.bat file, Favorites menu/Start menu alphabetizing, 618–24
Alt+Enter key combination, switching between screen modes, 157
American Registry for Internet Numbers (ARIN), IP address registration, 395
analog voice/fax modem, dial-up connections, 415
Analysis Report dialog box, disk defragmentation, 673
AND operator, 107
anonymous authentication, described, 472
anonymous logon, FTP connection, 526
answer files
  additional application installation, 26–29

answer files, *(continued)*
  ASCII text file conventions, 19–20
  automating mini-Setup Wizard, 25
  Cmdlines.txt, 26–28
  creating, 16–18
  customizing, 18–20
  described, 16
  [GuiRunOnce] section uses, 28–29
  password privacy issues, 20
  troubleshooting, 21
  using during Setup, 20–22
antivirus programs, disabling prior to installation, 10
Apcompat utility, described, 143–44
APIPA (Automatic Private IP Addressing), described, 397
APM (Advanced Power Management)
  battery alarm parameters, 263
  BIOS support issues, 260
  described, 258
  enabling, 260–61
  hibernation configuration, 261–62
  known bugs, 267
  power schemes, 262–63
  power status indicator, 263–64
  standby configuration, 262
  UPS configuration, 264–65
  vs ACPI, 257–60
AppEvent.evt (Application) log file, 83
Apple Macintosh computers, network printing support, 232
Appl e Macintosh, AppleTalk settings, 411–12
AppleTalk, non-TCP/IP settings, 411–12
Application (AppEvent.evt) log file, 83, 574
Application Compatibility dialog box, solving program compatibility, 144
Application Data folder, User Profiles, 314
application events, described, 84
Application log (AppEvent.evt), record applications events, 574
Application Log Properties, log file size/longevity settings, 90
application media pools, described, 238
application-level filtering, firewalls, 431
ARC (Advanced RISC Computing), 33, 35–36

archives, log files, 91
ARIN (American Registry for Internet Numbers), IP address registration, 395
ARP (Address Resolution Protocol), network troubleshooting tool, 407
asterisk (*) character, command prompt support, 181
asymmetric cryptography, described, 440
asymmetric encryption, described, 584
At command, task scheduling, 141–42
audit events, 577–78
audit policies, selecting, 480
auditing
  cautions about overuse, 578
  changing settings, 580
  described, 84, 573–75
  disadvantages, 574
  enabling, 577
  file/folder access, 578–80
  printer access, 580–82
  security, 479–81
  viewing events, 575–76
Auditing Entry dialog box, 480, 581
audits, changing settings, 580
authentication
  CA (certification authority) hierarchy, 588
  Microsoft NetMeeting, 509
  security, 472–73
  selecting type, 473
Authentication Methods dialog box, 479
author mode, running a user-mode console, 70
Authors Web group, 469
AutoComplete, Run dialog box, 453
AutoComplete Settings dialog box, opening, 454
Autoexec.bat file
  boot disk element, 43
  MS-DOS-based application settings, 163–64
automated installation
  additional applications, 26–29
  answer file/Setup program uses, 20–22
  creating answer files, 16–18
  customizing answer files, 18–20
automated installation, *(continued)*
  differences file, 22–23
  disk imaging (Sysprep.exe), 23–25
  methods, 14–15
  non-script method, 16
  small office strategy, 21–22
  Udf (uniqueness database file), 22–23
automatic detection, configuration scripts, 447
automatic installation, strong encryption, 556
Automatic Private IP Addressing (APIPA), described, 397
Automatically Log On dialog box, automated startup settings, 38–39
AutoPlay, disabling, 250–51
AutoRun, command prompt uses, 188–89
AutoRun file, listing Doskey macros, 600
Autorun.inf file, disabling, 250

B

background services, disabling prior to installation, 10
backup agents, disabling prior to installation, 10
Backup program
  preparing tapes, 253
  Removable Storage issues, 252–55
  tape data backups, 253–54
  troubleshooting, 253
  Windows NT workaround, 255
backups
  copy, 677
  daily, 677
  differential, 677
  existing data prior to installing Windows 2000, 8–9
  incremental, 677
  log files, 92–93
  normal, 677
  preparing tapes, 253
  registry, 659–60
  Removable Storage devices, 252–55
  restoring the registry, 659–60
  scheduling, 254–55
  tape data backup process, 253–54
  types, 677

- Baseline data dialog box, counter logs, 730
- basic authentication, described, 472
- basic disks
  - converting to a dynamic disk, 208–11
  - defined, 201
  - dynamic disk conversion, 213
  - extended partition creation, 207–8
  - logical drive creation, 208
  - marking the active partition, 208
  - partition creation, 205–8
- basic volume, described, 203
- bat file extension, batch programs, 610
- batch files .*See* batch programs
- batch programs
  - Alphabetize.bat, 618–24
  - automated compatibility checker, 7–8
  - bat (batch) file extension, 610
  - capitalization rules, 610
  - CD-ROM changers, 245–48
  - changing to a different folder, 624–25
  - CleanRecent.bat, 617–18
  - cmd file extension, 610
  - commands, 610–11
  - commenting, 612
  - described, 609–10
  - Dial.bat, 612–15
  - double colon (::) comment identifier, 612
  - environment variables, 616–17
  - ErrorLevel value testing, 614
  - executing, 612
  - file naming conventions, 610
  - local environment variables, 625–26
  - PopD command, 624–25
  - PushD command, 624–25
  - redirecting a Pause message to the Nul device, 624
  - replaceable parameters, 622
  - Rsbackup.bat, 615–17
- battery, alarm parameters, 263
- binary NOT operator, 107
- BIOS (basic input/output system)
  - APM support issues, 260
  - bootable CD setup process, 13
  - computer startup process, 33
  - MBR (master boot record), 33
- BIOS, *(continued)*
  - setting to non-Plug and Play operating system, 5
  - updating to overcome installation problems, 5
- BIOS settings, security, 557
- bookmarks, exporting prior to installing Windows 2000, 8
- Boolean operators
  - described, 96
  - Indexing Service, 107–8
  - Indexing Service support, 96
  - order of precedence, 108
- boot disks
  - creating, 42–45
  - required files, 43
  - uses, 42–43
  - vs Recovery Console, 43
- boot loader, recovering, 56–57
- boot managers, dual boot system alternative, 62
- boot menu
  - default startup options, 32–33
  - operating system elements, 48
  - removing items from, 35
  - timeout value editing, 34
- boot partition
  - deletion protection, 215
  - described, 49, 203
- Boot.ini file
  - ARC pathname editing, 35–36
  - boot disk element, 43
  - boot menu operating system elements, 48
  - build number display, 34
  - computer startup process, 33
  - disabling Windows splash screen, 34
  - driver name display, 34
  - driver name display, 34
  - hidden/system attributes, 33–34
  - installed memory display, 34
  - modifying, 33–36
  - multiple processor display, 34
  - operating system description editing, 34
  - serial mouse detection disabling, 34
  - service pack level display, 34

Boot.ini file, *(continued)*
timeout value editing, 34
bootable CD, installation strategy, 13
BootMagic, dual boot system alternative, 62
BootPart, dual boot system alternative, 62
Bootsect.dos file
boot disk element, 43
computer startup process, 33
dual boot system process, 48–49
Browse Folder dialog box, move folder, 436
Browse For Drive Path dialog box, path search, 217
Browsers Web group, 469
browsers, changing default, 435
bugs, Windows 2000 Professional, 267
build number, displaying during startup, 34

C

CA (Certification Authority)
certificates, 440, 475
described, 588–89
digital certificates, 440
hierarchy of certificate authentication, 588
PKI requirement, 584–85
cab (compressed archive) files, described, 15
cable modems
Internet connections, 421–22
network connections, 415
permanent IP address, 395
persistent connection, 422
cables
direct parallel connection, 485
peer-to-peer network connections, 362–63
cache, described, 377
caching
avoiding unwanted local cache, 380
documents automatically, 378
documents manually, 377
offline file uses, 377–80
Caching Settings dialog box, file caching for offline use, 377
Cacls.exe utility, viewing/editing NTFS permissions, 547
callto hyperlinks, Microsoft NetMeeting, 511–12
canonical verbs, described, 128
capacity, NTFS advantages, 541
caret (^) character, macro symbol identifier, 602
catalogs
adding/deleting folders, 113–14
creating/deleting, 115
defined, 96
excluding NTFS files, 114
folder viewing, 113–14
indexing files with unknown extensions, 112–13
Indexing Service creation process, 111–12
Category column, Event Viewer, 86–87
CD changer.msc console, creating, 243–45
CDFS (Compact Disk File System), 539
CD-ROM
disabling AutoPlay, 250–51
installing programs, 741–42
CD-ROM changers
batch program creation, 245–48
custom MMC console creation, 243–45
jukebox uses, 248–51
Mount.bat file, 246–47
Removable Storage support issues, 242–48
troubleshooting, 245
CD-ROM drives
installation requirements, 4
Removable Storage support, 241–42
Certificate dialog box, viewing certificate contents, 586
Certificate Export Wizard, 566, 593
Certificate Import Wizard, 567, 593
certificate mapping, 477
Certificate Request Wizard, enterprise-wide Certificate Services, 589
Certificates console
exporting/importing certificates, 593
requesting certificates, 593
view options, 593–94
Certificates dialog box
back up recovery agent certificate, 568

Certificates dialog box, *(continued)*
- digital certificate management, 591–92
- remove trusted certificates, 442–43

certificates
- backing up, 564–68
- digital, 440–42, 583–95
- installing/removing, 442–43
- IPSec authentication method, 492
- Microsoft NetMeeting authentication, 509
- recovery agent, 564
- revoked, 440
- security, 474–75

Certification Authority (CA) .*See* CA

Change Drive Letter And Path dialog box, drive letter/path assignments, 216

Change Profile Type dialog box, User Profiles, 318

character sets, language choices, 454–55

characters
- asterisk (*) wildcard, 181
- caret (^) macro symbol identifier, 602
- dollar sign ($) special shares, 373–74
- double colon (::) batch program comment identifier, 612
- question mark (?) wildcard, 181

charts, System Monitor, 726–27

Check Disk dialog box, file system/media error checking, 675–76

Check.bat file, automated compatibility checker batch file, 7–8

Check.txt file, automated compatibility checker text file, 7–8

child windows, adding to a console, 79

Ciad.msc (Indexing Service) console, Indexing Service management, 110–11

Cipher command, 563

Cipher.exe utility, 563
- command-line switches, 562
- new personal encryption certificate, 568

class A, IP address, 388

class B, IP address, 388

class C
- IP address, 388
- subnet mask, 390

class D, IP address, 388

class E, IP address, 388

CleanRecent.bat file, cleaning out the Recent Documents List, 617–18

client certificates, described, 475, 477

client computers, ICS configuration settings, 426–27

Client for Microsoft Networks, peer-to-peer networks, 364

clients
- cache management techniques, 378–80
- FTP (File Transfer Protocol), 525–36
- Telnet, 515–20

cmd file extension, batch programs, 610

Cmd.exe (Command Prompt) file
- command extensions, 190
- command-line syntax, 190–91
- described, 188
- vs Command.com, 174

Cmdhere.reg file, folder/command prompt session startup, 173

Cmdlines.txt file, additional application installation, 26–29

code/key, IPSec authentication method, 492

codec (coder/decoder), Internet connection speed issues, 503

collaboration, Web sites, 483

colors
- command prompt session settings, 177
- Disk Management panel views, 200
- System Monitor chart editing, 726–27

command delimiter, described, 227

command extensions, command prompt uses, 190

command line
- command combination symbols, 184
- editing keys, 180–81
- escape (^) symbol, 184–85
- FTP client uses, 527–33
- Net File command, 384
- Net Session command, 383–84
- Net Share command, 380–82
- Net Statistics command, 384–85
- Net Use command, 382–83
- network utilities, 290–93
- pausing/canceling commands, 185
- pipe (|) symbol, 183
- program command symbol conventions, 181–85

command line, *(continued)*
- redirecting input/output, 183
- redirection symbols, 182
- Remote.exe file, 355–56
- running System Information from, 685–87
- Telnet client, 516–19

command prompt
- AutoRun uses, 188–89
- browsing network resources, 193–94
- color settings, 177
- command combination symbols, 184
- command enhancements, 179–85
- command extension uses, 190
- command-line editing keys, 180–81
- described, 171–72
- Doskey settings, 177–78
- environment variables, 185–87
- escape (^) symbol, 184–85
- file/folder name completion, 189–90
- font settings, 176–77
- help system, 179–80
- listing current routing table, 392
- network commands, 191–94
- password-protected resource connection, 193
- pausing/canceling commands, 185
- pipe (|) symbol, 183
- program command symbol conventions, 181–85
- redirecting input/output, 183
- redirection symbols, 182
- Run As command uses, 143
- running commands from, 187–88
- Services management commands, 341
- shared resource connection, 192–93
- starting, 187–88
- starting a telnet client session, 517–18
- starting at a particular folder, 173
- starting programs from, 178–79
- starting/ending a session, 172–73
- uses, 171–72
- wildcard support, 181
- window customization techniques, 174–78
- window sizing/positioning, 175–76

command strings, described, 133–34

Command.com file
- boot disk element, 43
- vs Cmd.exe, 174

command-line switches, Cipher.exe, 562

command-line, Windows Explorer uses, 124–26

commands
- Action | All Tasks | Configure Server Extensions, 469
- Action | Find, System Information, 681
- Action | New | Virtual Directory, 467
- Action | Save As Text File, System Information, 684
- Actions | All Tasks | Close System Information File, 684
- Actions | All Tasks | Open System Information File, 684
- Actions | All Tasks | Save As System Information File, 684
- Actions | Refresh, System Information, 683
- Actions | Save As System Information File, System Information, 684
- At, 141–42
- batch, 610–11
- Cipher, 563
- command prompt help, 179–80
- Convert, 215
- Customize View, 80
- Delete Logical Drive, 215
- Delete Partition, 215
- Delete Volume, 215
- Edit | Add Key, Regedt32, 661
- Edit | Add Value, Regedt32, 662
- Edit | Find, Regedt32, 661
- Edit | New, Rededit, 661
- Format, 214
- FTP (File Transfer Protocol), 529–33
- Hide Mouse Pointer, 159
- mmc, 68
- MRU (most recently used) lists, 134–35
- Nbstat, 409
- Net, 408
- Net File, 384
- Net Localgroup, 292–93
- Net Session, 383–84
- Net Share, 380–82

commands, *(continued)*
Net Statistics, 384–85
Net Use, 382–83
Net User, 290–92
Net View, 193–94
Netstat, 408
Network Identification, 409
networks, 191–94
New Window From Here, 79
Nslookup, 409
Options | Read Only Mode, Regedt32, 661
pausing/canceling at the command line, 185
PopD, 624–25
PushD, 624–25
Recovery Console, 710
Registry | Connect Network Registry, Regedit, 666
Registry | Export Registry File, 667
Registry | Load Hive, Regedt32, 660
Registry | Restore, Regedt32, 659
Registry | Save Key, Regedt32, 659
Registry | Select Computer, Regedt32, 666
Remote, 355–56
replacing with Doskey macros, 604–5
Route, 403–5, 408
Route Print, 392
Run As, 142–43
Security | Permissions, Regedt32, 661, 665
Services management, 341
Set, 185–87
shortcut menu editing, 128–30
Start | Help, 693
Tools | Synchronize (IE), 438
View | Choose Columns, System Information, 682
View | Find Key, Regedt32, 661
View | Refresh Now, Windows Task Manager, 715
View | Update Speed | High, Windows Task Manager, 715
View | Update Speed | Low, Windows Task Manager, 715

commands, *(continued)*
View | Update Speed | Paused, Windows Task Manager, 715
winver, 11
comments, batch programs, 612
commit charge, described, 715
compatibility, FAT advantages, 542
compatibility checker
accessing from Setup program, 6
batch file creation, 7–8
components, Critical Update Notification, 676
compressed drives, uncompressing prior to installing Windows 2000, 9–10
compression, NTFS advantages, 540
Computer Associates International, InoculateIT AntiVirus AVBoot, 699–700
Computer column, Event Viewer, 87
Computer Configuration, Group Policy, 303–4
Computer Management console
creating a new console, 349–351
described, 348–49
Performance Logs and Alerts, 722
shortcut creation, 349
supported snap-ins, 348–49
computers
account creation, 10–11
default startup options, 32–33
direct parallel connection, 485
gatekeepers, 506–7
gateways, 506–7
inbound time partner, 342–43
last known good configuration startup, 707–8
locking, 134
network names, 409
peer-to-peer network connections, 363–64
POST (power-on self test) process, 33
pre-installation preparation, 9–10
Recovery Console, 42
safe mode startup, 706–7
single computer installation strategy, 12–14

computers, *(continued)*
viewing/printing system configuration, 270–74
Config.sys file
boot disk element, 43
MS-DOS-based application settings, q 161–63
configuration scripts
automatic detection, 447
control IE, 446
directed configuration, 447
vs Group Policy settings, 451
Configure Server Extensions Wizard, 469
connections
cable modems, 421–22
dial-up, 415–18
direct parallel, 485
DSL (digital subscriber line), 421–22
FTP (File Transfer Protocol), 526–27
incoming, 486–88
Internet types, 415
LAN, 415, 418–21
network, 415
network connection order settings, 410
non-TCP/IP settings, 411–12
peer-to-peer network cables, 362–63
persistent, 422
tunneling protocols, 489–90
viewing with Net Use command, 382–83
console tree
adding folders to, 75
described, 72
displaying, 74–75
consoles
Action menu elements, 72
ActiveX control addition, 76–77
CD changer.msc, 243–45
Certificates, 592–95
child window creation, 79
Ciad.msc (Indexing Service), 110–11
common elements, 72–73
Computer Management, 348–51
console tree, 72
console tree display, 74–75
creating from Computer Management console, 349–51
consoles, *(continued)*
data export file types, 73
details pane, 72–73
Disk Management, 71
extension addition, 76
Favorites addition, 80
folder addition, 75
Group Policy (gpedit.msc file), 298–309
hiding/displaying elements, 80
Internet link addition, 76–77
IPSec Security Policy Management, 492–98
Local Security Settings, 293–96, 492–98
Local Users And Groups, 287–89, 318–19
MMC included types, 68
msc file extension, 69
naming conventions, 80
Performance, 722–37
Remote Administration, 352–53
restriction options, 81–82
running, 69–70
running a user-mode console in author mode, 70
running with a target computer specification, 70
Services, 333–41
Shared Folders, 371–80
shortcut menus, 72
snap-in addition, 76
System Information, 71, 679–84
taskpad view addition, 77–79
troubleshooting, 69
uses, 71–73
View menu elements, 72
CONTAINS operator, 105–6
content ratings, using, 482
Contents property, Indexing Service query submission, 102–3
Control Panel
Add/Remove Programs, 146–51
cascading submenus, 119
Users and Passwords, 286–87
cookies
exporting prior to installing Windows 2000, 8
importing/exporting (IE), 452–53

cookies, *(continued)*
- temporary Internet file storage, 436

Cookies folder, User Profiles, 314
copy backup, described, 677
counter logs
- activity scheduling, 731–32
- creating, 729–33
- file name suffixes, 730–31
- file sizing, 731
- recording performance data, 728–33
- starting/stopping logging activity, 731–32
- supported file types, 731
- viewing in System Monitor, 733–34

counters
- adding to System Monitor, 725–26
- described, 723–24
- scaling factors, 726
- what to monitor, 735–37
- TLDs (top-level domains), 394

CPU Usage graph, Windows Task Manager, 720–21
Create a New Media Pool Properties dialog box, media pool settings, 239
Create Partition Wizard
- extended partition creation, 207–8
- marking the active partition, 208
- primary partition creation, 206–7

Create Report dialog box, Windows NT 4, 9
Create Shared Folder Wizard, share creation, 374
Create Volume Wizard, creating volumes on dynamic disks, 212
Critical Update Notification component, Windows Update, 676
Cscript.exe file, command-line scripting program, 628–29
Ctrl+Alt+Del key combination, disabling, 41
Ctrl+Alt+Delete key combination, displaying background services, 10
cursors, command prompt session settings, 177–78
Customize Toolbar dialog box (IE), 448, 451
Customize View dialog box, MMC display customization, 73
customizing, IE options, 455–60

D

daily backup, described, 677
data
- backing up before installing Windows 2000, 8–9
- exporting prior to installing Windows 2000, 8
- storing sensitive, 557–58

data recovery policy, described, 568
data types, registry, 658–59
Date column, Event Viewer, 86
dates, Indexing Service formats, 106–7
daylight saving time, Event Viewer support, 86
DDL (dynamic-link library), upgrade packs (migration DLLs), 6
decryption, files/folders, 562–63
default support programs, IE, 449
Dependency Walker (Depends.exe), troubleshooting uses, 700
Deployment Tools, installation, 15
Deptool.chm file, described, 15
Desired Performance dialog box, Indexing Service parameters, 116
Desktop folder, User Profiles, 314
desktops, behavior managed by Internet Explorer, 450
details pane, described, 72–73
device drivers
- displaying details, 272–73
- installing from a known location, 277
- installing from a list of known drivers, 277–78
- MS-DOS, 163
- reinstalling, 276–77
- resource conflict solving, 274
- signing options, 278
- updating/modifying, 275–78

Device Manager
- device configuration editing, 274–75
- device status checking, 272–74
- disabling/reenabling devices, 274
- displaying device driver details, 272–73
- displaying phantom devices, 270–71
- driver signing options, 278

Device Manager, *(continued)*
error codes, 278–79
hardware profiles, 279–80
installing device drivers, 277–78
multiprocessor support installation, 278
power management support determination, 259
print options, 272
reinstalling device drivers, 276–77
resource conflict solver, 274
resource setting editing, 274–75
starting, 270
uninstalling a device, 274
updating/modifying device drivers, 275–78
view options, 271
viewing/printing system configuration, 270–74
devices
configuration editing, 274–75
disabling/reenabling, 274
resource setting editing, 274–75
status checking, 272–74
uninstalling, 274
DHCP (Dynamic Host Configuration Protocol), described, 396–97
Dial.bat file, batch program example, 612–15
dial-up connections
creating, 416-18
described, 415
disconnecting, 418
modem types, 415
shortcut creation, 418
Dial-Up Networking Monitor, connection status monitoring, 418
differences file, automated installation, 22–23
differential backup, described, 677
digest authentication, described, 472
digital certificates, 440–42
asymmetric encryption, 584
CA (Certification Authority), 584–85, 588–90
Certificate Services, 589
common certificate purposes, 587
contents, 441
development history, 584–85
fees, 590
digital certificates, *(continued)*
importing/exporting, 586, 593
Internet software distribution, 441
items used, 440
logical certificate stores, 587
logical store, 587–88
physical store, 587
PKI (Public Key Infrastructure), 584
reasons for using, 585
renewing, 586
requesting, 585, 593
signing e-mail messages, 595–96
symmetric encryption, 584
Thawte, 590
trust hierarchy, 590
trusted root authority, 590
types, 586–87
VeriSign, 590
viewing, 586
digital subscriber line (DSL), network connections, 415
Direct Parallel Connection cables, direct computer connection, 485
directed configuration, configuration scripts, 447
directories
.*See also* Folders
apply security/permissions, 466
configure FrontPage extensions, 466
defined, 465–66
organizing files, 466
tasks in IIS, 466
DirectX Diagnostic Tool, troubleshooting uses, 696
disabling, EFS, 569–70
discussion server, Microsoft Office 2000, 448
Disk Cleanup, freeing up disk space, 670–71
Disk Defragmenter, optimizing disk performance, 672–75
disk imaging, described, 23
Disk Management console
adding a new disk, 204
assigning/changing drive letters, 215–18
basic disk management tasks, 205–11
basic disk structure, 201
box sizing, 200

Disk Management console, *(continued)*
color settings, 200
converting basic disk to a dynamic disk, 208–11
creating mounted drives, 217–18
described, 197–98
Disk List display panel, 199–200
disk property/status checking, 218–20
dynamic disk management tasks, 211–12
dynamic disk structure, 201–2
dynamic disk to basic disk conversion, 213
enhancements, 198
extended partition creation, 207–8
fault-tolerant volumes, 204
formatting an existing volume, 214
Graphical View display panel, 200
hard disk identifiers, 201
linear scaling, 200–201
logarithmic scaling, 200–201
logical drives, 202–3, 208
marking the active partition, 208
mounted drives, 204–5
partitions, 202–3
primary partition creation, 206–7
remote computer techniques, 199
screen elements, 71, 198–201
starting, 198
switching between views, 200
troubleshooting basic to dynamic disk
conversion, 211
uses, 197–98
Volume List display panel, 199
volume property/status checking, 218–20
volumes, 203–4
disk quotas
creating a new quota entry, 553–54
deleting, 554
enabling, 550–52
enabling on remote volumes, 552
management techniques, 552–54
NTFS advantages, 541
NTFS enforcement, 550
Quota Entries window, 552–54
disk utilities, compatibility issues, 6
disk-compression programs, Windows 2000 non-support, 9
Diskeeper utility
defragmentation tool, 675
MFT (Master File Table) defragmenting, 543
disks
adding to computer, 204
Disk Defragmenter, 672–75
file system error checking, 675–76
freeing up space, 669–72
media error checking, 675–76
NTFS file compression, 671–72
property checking, 218–20
status checking, 218–20
Display Properties dialog box, logon screen customization, 39–40
DLL Help Database, troubleshooting uses, 706
DNS (domain name system)
described, 10, 393–96
development history, 393
FQDN (Fully Qualified Domain Name), 394
hierarchical structure, 394
name resolution, 393–95
top-level domains, 394
DNS servers, name resolution, 395
documentation
FrontPage Server Extensions, 469
viewing Internet Information Server, 465
documents
automatic caching, 378
Indexing Service supported types, 97
manual caching, 377
Documents menu, MRU (most recently used) list, 134
dollar sign ($) character
macro parameters, 601
special shares, 373–74
domain accounts
management techniques, 293
vs local accounts, 283–85
domain name system (DNS), described, 10, 393–96
domain names, ICANN registration services, 396

domain-level policy settings, vs audit policy settings, 576
domains
 administration techniques, 356–57
 Adminpak.msi file, 356–57
 described, 10
 joining, 365
 joining after installation, 11
 naming, 409
 TLDs (top-level domains), 394
Doskey
 command prompt session settings, 177–78
 switches, 606
Doskey macros
 comment placement, 601
 defining, 600
 described, 599
 dollar sign ($) character, 601
 folder-listing commands, 603–4
 grouping, 601
 listing in AutoRun file, 600
 management techniques, 600–601
 parameter uses, 601–2
 program uses, 606–7
 replacing Windows 2000 commands, 604–5
 saving to a file, 600
 special characters, 603
 symbol uses, 602–4
dotted quad format, described, 399
dotted-decimal IP address, described, 388
double colon (::) characters, batch program comment identifier, 612
DoubleSpace, Windows 2000 non-support, 9
downloaded files, final destination, 436–38
Downloaded Program Files Folder
 ActiveX controls, 438
 opening, 438
Dr. Watson
 append to existing log file setting, 695
 application error response sequence, 693–94
 crash dump path, 695
 creating a crash dump file, 695
 dump all thread contexts setting, 695
 dump symbol table, 695
Dr. Watsor, *(continued)*
 log file path, 694
 number of errors to save settings, 695
 number of instruction settings, 695
 option settings, 694–95
 sound notification settings, 695
 viewing log files, 695–96
 visual notification settings, 695
 Wave file path, 695
drive letters, assigning/changing, 215–18
drive paths, assigning, 215–18
Driver Signing Options dialog box, driver signing options, 278
drivers
 displaying name during startup, 34
 Windows Update uses, 676
drives, compressed, 9–10
DriveSpace, Windows 2000 non-support, 9
DSL (digital subscriber line)
 guaranteed data rates, 422
 Internet connections, 421–22
 network connections, 415
 persistent connection, 422
DSL modem, permanent IP address, 395
dual boot systems
 boot floppy file considerations, 43
 boot managers, 62
 boot menu elements, 48
 boot partition, 49
 compatible file system issues, 49–50
 default startup options, 32–33
 described, 13
 hardware solutions, 63
 limitation work arounds, 52–53
 limitations, 49–50
 MS-DOS addition, 53–54
 operating system addition, 53–60
 Outlook Express issues, 51
 paging (swap) file sharing, 57–58
 partition managers, 62
 reasons for using, 47
 recovering the boot loader, 56–57
 removing operating systems, 60–61
 separate partition installation
 advantages, 51
 supported operating systems, 47
 system partition, 49

dual boot systems, *(continued)*
  third-party alternatives, 62–63
  Windows 3.x addition, 53–54
  Windows 9x, 54–58
  Windows NT addition, 58–59
DUN (dial-up networking) connection, routing options, 403–4
DVD drive, installation requirements, 4
dynamic disks
  converting from basic disk, 208–11
  converting to a basic disk, 213
  defined, 201–2
  extending a volume, 212–13
  management tasks, 211–12
  volume creation, 212
  volume limitations, 209
Dynamic Host Configuration Protocol (DHCP), described, 396–97
dynamic routing
  described, 391
  RIP (Routing Information Protocol)
  Listening, 391, 405
dynamic volume, described, 203
dynamic-link library (DDL), upgrade packs (migration DLLs), 6

E

Edit Drive Letter or Path dialog box, drive letter/path editing, 216
EFS (encrypting file system)
  disabling, 569–70
  enabling, 570–71
  storing sensitive data, 557–58
e-mail
  encrypting, 595–96
  exporting data prior to installing
  Windows 2000, 8
e-mail address, FTP connection password, 526
emergency recovery disk (ERD)
  creating, 678
  troubleshooting uses, 711–12
  updating importance, 690
empty recovery policy, creating, 570
encrypting file system (EFS), 557
encryption
  advantages for folders, 558
  asymmetric, 584
  back up access information, 558
  backing up certificates, 564–68
  checking files for, 563
  creating new personal certificate, 568
  dangers from other authorized users, 562
  defined, 440, 555
  EFS, 557–58
  e-mail messages, 595–96
  enabling, 570–71
  file behavior, 561–62
  files, 557–63
  files vs folders, 557–60
  folders, 557–63
  identifying encrypter, 569
  Microsoft NetMeeting, 509–10
  NTFS advantages, 540
  NTFS compression non-support, 671
  PKI (Public Key Infrastructure), 584
  preventing, 569–70
  recovering encrypted files/folders, 568–69
  recovery policy, 560
  security, 474–79
  symmetric, 584
  system file limitations, 559
Enter Network Password dialog box, user account management, 284
  Enterprise Certificate Authority
  Services, 477, 481
environment variables
  batch programs, 616–17
  modifying, 187
  Path, 134
  predefined, 186
  viewing, 185–86
EQUALS operator, 105–6
ERD (emergency repair disk)
  creating, 678
  troubleshooting uses, 711–12
  updating importance, 690
error and event messages help (W2000msgs.chm), 703

error codes
    Device Manager, 278–79
    System Information devices, 682
error events, described, 84
ErrorLevel value testing, batch programs, 614
escape (^) symbol, described, 184–85
Event column, Event Viewer, 87
event logs, IPSec troubleshooting, 500
Event Properties dialog box, 87–88, 576
Event Viewer
    access methods, 85–87
    Application (AppEvent.evt) log file, 83
    archiving log files, 91
    backing up log files, 92–93
    Category column, 86–87
    clearing log files, 91
    Computer column, 87
    Date column, 86
    daylight saving time support, 86
    described, 83–85, 575
    details pane elements, 85–87
    displaying archived log files, 91–92
    Event column, 87
    event searches, 89
    examining event details, 87–88
    exporting log file information, 92
    hiding/displaying columns, 86
    log display filters, 88–89
    log file longevity settings, 90–91
    log file size settings, 90–91
    monitoring remote computers, 93–94
    multiple log views, 89
    Security (SecEvent.evt) log file, 83
    Source column, 86
    System (SysEvent.evt) log file, 83
    Time column, 86
    Type column, 86
    User column, 87
events
    application, 84
    described, 83
    errors, 84
    examining, 87–88
    information, 85
    log files, 83
    monitoring on remote computers, 93–94
    searches, 89
events, *(continued)*
    security auditing, 84
    system, 84
    types, 84–85
    viewing audit, 575–76
    warnings, 84
Exec.wsf file, executing commands on remote computers, 644–52
Executive Software, Diskeeper defragmentation tool, 543, 675
Explorer bars, adding to Internet Explorer, 461–62
exporting
    favorites/cookies, 452–53
    personal encryption certificate, 565–66
expressions, queries, 101–2
Extend Volume Wizard, extending a volume on a dynamic disk, 213
extended partitions
    deletion protection, 215
    described, 202–3
extended volumes, limitations, 213
Extensible Markup Language (XML) tags, 631–32
extensions
    adding to a console, 76
    applying to Web sites, 469
    user interface names, 469

F

FAT (file allocation table)
    advantages, 541–42
    compatibility advantages, 542
    converting volumes to NTFS, 542–43
    file system types, 539
    small volume support, 542
    speed advantages, 542
    volume label naming conventions, 215
FAT12 file system, 539
FAT16 file system
    described, 539
    dual boot system compatibility issues, 49–50
FAT32 file system
    described, 539

FAT32 file system, *(continued)*
dual boot system compatibility issues, 49–50
volume label naming conventions, 215
fatal errors, stop-error behavior configuration, 691–92
Favorites
adding to a console, 80
importing/exporting (IE), 452–53
Favorites folder, User Profiles, 314
Fc.exe, registry file comparison program, 667
FEK (file encryption key), 557
File and Printer Sharing for Microsoft Networks, peer-to-peer networks, 364
file compression, freeing up disk space, 671–72
file encryption key (FEK), 557
file extensions
bat (batch), 610
cab (compressed archive), 15
cmd, 610
evt (Event Log), 91
hiding/displaying in Windows
Explorer, 120–21
job (task object), 139
msc (MMC consoles), 69
msi (Windows Installer application)
support, 146–47, 151
reg (Regedit export file), 660
suppressing selected types, 121
udf (uniqueness database file), 22
wsf (Windows Script Host), 631–32
File Signature Verification utility, troubleshooting uses, 697–98
file systems
CDFS (Compact Disk File System), 539
described, 539
dual boot system compatibility issues, 49–50
error checking, 675–76
FAT (file allocation table) types, 539
FAT12, 539
FAT16, 49–50
FAT16, 539
FAT32, 49–50
FAT32, 539
file systems, *(continued)*
new partition assignment, 206
NTFS, 49–50, 539–54
selection guidelines, 539–543
UDF (Universal Disk Format), 539
File Transfer Protocol (FTP), 438, 463
FileProp.vbs file, FileSystemObject example, 638–39
files
accessing temporary Internet, 436
Adminpak.msi, 356–57
Alphabetize.bat, 618–24
answer, 16–22
AppEvent.evt (Application log), 574
Application (AppEvent.evt), 83
auditing access, 578–80
auditing successful access 578
Autoexec.bat, 43, 163–64
AutoRun, 600
Autorun.inf, 250
backing up prior to installing Windows 2000, 8–9
behavior of encrypted, 561–62
being prompted for location, 437–38
Boot.ini, 33–36, 43, 48
Bootsect.dos, 33, 43, 48–49
cab (compressed archive), 15
caching identification, 377
Cacls.exe, 547
Check.bat, 7–8
Check.txt, 7–8
checking for encryption, 563
CleanRecent.bat, 617–18
Cmd.exe (Windows 2000 command
processor), 174, 188
Cmdhere.reg (folder/command prompt
session) startup, 173
Cmdlines.txt, 26–28
command prompt name completion, 189–90
Command.com (MS-DOS command
processor), 43, 174
Config.sys, 43, 161–63
Cscript.exe, 628–29
decrypting, 562–63
Depends.exe (Dependency Walker), 700
Deptool.chm, 15

files, *(continued)*
- Dial.bat, 612–15
- display audit settings, 579
- downloading, 435–39
- downloading without certification, 442
- encrypted vs unencrypted, 561–62
- encrypting, 557–63
- Exec.wsf, 644–52
- FileProp.vbs, 638–39
- Filever.exe (FileVer utility), 700–701
- Folders.vbs, 629–31
- Ftp.exe (FTP command-line client), 527–33
- Gpedit.msc (Group Policy), 40–41
- gpedit.msc (Group Policy) console, 298–309
- Gpt.ini, 301
- Hal.dll, 33
- hiding physical location, 466
- hiding/displaying in Windows Explorer, 119–20
- identifying encrypter, 569
- IO.sys, 43
- Lsass.exe (Local Security Administration), 33
- Memsnap.exe (memory profiling tool), 701
- Mount.bat, 246–47
- Mountvol.exe, 549–50
- Msdos.sys, 43
- Msiexec.exe, 147
- Msinfo32.exe, 680
- Net.exe, 290–93
- Noise.eng, 98
- Ntbackup.exe, 659–60
- Ntbackup.exe, 677
- Ntbootdd.sys, 33, 43
- Ntdetect.com, 33, 43
- NTFS compression, 671–72
- NTFS security permissions, 544–47
- Ntldr (bootstrap loader), 33, 43, 48–49
- Ntoskrnl.exe, 33
- offline, 376–80
- paging (swap), 57–58
- Pmon.exe (Process Resource Monitor), 702
- Processor.vbs, 640–44

files, *(continued)*
- protecting from authorized users, 562
- protection methods, 147
- Pviewer.exe (Process Viewer), 702–3
- Rasphone.exe, 418
- recovering encrypted, 568–69
- Regedit.exe, 354, 655
- Regedt32.exe, 354, 655
- Registry.pol, 303
- Remote.exe, 355–56
- Rsbackup.bat, 615–17
- SecEvent.evt (Security log), 574
- Secpol.msc (Local Security Policy), 40–41
- Security (SecEvent.evt), 83
- set up auditing, 579–80
- Setupcl.exe, 15
- Setupmgr.exe (Setup Manager Wizard), 15–18
- Setupmgx.dll, 15
- Sfc.exe (System File Checker), 147
- SysEvent.evt (System log), 83, 574
- Sysmon.ocx (System Monitor), 728
- Sysprep.exe, 15, 23–25
- System.ini (Windows 3.x), 155
- Telnet.exe, 516
- Tlist.exe, 338
- tlntadmn.exe, 521
- types to download, 437
- Udf (uniqueness database file), 22–23
- Unattend.doc, 15
- Upgrade.txt, 7
- W2000msgs.chm, 703
- Win 2000 Pro CD, 746–747
- Win.ini (Windows 3.x), 155
- Winlogon.exe, 33
- Winn32.log, 7
- Winnt.exe, 14
- Winnt32.exe, 6–8, 14
- Wscript.exe, 628–29

FileSystemObject, Windows Script Host, 638–40

FileVer (Filever.exe), 700–701

filter lists, adding to IPSec filter rule, 494–96

filter rules
- adding to a IPSec policy, 493–94
- IPSec, 491

Filter Wizard, adding filter lists to the filter rule, 496
filters
application-level, 431
described, 97
event logs, 88–89
IP Protocol ID 50, 500
IP Protocol ID 51, 500
UDP Port 500, 500
Find in System Information dialog box, information item search, 681
firewalls
application-level filtering, 431
described, 430–31
FTP issues, 527
IPSec filter requirements, 500
packet filtering, 430–33
selection criteria, 431
FireWire devices, ACPI support, 258
floppy disks, booting from, 42–45
floppy drives
boot floppy creation, 42–45
installation requirements, 4
setup disk creation, 13
Folder Options dialog box, offline file configuration, 379
folders
.*See also* directories
adding to the console tree, 75
adding to the Start menu, 123–24
adding to the taskbar, 124
adding/deleting from Indexing Service catalog, 113–14
advantages of encryption, 558
aliases, 113
auditing, access, 578–80
command prompt name completion, 189–90
decrypting, 562–63
directories, 465
display audit settings, 579
encrypting, 557–63
hiding/displaying in Windows Explorer, 119–20
manually rescanning in the Indexing Service, 115
NTFS compression, 671–72
folders, *(continued)*
NTFS security permissions, 544–47
recovering encrypted, 568–69
removing "nag" screens when viewing contents, 121–22
set up auditing, 579–80
sharing on a peer-to-peer network, 367
shell, 126–28
starting a command prompt session from, 173
Temporary Internet File, 436
Value Added, 744–46
Folders bar, hiding/displaying in Windows Explorer, 118
fonts
command prompt session settings, 176–77
MS-DOS-based application property settings, 165
System Monitor chart editing, 726–27
Format dialog box, formatting partitions/logical drives/volumes, 214
Fpremadmexe command-line utilities, 470
Fpsrvadm.exe, extension snap-in, 470
FQDN (Fully Qualified Domain Name), described, 394
Free folder, media pools, 237
free-text expressions, queries, 101–2
FrontPage, configuring server extensions, 468–71
FrontPage extensions, directories to configure, 466
FrontPage Server Extensions
advantages, 469
HTML Administration Forms, 470
removing from Web sites, 471
FTP (File Transfer Protocol)
anonymous logon, 526
ASCII file-transfer mode, 526
binary file-transfer mode, 526
command entering conventions, 529–33
command-line client (Ftp.exe) file, 527–33
described, 463
development history, 525
establishing connections, 526–27
firewall issues, 527

FTP, *(continued)*
- graphical FTP client/Windows Explorer, 534–35
- passive mode, 533
- proxy server issues, 527
- response codes, 529
- security issues, 526
- server operating system types, 526
- text-based client/Windows Explorer, 535
- URL (uniform resource locator) conventions, 525

FTP folder
- unsupported functions, 439
- viewing sites with anonymous logons, 438–39

FTP proxy connection, unsupported by FTP folder, 439

FTP server, running, 482–83

FTP sites, logons, 438–39

Ftp.exe file, FTP command-line client, 527–33

Fully Qualified Domain Name (FQDN), described, 394

functions, unsupported in FTP folder, 439

G

gatekeepers, Microsoft NetMeeting, 506–7

gateway computers
- ICS requirement, 423
- ICS configuration, 426

gateways
- described, 391
- Microsoft NetMeeting, 506–7

Gilles Vollant Software, BootPart, 62

globally unique identifier (GUID), opening shell folders, 126

Gpedit.msc (Group Policy) file, logon security options, 40–41

GPO (Group Policy object)
- described, 301
- Gpt.ini file, 301
- GroupPolicy folder elements, 301–2

Gpt.ini file, described, 301

graphical FTP client, using from Windows Explorer, 534–35

Group Policy Console
- access limited to Administrators Group, 450
- access methods, 298–299
- Active Directory interaction, 303
- adding/removing policy templates, 300–301
- adding/removing startup programs, 136
- Computer Configuration branch, 303–4
- configuring Internet Explorer, 450–51
- custom console creation, 299
- customizing settings for different users, 307–9
- customizing window elements, 299–301
- described, 297–98
- disabling unnecessary for performance
- enhancement, 304–5
- displaying only configured policies, 301
- enabling disk quotas, 551–52
- enabling/disabling settings, 305–7
- Folder Redirection extension, 328–29
- gpedit.msc file, 298–309
- GPO (Group Policy object), 301–5
- IPSec policy management, 492–98
- logoff scripts, 321
- logon scripts, 321
- Microsoft NetMeeting policies, 510–11
- not configured default setting, 305
- periodic refresh, 303
- publish/assign application capability, 146
- registry-based policy management, 297
- script assignment, 298
- script settings, 322
- script types, 321–22
- security option specifications, 298
- settings, 302–9
- settings precedence order, 304
- shutdown scripts, 321
- starting from a remote computer, 298–99
- startup scripts, 321
- User Configuration branch, 304
- user folder redirection, 328–29
- uses, 297–298

Group Policy Console, *(continued)*
vs System Policy Editor, 309
Group Policy (Gpedit.msc) file, logon security options, 40–41
Group Policy object (GPO)
described, 301
GroupPolicy folder elements, 301–2
GroupPolicy folder, files/folders, 301–2
groups
adding/deleting members, 293
Net Localgroup command uses, 292–93
security settings, 293–96
setup methods, 286–93
viewing information, 292
GUID (globally unique identifier), opening shell folders, 126

H

hackers, described, 428–29
Hal.dll file, computer startup process, 33
hard disks
adding to computer, 204
basic disk management tasks, 205–11
described, 201
Disk Defragmenter, 672–75
Disk Management identifiers, 201
dual boot system solutions, 63
extended partition creation, 207–8
file system error checking, 675–76
freeing up disk space, 669–72
installation requirements, 4
MBR (master boot record), 33
media error checking, 675–76
NTFS file compression, 671–72
partition creation, 205–8
security risk, 557
hardware
dual boot system solutions, 63
HCL (Hardware Compatibility List), 5, 705
installation requirements, 4–5
printing configuration information, 8–9
Removable Storage supported devices, 241–51
Hardware Compatibility List (HCL), 5, 362, 705
Hardware Profiles dialog box, described, 279–80
hardware profiles, described, 279–80
HCL (Hardware Compatibility List)
CD-ROM changer issues, 243
described, 5, 705
NIC compatibility issues, 362
help system
command prompt help, 179–80
displaying the command reference, 611
troubleshooters, 692–93
hexadecimal values, registry display, 657
hibernation, APM configuration, 261–62
hidden files, displaying in Windows Explorer, 119–20
High Encryption Pack, upgrading, 556
history
command-line commands, 180–81
Doskey settings, 177–78
Windows Task Manager graphs, 720–21
History bar, MRU (most recently used) list, 134
history lists, hiding from casual snoopers, 134–35
hives
backing up/restoring, 659–60
registry structure, 657
HKEY_CLASSES_ROOT, registry root key, 656
HKEY_CURRENT_CONFIG, registry root key, 656
HKEY_CURRENT_USER, registry root key, 656
HKEY_DYN_DATA, registry root key, 656
HKEY_LOCAL_MACHINE, registry root key, 656
HKEY_USERS, registry root key, 656
home directory
changing, 466
stored locations, 466
home page, changing, 471
Home Phoneline Networking Alliance (HomePNA), peer-to-peer networks, 362
HomePNA (Home Phoneline Networking Alliance), peer-to-peer networks, 362

Host a Meeting dialog box, requiring passwords, 508
host ID, IP address, 388
Hotmail
  configuring, 449
  Microsoft Passport source, 505, 512
HTML editor (IE), selecting, 449
HTML files, Indexing Service support, 97
HTTP vs HTTPS, 476
hubs, peer-to-peer networks, 364
HyperTerminal, Telnet client, 519–520

I

IANA (Internet Assigned Numbers Authority)
  IP address registration process, 395
  private reserved IP address, 389
ICANN (Internet Corporation for Assigned Name and Number), domain names, 396
icons, console selections, 80
ICQ (Internet Chat Request), instant messaging, 501
ICS (Internet Connection Sharing)
  client computer settings, 426–27
  configuration, 425–27
  described, 423
  gateway computer, 423, 426
  ports, 425
  shared connection setup, 423–25
  sockets, 425
  vs routers, 423
IE . *See* Microsoft Internet Explorer (IE)
IEAK (Internet Explorer Administration Kit), 447
IIS (Internet Information Services)
  changing home page, 471
  configuring FrontPage Server
  Extensions, 465, 468–71
  control with Internet Information
  Services snap-in, 465
  creating folders, 467
  described, 463
  directories, 465–68
  directory tasks, 466
  extension administration tools, 470
  Indexing Service development history, 95
  installing, 464–65
  Internet printing, 483–84
  Microsoft Personal Web Manager, 468
  opening 465
  restricting access to authors/
  administrators, 465
  Secure Sockets Layer (SSL), 575
  security management, 472–81
  using, 465–71
  viewing documentation, 465
  virtual directories, 467
ILS (Internet Locator Service), Microsoft NetMeeting people search, 504–5
Import folder, media pools, 237–38
Import/Export Wizard, favorites/cookies, 452–53
importing, favorites/cookies, 452–53
inbound time partner, Windows Time service, 342–43
incoming connections, creating, 486–88
incremental backup, described, 677
Indexing Service
  activating, 98–99
  administration techniques, 110–16
  alternative word form queries, 110
  AND operator, 107
  Boolean operator support, 96
  Boolean operators, 107–8
  case insensitive default, 98
  catalog creation process, 111–12
  catalog folder addition, 113–14
  catalog folder removal, 113–14
  catalogs, 96, 111–14
  Ciad.msc console, 110–11
  CONTAINS operator, 105–6
  content query submission, 102–3
  creating/deleting catalogs, 115
  date/time expression formats, 106–7
  described, 95–96
  development history, 95
  EQUALS operator, 105–6
  excluding NTFS files, 114
  filters, 97
  folder name aliases, 113
  free-text expressions, 101–2

Indexing Service, *(continued)*
ignored words, 97–98
indexing files with unknown extensions, 112–13
limitations, 97–98
long form queries, 101
manually rescanning folders, 115
MS-DOS-style wildcard characters, 109
Noise.eng file, 98
NOT operator, 107
OR operator, 107
pattern-matching queries, 108–10
pausing, 113
performance parameter adjustments, 115–16
phrase expressions, 101–2
proximity operator, 108
proximity operator support, 96
query submission, 99–110
relational operators, 106
restarting, 113
Search Assistant integration, 96
security issues, 96
short form queries, 100–101
stopping, 113
supported document types, 97
supported properties, 104–5
UNIX-style regular expressions, 109
viewing folders in a catalog, 113–14
Indexing Service on Local Machine Properties dialog box, 112–13
Indexing Service Settings dialog box, described, 98–99
Indexing Service Usage dialog box, performance parameters, 115
information events, described, 85
InoculateIT AntiVirus AVBoot, troubleshooting uses, 699–700
installation
automating, 14–25
backing up existing data prior to running Setup, 8–9
bootable CD process, 13
Cmdlines.txt file uses, 26–29
compatibility checker, 6–8
computer account creation, 10–11
computer preparation, 9–10
Deployment Tools, 15
FrontPage Server Extensions, 468–70
HCL (Hardware Compatibility List), 5
IIS, 464–65
legacy software compatibility testing, 6–8
pre-installation issues, 4–12
printing hardware configuration information, 8–9
programs from CD-ROM, 741–42
single computer strategy, 12–14
Support Tools, 15
troubleshooting, 5
uncompressing compressed drives, 9–10
vs upgrade, 11–12
Windows 200 High Encryption Pack, 555–57
instances, described, 723–724
instant messaging, MSN Messenger Service, 512–13
Integrated Services Digital Network (ISDN) modem, dial-up connections, 415
Integrated Windows authentication, described, 472
IntelliMirror
described, 322–23
mandatory user profiles, 327
profile creation, 325–27
roaming profiler shared folder setup, 324
roaming user profiles, 323–27
user account setup, 324–25
user configuration settings, 312
user folder redirection, 328–29
Intermediate Certification Authorities, Certificates dialog box, 442
Internet Assigned Numbers Authority (IANA), private reserved IP address, 389
Internet
adding links to a console, 76–77
cable connections, 421–22
client printer setup, 230–31
codec (coder/decoder) connection speed issues, 503
communication methods, 501–14
connection sharing, 423–28

Internet, *(continued)*
connection types, 415
creating dial-up connections, 416–18
dial-up connections, 415
direct connections, 415
disconnecting a dial-up connection, 418
downloading files, 435–39
DSL (digital subscriber line)
connections, 421–22
firewalls, 430–31
FTP clients, 525–36
hackers, 428–29
LAN connection, 418–21
mail/news file Indexing Service
support, 97
Microsoft NetMeeting, 502–12
packet filtering configuration, 432–33
security issues, 428–34
TCP/IP configuration, 422
TCP/IP port security issues, 429–30
troubleshooting resources, 704–6
tunneling, 430
VPNs (virtual private networks), 415
Internet Chat Request (ICQ), instant
messaging, 501
Internet Connection Sharing (ICS),
described, 423
Internet Connection Wizard
dial-up connection creation, 416–18
LAN connection, 418–19
Internet Corporation for Assigned Name and
Number (ICANN), domain
names, 396
Internet Explorer Administration
Kit (IEAK), 447
Internet Explorer Profile Manager, 447
Internet Information Services (IIS), 463
Internet Information Services snap-in, control
IIS, 465
Internet instant messaging, MSN Messenger
Service, 512–13
Internet Options dialog box
accessing temporary files, 436
Advanced tab, 455–60
automatically detect settings, 447
disabling tabs, 451
Enable Profile Assistant, 445
Internet Options dialog box, *(continued)*
Programs tab, 449
remove trusted publishers, 443
Security tab, 443
Internet Printing Protocol (IPP), 483
Internet Protocol, peer-to-peer networks, 364
Internet Protocol (TCP/IP) Properties
dialog box
described, 397–403
DNS settings, 400–401
IP settings, 399–400
WINS server, 402–3
Internet Protocol security (IPSec), 555
Internet Service Provider (ISP), IP address
allocations, 395–96
intranet, defined, 464
IO.sys file, boot disk element, 43
IP address
classes, 388
conventions, 388–89
displaying, 504
host ID, 388
IANA private reserved addresses, 389
ISP (Internet Service Provider)
allocations, 395–96
name resolution, 393–95
network ID, 388
registration services, 395–96
IP Protocol ID 50, IPSec Encapsulating
Security protocol traffic, 500
IP Protocol ID 51, IPSec Authentication
Header traffic, 500
IP Security (IPSec) Tunnel Mode,
described, 490
IP Security Policy Properties dialog box, filter
rules, 493–94
IP Security Policy Wizard, policy shell
creation, 493
Ipconfig utility
network troubleshooting tool, 406
verifying ICS configuration settings, 425
IPP (Internet Printing Protocol), 483
IPSec (Internet Protocol security)
adding filter lists to the filter rule,
494–96
adding filter rules to a policy, 493–94
authentication methods, 492

IPSec, *(continued)*
- connections, 492
- described, 555
- enabling a policy, 498
- end-to-end security, 490–92
- filter action, 492
- filter list, 491
- filter rule components, 491
- firewall filter requirements, 500
- policy creation, 492–97
- policy editing, 498–99
- policy shell creation, 493
- rule components, 491–92
- rule configuration, 496–97
- troubleshooting, 500
- tunnel setting, 492

IPSec (IP Security) Tunnel Mode, described, 490

IPSec Monitor, IPSec troubleshooting, 500

IPSec Security Policy Management console, IPSec policies, 492–98

IPX, non-TCP/IP settings, 411–12

ISDN (Integrated Services Digital Network) modem, dial-up connections, 415

ISP (Internet Service Provider)
- IP address allocations, 395–96
- domain name registration process, 396
- Microsoft Internet Referral Service, 416–17

Items to Synchronize dialog box, manage offline Web pages, 438

J

Java, security, 445

JeMar Software, Tweaki for Power Users, 130

jukebox, Removable Storage support, 248

junction point
- described, 204
- volume mount point, 549

K

Kerberos V5 protocol, IPSec authentication method, 492

Kermit, HyperTerminal protocol, 519–20

keyboards
- installation requirements, 4
- MS-DOS-based application text selection techniques, 160

keys
- adding/deleting from the registry, 661
- hives, 656–57
- permission editing, 665–66
- registry structure, 656–57

L

L2TP (Layer 2 Tunneling Protocol), described, 489

LAN (local area network)
- Internet connection types, 415
- Internet connections, 418–21
- Microsoft Proxy Server, 419
- private addressing, 419
- TCP/IP configuration, 422

languages, selecting character sets, 454–55

Layer 2 Tunneling Protocol (L2TP), described, 489

legacy applications, msi file creation, 151

legacy software, compatibility issues, 6–8

links, adding to a console, 76–77

Linksys, cable/DSL routers, 424

local accounts, vs domain accounts, 283–85

local area network (LAN) .*See* LAN

local cache, avoiding unwanted, 380

Local Computer Policy Properties dialog box, Group Policy settings, 305

local environment variables, batch programs, 625–26

Local Security Administration (Lsass.exe) file, 33

Local Security Policy (Secpol.msc) file, logon security options, 40–41

Local Security Settings console
- enabling auditing, 576
- IPSec policy management, 492–98
- lockout policies, 293–95
- logon security policy options, 41–42
- password policies, 293–95

Local Security snap-in, 479

Local Settings folder, User Profiles, 314

local user account
- logon script, 320
- setup methods, 286–93

local user profiles
- described, 315
- folder contents, 313–15
- folder paths, 313

Local Users and Groups console
- assigning user profiles, 318–19
- local user/group setup, 287–89

lockout policies, user/group settings, 293–95

log files
- Application (AppEvent.evt), 83
- archiving, 91
- backing up, 92–93
- clearing, 91
- displaying archived, 91–92
- Dr. Watson, 695–96
- exporting information, 92
- filters, 88–89
- longevity settings, 90–91
- Security (SecEvent.evt), 83
- size settings, 90–91
- System (SysEvent.evt), 83
- troubleshooting corrupted, 93
- troubleshooting size problems, 91
- troubleshooting uses, 83–84
- viewing with Event Viewer, 575

Log On To Windows dialog box, bypass cautions/concerns, 37

logical drives
- creating, 208
- deleting, 214–15
- described, 202–3
- formatting, 214

log-in formats, selecting, 480–81

logoff scripts, Group Policy, 321

logon rights, described, 296

logon screen
- customizing, 39–40
- troubleshooting, 40

logon scripts
- described, 320
- Group Policy, 321
- local user account, 320
- Telnet, 523–24

logons
- Allow System To Be Shut Down Without Having To Log On policy, 41
- Disable CTRL+ALT+DEL Requirement For Logon policy, 41
- Do Not Display Last User Name In Logon Screen policy, 41
- FTP sites, 438–39
- Message Text For Users Attempting To Log On policy, 41
- Message Title For Users Attempting To Log On policy, 41
- pre-logon option settings, 31–37
- security options, 40–41
- startup dialog box bypass cautions/concerns, 37
- startup program management techniques, 135–37
- task scheduling, 138

long form queries, Indexing Service, 101

Lsass.exe (Local Security Administration) file, computer startup process, 33

M

Machine folder, Group Policy, 302

macros
- comment placement, 601
- described, 599–600
- dollar sign ($) character, 601
- folder-listing commands, 603–4
- grouping, 601
- listing in AutoRun file, 600
- management techniques, 600–601
- parameter uses, 601–2
- program uses, 606–7
- replacing Windows 2000 commands, 604–5
- saving to a file, 600
- special characters, 603
- symbol uses, 602–4

maintenance
- backups, 677
- Disk Cleanup, 670–71
- Disk Defragmenter, 672–75
- disk performance optimization, 672–75

maintenance, *(continued)*
ERD (emergency recovery disk), 678
file system error checking, 675–76
freeing up disk space, 669–72
media error checking, 675–76
NTFS file compression, 671–72
Windows Update uses, 676
Manage Auditing and Security Log Right, 575–78
Manage IP Filter Lists and Filter Actions dialog box, IPSec editing, 499
management consoles, creating, 471
mandatory user profiles, described, 315, 327
mapped drive, disconnecting, 383
master boot record (MBR), computer startup process, 33
Master File Table (MFT), NTFS, 543
MBR (master boot record), computer startup process, 33
media, error checking, 675–76
Media Pools folder
described, 236
media management techniques, 239–41
media pool creation, 238–39
settings, 237–38
media pools
application, 238
creating, 238–39
described, 237
Free folder, 237
Import folder, 237–38
media management techniques, 239–41
troubleshooting, 239
Unrecognized folder, 237–38
Mem Usage graph, Windows Task Manager, 720–21
memory
.*See also* RAM (random access memory)
16-bit application crash prevention, 155–57
baseline data, 736
displaying installed amount during startup, 34
installation requirements, 4
leak monitoring, 736–37
MS-DOS-based application property settings, 166
memory, *(continued)*
virtual, 715
Windows Task Manager display, 721
memory profiling tool (Memsnap.exe), troubleshooting uses, 701
Messenger service, described, 344–46
MFT (Master File Table)
NTFS, 543
fragmentation concerns, 674
increasing allocation ratios, 674
Microsoft Certificates Services, access means, 589
Microsoft Internet Directory, Microsoft NetMeeting people search, 505–6
Microsoft Internet Explorer (IE)
adding Explorer bars, 461–62
adding/removing trusted publishers, 443
Advanced options, 455–60
AutoComplete feature, 453–54
AutoComplete Settings dialog box, 454
AutoCorrect feature, 453
Browse Folder dialog box, 436
Certificates dialog box, 442
configuration scripts, 446
cookies, 452–53
Customize Toolbar dialog box, 448, 451
customizing, 446–62
customizing options, 455–60
default support programs, 449
disabling, 435
executing commands on a remote computer, 644–52
Folder Options dialog box, 438
FTP folder view, 438
FTP folders, 438
Group Policy, 450
Group Policy settings vs configuration scripts, 451
Hotmail accounts, 449
importing/exporting favorites, 452–53
Internet Options dialog box, 436, 443, 445, 447, 449
Items to Synchronize dialog box, 438
Java custom security, 445
language encoding, 454–55
Microsoft Office 2000, 448

Microsoft Internet Explorer, *(continued)*
- Microsoft Web accessories, 460–61
- Profile Assistant, 445–46
- Refresh button, 437
- Security Warning dialog box, 443
- security zones, 443–45
- security/privacy, 440–46
- selecting HTML editor, 449
- Settings dialog box, 436
- storing digital certificates, 441
- storing downloaded files, 436–39
- Temporary Internet Files, 436
- toolbar customization, 448
- Trusted Root Certification Authorities, 442
- Web accessories, installing, 461

Microsoft Internet Explorer 5 Power Tweaks Web Accessories, 444

Microsoft Internet Referral Service, ISP selections, 416–17

Microsoft Knowledge Base (MKB), troubleshooting uses, 705–6

Microsoft Management Console (MMC)
- controlling IIS, 465
- described, 67
- Action menu elements, 72
- author mode, 69–70
- Certificates console, 592–95
- Certificates dialog box, 566
- Computer Management console, 348–51
- console common elements, 72–73
- console creation, 73–83
- console tree, 72
- console uses, 71–73
- creating, 73–83
- creating Web console, 471
- custom CD-ROM changer console creation, 243–45
- data export file types, 73
- details pane, 72–73
- Disk Management console, 71
- Event Viewer snap-in, 575
- included consoles, 68
- modes, 69
- Performance console, 722–37
- running a user-mode console in author mode, 70

Microsoft Management Console, *(continued)*
- running consoles, 69–70
- running with no snap-in, 74
- Services console, 331–41
- Shared Folders console, 371–80
- shortcut menus, 72
- snap-in host, 67
- System Information console, 71, 679–84
- troubleshooting console startup, 69
- user modes, 69, 80–81
- View menu elements, 72

Microsoft NetMeeting
- ActiveX control/Web page integration, 511–12
- adding users to Speed Dial list, 504
- callto hyperlinks, 511–12
- certificates, 509
- codec (coder/decoder), 503
- displaying your IP address, 504
- encryption techniques, 509–10
- gatekeepers, 506–7
- gateways, 506–7
- hosting a meeting, 508
- ILS (Internet Locator Service), 504–5
- Internet communication method, 501
- Microsoft Internet Directory, 505–6
- obtaining a Microsoft Passport, 505
- passwords, 508–10
- people searches, 503–6
- policies, 510–11
- Remote Desktop Sharing, 507
- security provisions, 508–10
- settings, 502–3
- user authentication, 509
- Web page integration, 511–12

Microsoft Office 2000
- IE, 448
- Indexing Service document support, 97

Microsoft Outlook Express
- certificate configuration, 595–96
- Windows Address Book, 504
- WSP Client requirement, 419

Microsoft Passport, MSN Messenger Service requirement, 512–13

Microsoft Personal Web Manager, opening, 468

Microsoft Phone Dialer, Internet communication method, 501–2
Microsoft Proxy Server
- automatic configuration script, 421
- LAN connection, 419
- when to use/not use, 421
- WSP Client (Winsock Proxy Client), 419–21

Microsoft Server Extensions, installation, 470
Microsoft Windows 2000
- ACPI compliant determination process, 259
- adding/removing components, 149–51
- build number determination, 11
- DriveSpace/DoubleSpace non-support, 9
- dual boot supported operating systems, 47
- erasing oldest log entries, 574
- hardware requirements, 4–5
- known bugs, 267
- pre-installation issues, 4–12
- pre-logon options, 31–37
- removing from dual boot systems, 61
- supported file systems, 539
- upgrade vs clean installation, 11–12

Microsoft Windows 2000 High Encryption Pack, installing, 555–57
Microsoft Windows 2000 newsgroups, 704
Microsoft Windows 2000 Professional, CD contents, 743–48
Microsoft Windows 2000 Professional Resource Kit, 296
Microsoft Windows 2000 Server
- computer account creation, 10
- fault-tolerant disk storage, 204

Microsoft Windows 2000 Support Tools, installation, 744
Microsoft Windows 3.x
- application support, 153
- client printer setup, 229
- crash prevention, 155–57
- dual boot system addition, 53–54
- preemptive multitasking, 157
- running supported programs, 154–57
- System.ini compatibility issues, 155
- Win.ini compatibility issues, 155

Microsoft Windows 98, Telnet.exe, 516
Microsoft Windows 9x
- application support, 153
- client printer setup, 229–30
- dual boot system addition, 54–58
- MS-DOS boot enabling, 54
- removing from dual boot systems, 60–61
- uncompressing compressed drives, 10

Microsoft Windows 9x/NT
- compatibility checker, 6–8
- software compatibility testing, 6–8
- task manager display, 10

Microsoft Windows NT 4
- Backup program workaround, 255
- client printer setup, 229
- dual boot system addition, 58–59
- local user profile folder path, 313
- printing a configuration report, 9
- removing from dual boot systems, 61

Microsoft Windows NT file system (NTFS), described, 465
Microsoft Windows NT Print Server, Windows 2000 driver installation, 231
Microsoft Windows NT Server, computer account creation, 10
Microsoft Windows Professional 2000, Web server limitations, 464
mini-Setup Wizard, Sysprep.exe file uses, 23–25
MKB (Microsoft Knowledge Base), troubleshooting uses, 705–6
MMC .*See* Microsoft Management Console
Mobile Essentials program, multiple IP configuration management, 406
modems, dial-up connections, 415
monitors, installation requirements, 4
mount point, described, 204
Mount.bat file, CD-ROM changer, 246–47
mounted drives
- creating, 217–18
- creating with NTFS volume mount points, 548–50
- described, 204–5
- Mountvol.exe utility, 549–50
- viewing, 217

Mountvol.exe file, mounted drive creation, 549–50
mouse
- Hide Mouse Pointer command, 159
- installation requirements, 4
- MS-DOS-based application options, 158–59
- QuickEdit mode, 158
- serial mouse detection disabling, 34

MRU (most recently used) lists, described, 134–35
MS-DOS
- application configuration settings, 161–64
- application support, 153
- Autoexec.bat file application settings, 163–64
- boot method alternatives, 54
- booting from Windows 9x, 54
- client printer setup, 229–30
- Config.sys file, 161–63
- copy-and-paste service support, 159–61
- copying from an MS-DOS-based application, 159–60
- device drivers, 163
- dual boot system addition, 53–54
- full screen vs window mode, 157
- Hide Mouse Pointer command, 159
- mouse options, 158–59
- MRU (most recently used) lists, 134
- pasting into an MS-DOS-based application, 160–61
- printing from supported applications, 169
- program property settings, 164–69
- QuickEdit mode, 158
- removing from dual boot systems, 60–61
- running supported programs, 157–69
- shared printer naming conventions, 222
- startup floppy disk uses, 44–45
- text selection techniques, 160
- uncompressing compressed drives, 10

Msdos.sys file, boot disk element, 43
Msiexec.exe file, Windows Installer command-line executable, 147
Msinfo32.exe file, versions, 680
MSN Messenger Service
- Internet communication method, 501
- Internet instant messaging, 512–13
- Microsoft Internet Directory support, 505–6

MSN, Microsoft Passport source, 505, 512–13
multiboot, described, 47
multiple booting, described, 47
My Computer, adding to the Start menu, 123–24
My Document folder, User Profiles, 314
My Network Places, viewing all computers, 365

N

nag screens, removing when viewing folder contents, 121–22
name resolution, described, 393–95
native property sets, NTFS advantages, 540–41
Nbstat command, network troubleshooting tool, 409
Net command, network troubleshooting tool, 408
Net File command, viewing/closing open shared files, 384
Net Localgroup command
- adding/deleting group members, 293
- viewing group information, 292

Net Session command, viewing session information, 383–84
Net Share command
- adding/modifying a share, 381–82
- deleting a user share, 382
- viewing share information, 381

Net Statistics command, statistic log display, 384–85
Net Use command
- disconnecting a mapped drive, 383
- viewing connections, 382–83

Net User command
- modifying user accounts, 291–92
- viewing user account information, 290–91

Net View command, browsing network resources, 193–94

Net.exe file, command line utilities, 290–93
NetBEUI
  connection order settings, 410
  non-TCP/IP settings, 411–12
NetBIOS
  name resolution, 393
  TCP ports, 433–34
  unbinding, 434
NetHood folder, User Profiles, 314
NetMeeting Resource Kit Wizard, policy setting, 511
Netsh utility, network troubleshooting tool, 409
Netstat command, network troubleshooting tool, 408
Netswitcher program, multiple IP configuration management, 406
network adapters, installation requirements, 5
Network and Dial-Up Connections
  checking connection status, 365
  client computer settings, 426–27
  connection creation, 365
  connection-specific properties, 398–403
  copying a connection, 365
  dial-up connection creation, 416
  DNS settings, 400–01
  enabling IPSec policies, 498
  gateway computer configuration, 426
  IP settings, 399–400
  joining a workgroup/domain, 365
  network connections, 364–65
  opening a connection, 365
  renaming a computer, 365
  shortcut creation, 365
  TCP/IP configuration, 397–406
  viewing/modifying connections, 365
  VPN connection sharing, 427–28
  WINS server settings, 402–3
network client, described, 364
Network Connection Wizard
  dial-up connection creation, 416
  incoming connections, 486–88
network connections, described, 415
network credentials, certification technology, 441
network ID, IP address, 388
Network Identification command, computer naming, 409
Network Identification Wizard, computer account creation, 10
network interface card (NIC), peer-to-peer network requirement, 362
network protocol, described, 364
Network Time Protocol (NTP), 343
networks
  adding/deleting group members, 293
  advanced printer properties, 224–26
  ARP (Address Resolution Protocol), 407
  browsing resources from the command prompt, 193–94
  command-line utilities, 290–93
  common commands, 191–94
  connecting to shared resources from the command prompt, 192–93
  connection order settings, 410
  deleting user accounts, 292
  distribution folder setup, 14
  domain account management techniques, 293
  group security settings, 293–96
  group setup, 286–93
  Ipconfig, 406
  LAN (local area network), 415
  local accounts vs domain accounts, 283–85
  local user setup, 286–93
  Microsoft Proxy Server, 419–21
  modifying user accounts, 291–92
  Nbstat command, 409
  Net command, 408
  Net User command uses, 290–92
  Netsh utility, 409
  Netstat command, 408
  Network Identification command, 409
  network printer connection setup, 228–29
  non-TCP/IP settings, 411–12
  Nslookup command, 409
  password-protected resources, 193
  peer-to-peer, 361–70
  permissions, 296
  Ping, 407
  print separator page uses, 227–28

networks, *(continued)*
- printer permissions/privileges, 223–24
- Remote Administration requirements, 347–48
- Route command, 408
- Services management commands, 341
- shared folder installation requirements, 5
- shared folder installation strategy, 14
- shared Internet connection, 423–25
- sharing printers, 221–23
- SID (security identifier), 23
- Tracert, 407–8
- troubleshooting tools, 406–9
- user account security settings, 293–96
- user rights, 296
- viewing group information, 292
- viewing user account information, 290–91

New Subweb Wizard, 470

New Taskpad View Wizard, adding taskpad views to a console, 78–79

newsgroups, Windows 2000, 704

NIC (network interface card)
- hardware address display, 388
- HCL (Hardware Compatibility List) issues, 362
- peer-to-peer network requirement, 362

noise words, Indexing Service ignored, 97–98

normal backup, described, 677

NOT operator, 107

Notepad
- Boot.ini file modifications, 33–36
- compatibility checker batch file creation, 7–8

Novell NetWare networks, non-TCP/IP settings, 411–12

Nslookup command, network troubleshooting tool, 409

Ntbackup.exe program
- backing up/restoring the registry, 659–60
- backup types, 677
- copy backup, 677
- daily backup, 677
- differential backup, 677
- ERD (emergency recovery disk), 678

Ntbackup.exe program, *(continued)*
- incremental backup, 677
- normal backup, 677

Ntbootdd.sys file
- boot disk element, 43
- computer startup process, 33

Ntdetect.com file, computer startup process, 33

Ntdlr file, boot disk element, 43

NTFS auditing, monitoring activity, 479–80

NTFS file system
- ACL (access control list), 544–47
- advantages, 540–41
- Cacls.exe utility, 547
- capacity, 541
- compression advantages, 540
- disk quota enforcement, 550
- disk quota management techniques, 541, 552–54
- dual boot system compatibility issues, 49–50
- enabling disk quotas, 550–52
- encryption advantages, 540
- excluding files from Indexing Service catalogs, 114
- FAT volume conversion, 542–43
- file naming conventions, 541
- folder/file security, 544–47
- MFT (Master File Table), 543
- mounted drive creation with volume mount points, 548–50
- native property sets, 540–41
- permission editing, 545–47
- recovery advantages, 540
- restricting access to Web pages, 365
- security advantages, 540
- setting permissions for FrontPage Server Extensions, 470
- using file compression to free up disk space, 671–72
- viewing/modifying user SID (security identifier), 544
- volume label naming conventions, 215
- volume mount points, 540

NTFS permissions
- access control, 474
- disadvantages, 557

NTFS permissions, *(continued)*
vs share permissions, 367
NTFSDOS utility
security cautions/concerns, 45
security risk, 557
Ntldr (bootstrap loader) file
boot disk element, 43
computer startup process, 33
dual boot system process, 48–49
Ntoskrnl.exe file, computer startup process, 33
NTP (Network Time Protocol), 343

O

objects
described, 723
FileSystemObject, 638–40
GPO (Group Policy object), 301–5
instances of, 723–24
scheduled tasks, 139
VBScript, 637
Office Resource Kit, policy templates, 300
offline files
caching, 377–80
described, 376–77
server/client relationship, 376–80
offline Web page files, stored location, 438
online banking services, encryption requirements, 555
opening files vs downloading, 437
operating systems
adding to a multiple boot system, 53–60
Boot.ini file editing, 34
compatible file system issues, 49–50
default startup options, 32–33
dual boot, 12
FTP server types, 526
non-Plug and Play/BIOS setting advantages, 5
removing from dual boot systems, 60–61
separate partition installation advantages, 51
swap (paging) file sharing, 57–58
Operator Requests folder, described, 236
operators
AND operator, 107
Boolean, 96
CONTAINS, 105–6
EQUALS, 105–6
NOT operator, 107
OR operator, 107
order of precedence, 108
proximity, 108
proximity, 96
relational, 106
options, Internet Esplorer, 455–60
OR operator, 107
OS/2, application support, 153
Other people tab, Certificates dialog box, 442
Outlook Express, dual boot system issues, 51
overwriting, security events, 574–75

P

packet filtering
configuration, 432–33
described, 430
Trojan horse concerns, 432
vs IPSec, 490–92
paging (swap) file
dual boot system sharing, 57–58
monitoring, 736
security risk, 557
Windows Task Manager sizing, 721–22
Parallel Technologies, Direct Parallel Connection cables, 485
Partition Commander, dual boot system alternative, 62
partition managers, dual boot systems, 62
PartitionMagic, dual boot system alternative, 62
partitions
active, 203
boot, 49, 203
converting basic disk to a dynamic disk, 208–11
creating on basic disks, 205–8
deleting, 214–15
described, 202–3
dual boot system installation, 51

partitions, *(continued)*
extended, 202–3, 207–8
formatting, 214
marking as active, 208
primary, 202, 206–7
system, 49
password-protected resources, network connections, 193
passwords
answer file privacy issues, 20
bypassing on startup, 37–38
changing, 576
FTP connection, 526
Microsoft NetMeeting, 508–10
protect exported certificates, 566
user/group settings, 293–95
Path environment variable, viewing/editing, 134
payroll database, auditing access, 578–79
PC cards, ACPI support, 258
peer-to-peer networks
100BaseT connections, 362
10Base-T alternatives, 362
adding user accounts, 368
cable connections, 362–63
checking connection status, 365
Client for Microsoft Networks, 364
connection configuration, 364–65
connection creation, 365
copying a connection, 365
described, 361
File and Printer Sharing for Microsoft Networks, 364
folder sharing, 367
HomePNA connections, 362
hubs, 364
Internet Protocol, 364
joining a different workgroup/domain, 365
Network and Dial-Up Connections folder, 364–65
NIC requirement, 362
opening a connection, 365
printer sharing, 367
renaming a computer, 365
security issues, 368–70
shared resource permissions, 368–70
peer-to-peer networks, *(continued)*
shortcut creation, 365
TCP/IP, 364
uplink ports, 364
viewing/modifying connections, 365
people search, Microsoft NetMeeting, 503–6
Performance console
alerts, 734–35
counter logs, 728–34
counters, 723–24
instances, 723–24
objects, 723–24
System Monitor, 724–28
trace logs, 729
what to monitor, 735–37
Performance Logs and Alerts, alert settings, 734–35
performance monitoring
baseline for memory use, 736
memory leaks, 736–37
Performance Console, 722–37
reasons for, 713–14
what to monitor, 735–37
Windows Task Manager, 714–22
periodic refresh, Group Policy, 303
permissions
described, 296
directories to apply, 466
NTFS file/folder security, 544–47
registry keys, 661
Removable Storage devices, 252
share vs NTFS, 367
shared resources, 368–70
Permissions dialog box, key permission editing, 665–66
Permissions Wizard, 474
persistent connection, described, 422
personal certificate, backups, 558
personal encryption certificate
creating new, 568
described, 564
exporting, 565–66
importing, 566–67
Personal tab, Certificates dialog box, 442
Personal Web Server (PWS), 463
phantom devices
described, 270

phantom devices, *(continued)*
    displaying, 270–71
phrase expressions, queries, 101–2
Physical Locations folder, described, 236
PICS (Platform for Internet Content Selection), 482
Ping
    IPSec troubleshooting, 500
    network troubleshooting tool, 407
pipe (|) symbol, described, 183
PKI (Public Key Infrastructure)
    asymmetric encryption, 584
    CA (certification authority)
    requirement, 584–85
placeholders, registry key values, 657
Platform for Internet Content Selection (PICS), 482
PnP (Plug and Play)
    non-PnP BIOS setting advantages, 5
    custom solution compatibility issues, 6
Point-to-Point Tunneling Protocol (PPTP), described, 489
policies
    adding/removing Group Policy
    templates, 300–301
    Allow System To Be Shut Down
    Without Having To Log On, 41
    Disable CTRL+ALT+DEL Requirement
    For Logon, 41
    displaying in Group Policy, 301
    Do Not Display Last User Name In
    Logon Screen, 41
    enabling IPSec policies, 498
    IPSec, 492–98
    IPSec filter list addition, 494–96
    IPSec filter rule addition, 493–94
    logon security option settings, 40–41
    Message Text For Users Attempting To
    Log On, 41
    Message Title For Users Attempting To
    Log On, 41
    Microsoft NetMeeting, 510–511
policy integrity check, IPSec troubleshooting, 500
port 123, SNTP support, 343
port 23, Telnet client connection, 517–18
ports
    23 (SNTP support), 343
    123 (Telnet client connection), 517–18
    described, 429
    ICS requirements, 425
    network hubs, 364
    packet filtering, 430–33
    TCP/IP security issues, 429–30
    Trojan horse concerns, 431
    uplink, 364
POSIX
    application support, 153
    running supported applications, 169
POST (power-on self test), computer startup process, 33
power management
    ACPI vs APM, 257–60
    battery alarm parameters, 263
    hibernation, 261–62
    known bugs, 267
    power status indicator, 263–64
    standby, 262
    support levels, 257
    troubleshooting, 266
    UPS (Uninterruptible Power Supply), 264–65
Power Options Properties dialog box
    power status indicator, 264
    UPS information, 265
power schemes, APM, 262–63
power status, APM indicator, 264
power-management software, compatibility issues, 6
power-on self test (POST), computer startup process, 33
PowerQuest Corporation, 62
PPTP (Point-to-Point Tunneling Protocol), described, 489
predefined keys, registry structure, 656
pre-logon options, 31–37
primary partition
    creating, 206–7
    described, 202
Print Server Properties dialog box
    Log Spooler Information Events, 582
    server property settings, 233

print servers
advanced printer properties, 224–26
Apple Macintosh computer support, 232
network connection setup, 228–29
non-Windows 2000 client setup, 229–32
printer permissions/privileges, 223–24
property settings, 232–34
separator page uses, 227–28
sharing printers, 221–23
printers
auditing access, 580–82
auditing advantages/disadvantages, 582
network connection setup, 228–29
non-Windows 2000 client setup, 229–32
permissions/privileges, 223–24
property settings, 224–26
remote management, 354
separator pages, 227–28
sharing, 221–23
sharing on a peer-to-peer network, 367
Printers folder, sharing printers, 221–23
PrintHood folder, User Profiles, 314
printing
hardware configuration information, 8–9
MS-DOS-based applications, 169
Setuptxt folder information files, 12
system configuration, 270–74
System Monitor charts, 727
privacy
AutoComplete data, 454
Internet Explorer, 440–46
private key
backing up, 558
digital certificates, 440
PKI (Public Key Infrastructure), 584
private networks, tunneling protocols, 489–90
privileges, Removable Storage devices, 252
Process Resource Monitor (Pmon.exe), troubleshooting uses, 702
Process Viewer (Pviewer.exe), troubleshooting uses, 702–3
Processor.vbs file, displaying processor properties, 640–44
processors
affinity editing, 720
displaying multiple during startup, 34
displaying properties, 640–44
installation requirements, 4
multiprocessor support installation, 278
Windows Task Manager information
display, 715
Profile Assistant, security, 445–46
profiles
.*See also* User Profiles
assigning, 318–19
changing type, 317–18
copying, 317
deleting, 316–17
troubleshooting, 319
programs
16-bit vs 32-bit applications, 154
adding/removing Windows
components, 149–51
Apcompat utility uses, 143–44
automatic caching, 378
changing/removing applications, 148–49
command line redirection symbols, 182–83
configuring default support, 449
copying from an MS-DOS-based application, 159–60
Doskey macro uses, 606–7
downloading compatibility updates, 143
file protection methods, 147
installing from CD, 741–42
installing under a different user
account, 151
installing with Add/Remove Programs, 149
MRU (most recently used) lists, 134–35
MS-DOS-based application
configuration settings, 161–64
MS-DOS-based application property
settings, 164–69
MS-DOS-based applications, 157–59
other operating system supported types, 153

program, *(continued)*
pasting into and MS-DOS-based application, 160–61
POSIX-based applications, 169
publish/assign application capability, 146
running from the command line, 133–35
running under a different user account, 142–43
self-repairing applications, 146
standard error device, 183
standard output device, 183
starting from the command prompt, 178–79
startup management techniques, 135–37
Windows 3.x supported applications, 154–57
properties
Contents, 102–3
name prefixes, 105
supported Indexing Service types, 104–5
protocols
configuring, 412
HTTP vs HTTPS, 476
HyperTerminal, 519
installing, 412
Kerberos V5, 492
Telnet, 515–24
tunneling, 489–90
URL component, 476
proximity operators
described, 96, 108
Indexing Service support, 96
order of precedence, 108
proxy, described, 395
proxy servers
FTP issues, 527
described, 419
public key
digital certificates, 440
PKI (Public Key Infrastructure), 584
public permissions, 474
PWS (Personal Web Server), 463

Q

queries
alternative word form, 110
AND operator, 107
Boolean operators, 107–8
CONTAINS operator, 105–6
content query submission, 102–3
date/time expression formats, 106–7
EQUALS operator, 105–6
free-text expressions, 101–2
Indexing Service submission, 99–110
long form, 101
MS-DOS-style wildcard characters, 109
NOT operator, 107
OR operator, 107
pattern-matching, 108–10
phrase expressions, 101–2
property name prefixes, 105
proximity operator, 108
relational operators, 106
short form, 100–101
UNIX-style regular expressions, 109
question mark (?) character, command prompt support, 181
QuickEdit mode
command prompt session settings, 178
MS-DOS-based application/mouse support, 158
Quota Entries, viewing/modifying quota entries, 552–54

R

RAM (random access memory) .*See* memory
RASC (Recreational Software Advisory Council), 482
Rasphone.exe file, disconnecting a dial-up connection, 418
RealPlayer, WSP Client requirement, 419
Recent folder
MRU (most recently used) document storage, 134
User Profiles, 314

recovery, NTFS advantages, 540
recovery agent certificate, backing up, 558, 564, 568–69
Recovery Console
  described, 42
  installing as a boot option, 690–91
  troubleshooting uses, 708–11
  vs boot disks, 43
recovery policy, encryption problems, 560
recurring tasks
  scheduling, 138
  time/duration editing, 140
redirect, defined, 482
redirecting requests, 482
redirection symbols, 182
Refresh button, update temporary files, 437
reg (Regedit export file) file extension, 660
REG_BINARY data type, 658
REG_DWORD data type, 658
REG_EXPAND_SZ data type, 658
REG_FULL_RESOURCE_DESCRIPTOR data type, 659
REG_LINK data type, 658
REG_MULTI_SZ data type, 658
REG_NONE data type, 658
REG_RESOURCE_LIST data type, 659
REG_RESOURCE_REQUIREMENTS_LIST data type, 659
REG_SZ data type, 658
Regedit.exe program
  adding/deleting keys, 661
  adding/deleting values, 662
  backing up/restoring hives, 659–60
  data editing, 661
  editing techniques, 661–65
  editing with .reg files, 662–65
  key permission editing, 665–66
  limitations, 655
  reg file extension, 660
  remote computer registry editing, 666
  remote registry management, 354
  vs Regedt32.exe program, 660–61
Regedt32.exe program
  adding/deleting keys, 661
  adding/deleting values, 662
  backing up/restoring hives, 659–60
  data editing, 661
Regedt32.exe program, *(continued)*
  editing techniques, 661–65
  key permission editing, 665–66
  limitations, 655
  remote computer registry editing, 666
  remote registry management, 354
  vs Regedit.exe program, 660–61
registry
  adding/changing shortcut menu commands, 128–30
  adding/deleting keys, 661
  adding/deleting values, 662
  adding/removing startup programs, 135–36
  AutoRun values, 188–89
  backing up, 659–60
  capitalization indifference, 658
  command extension enabling/disabling, 190
  command prompt file/folder name completion, 189–90
  data editing, 661
  data types, 658–59
  disabling 8.3 file naming conventions, 541
  displaying unknown file extensions, 120–21
  dumping to a file, 667
  editing techniques, 661–65
  editing with .reg files, 662–65
  Fc.exe file comparison program, 667
  file comparison programs, 667
  hexadecimal value display, 657
  hierarchy structure, 656–58
  hives, 657
  HKEY_CLASSES_ROOT key, 656
  HKEY_CURRENT_CONFIG key, 656
  HKEY_CURRENT_USER key, 656
  HKEY_DYN_DATA key, 656
  HKEY_LOCAL_MACHINE key, 656
  HKEY_USERS key, 656
  key permission editing, 665–66
  key types, 656–57
  logon screen customization, 39–40
  MFT buffer zone sizing, 543
  not allowing overwriting of security events, 574–75

registry, *(continued)*
- Ntbackup.exe utility, 659–60
- placeholders, 657
- REG_BINARY data type, 658
- REG_DWORD data type, 658
- REG_EXPAND_SZ data type, 658
- REG_FULL_RESOURCE_DESCRIPTOR data type, 659
- REG_LINK data type, 658
- REG_MULTI_SZ data type, 658
- REG_NONE data type, 658
- REG_RESOURCE_LIST data type, 659
- REG_RESOURCE_REQUIREMENTS_LIST data type, 659
- REG_SZ data type, 658
- Regedit.exe program, 655
- Regedt32.exe program, 655
- relocating shell folders, 127–28
- remote computer editing, 666
- remote management, 354
- restoring, 659–60
- root keys, 656–57
- starting a command prompt session from a folder, 173
- subkeys, 656–657
- suppressing selected file extension types, 121
- Telnet server values, 522–23
- third-party monitoring tools, 666–67
- troubleshooting log file size problems, 91
- Windiff file comparison utility, 667

registry entry, changing for security, 557

registry keys, exporting prior to installation issues, 8

Registry.pol files, Group Policy periodic refresh, 303

Regmon, registry monitoring tool, 666–67

release notes, strong encryption installation, 556

Remote Administration
- predefined consoles/capabilities, 352–53
- requirements, 347–48
- RPC (Remote Procedure Call), 348
- troubleshooting, 348

remote computers
- connection methods, 485
- dial-up connection support, 485
- direct connection support, 485
- Disk Management techniques, 199
- enabling disk quotas, 552
- Event Viewer time display issues, 86
- executing commands on, 644–52
- incoming connections, 486–88
- monitoring events, 93–94
- registry editing, 666
- Remote Administration, 347–48
- Remote Desktop Sharing, 507
- starting Group Policy from, 298–99
- tunneling protocols, 489–90
- VPN (virtual private network) connection support, 485

Remote Desktop Sharing, Microsoft NetMeeting, 507

Remote Installation Services (RIS), described, 15

Remote Procedure Call (RPC), Remote Administration, 348

remote volumes, enabling disk quotas, 552

Remote.exe file, command-line utility, 355–56

Removable Storage
- application media pools, 238
- backup devices, 252–55
- CD Changers, 242–48
- creating a media pool, 238–39
- described, 235
- device security issues, 251–52
- disabling AutoPlay, 250–51
- hardware devices, 241–51
- jukebox, 248–51
- Media Pools folder, 236–41
- Operator Requests folder, 236
- Physical Locations folder, 236
- Rsbackup.bat file, 615–17
- stand-alone drives, 241–42
- system media pools, 237
- top-level folders, 236
- Work Queue folder, 236

reparse point, described, 204

reports
- compatibility checker, 7

reports, *(continued)*
- hardware configuration/Windows NT 4, 9

Require Security Properties dialog box, IPSec rule configuration, 497
resource conflicts, solving, 274
Restricted sites, add/remove, 443–44
RIP (Routing Information Protocol) Listening
- described, 391, 405
- routing table updates, 405

RIS (Remote Installation Services), described, 15
risk-free browsing, Regedit vs Regedt32, 661
roaming user profiles
- creating, 325–27
- described, 315, 317, 323
- IntelliMirror, 323–27
- shared folder setup, 324
- user account setup, 324–25

robotic libraries, described, 241
root directory, as home directory, 466
root keys
- registry structure, 656
- subkeys, 656–57

Route command, network troubleshooting tool, 408
routers
- cable/DSL, 424
- subnets, 389–91
- vs ICS (Internet Connection Sharing), 423

routing
- described, 391–93
- DUN (dial-up networking) options, 403–4
- RIP (Routing Information Protocol) Listening, 405

Routing Information Protocol (RIP) Listening, described, 391, 405
routing tables, 391–93, 405
RPC (Remote Procedure Call), Remote Administration, 348
Rsbackup.bat file, backing up removable storage database, 615–17
rule, IPSec, 491
Run As command, running programs under a different user account, 142–43
Run command line, running programs from, 133–35
Run dialog box, AutoComplete, 453
Run keys, adding/removing programs, 135
Running Microsoft Windows 2000 Professional, 221
RunOnce keys, adding/removing startup programs, 136

S

sampling interval, System Monitor settings, 727
scheduled tasks, remote setup, 354–55
Scheduled Tasks folder
- adding/removing startup programs, 136
- job (task object) file extension, 139
- remote setup, 354–55
- removing tasks, 140
- task monitoring, 139–40

Scheduled Tasks Wizard, task scheduling, 137–39
screen buffer, windows/command prompt session settings, 175
Script Debugger
- currently running script display, 634
- Debug toolbar buttons, 636
- debugging Windows Script Host scripts, 632–37
- history calls, 634
- stepping through scripts, 635–37
- variable manipulation, 635
- viewing script information, 634–35

scripts
- automatic configuration, 421
- debugging in Windows Script Host, 632–37
- Group Policy, 321–22
- logoff, 321
- logon, 320
- shutdown, 321
- startup, 321
- Telnet logon, 523–24

Search Assistant, Indexing Service integration, 96
searches
- domain accounts, 285

searches, *(continued)*
events, 89
Microsoft NetMeeting people, 503–6
Regedit vs Regedt32, 661
System Information information items, 681–82
SecEvent.evt log file, 83
Secpol.msc (Local Security Policy) file, logon security options, 40–41
Secure Communications dialog box, 475–77
secure permission, 474
Secure Sockets Layer (SSL)
connection slowdown, 476
encryption protocol, 474
requiring for Web site, 476–78
securities, directories to apply, 466
security
access control, 473–74
access limits, 478–79
asymmetric cryptography, 440
auditing, 479–81, 574
authentication, 472–73
AutoComplete data, 454
BIOS settings, 557
certificate mapping, 477
changing passwords, 576
changing registry entry, 557
controlling access to Web pages, 469
designated recovery agents, 558
digital certificates, 440–42, 583–95
encryption, 474–79
end-to-end, 490–92
event auditing, 84
firewalls, 430–31
hard disks, 557
hiding history lists, 134–35
IE, 440–46
importing personal encryption certificate, 566–67
Indexing Service issues, 96
installing/removing trusted certificates, 442–43
Internet issues, 428–34
Internet software distribution, 441
logon options, 40–41
Microsoft NetMeeting, 508–10
NTFS advantages, 540

security, *(continued)*
NTFS file/folder permissions, 544–47
NTFS permissions, 470
NTFSDOS program cautions/concerns, 45
packet filtering configuration, 432–33
paging file, 557
peer-to-peer network issues, 368–70
Profile assistant, 445–46
protecting encrypted files, 562
recovering encrypted files/folders, 568–69
Regedit vs Regedt32, 661
Removable Storage devices, 251–52
scheduled task cautions/concerns, 138
selecting site levels, 444
setting up Java, 445
Settings box, 444–45
TCP port testing, 434
TCP/IP ports, 429–30
Trojan horses, 432
user account settings, 293–96
Webmaster identity, 469
security auditing
changing settings, 580
disadvantages, 574, 578
enabling, 576–78
file/folder access, 578–80
implemented by NTFS volumes, 579
printer access, 580–82
viewing events, 575–76
security certificates, 474–77
security events
avoid missing, 574–75
deletion limitations, 574–75
security groups, default, 469
security identifier (SID)
ACL (access control list), 544, 547
described, 23
Security log (SecEvent.evt), 83
Administrators Group to view, 575
Event Properties dialog box, 576
record failed file-read requests, 574
system shutdown when full, 575–76
Security Rule Wizard, adding filter lists to the filter rule, 494–96
Security Warning dialog box, add trusted publishers, 443

security zones, 443–44
Select Users or Groups dialog box, domain account listing, 285
SendTo folder, User Profiles, 314
separator pages
  command delimiter, 227
  page codes, 228
server certificates
  described, 474
  obtaining, 481
server home directories, Internet Information Server, 466
server/client relationship, offline files, 376–80
servers
  ACPI support, 258
  FTP, 526
  home directory, 466
  Telnet, 521–24
service pack, level display during startup, 34
Services console
  adding/removing, 341–42
  Alerter, 346
  automatic startup, 334
  command prompt management commands, 341
  configuration, 333–36
  described, 331–32
  disabling, 334
  failure options, 336
  manual startup, 334
  Messenger, 344–46
  name determination, 336–41
  pausing concerns, 333
  recovery action specifications, 334–36
  starting/stopping, 332–33
  startup options, 334
  status display, 333
  Tlist.exe file utility, 338
  troubleshooting, 336, 338
  viewing dependencies, 336
  W32Time, 342–44
Set command, viewing/editing environment variables, 185–87
Settings dialog box, manage Temporary Internet Files, 436
Setup application, Windows Installer, 145–46
Setup Manager Wizard
  answer file creation, 16–18
  computer naming conventions, 17–18
  customizing an answer file, 18–20
  differences file creation, 22–23
  starting, 17
  troubleshooting answer files, 21
Setup program
  backing up existing data prior to installation, 8–9
  compatibility checker, 6–8
  upgrade vs clean installation, 11–12
Setup Wizard, dual boot system installation, 59–60
Setupcl.exe file, described, 15
Setupmgr.exe file (Setup Manager Wizard), described, 15–18
Setupmgx.dll file, described, 15
Sfc.exe (System File Checker), file protections, 147
share permissions, vs NTFS permissions, 367
Shared Folders console
  administrative shares, 373–74
  automatic document caching, 378
  described, 371
  file caching for offline use, 377–78
  manual document caching, 377
  removing shares, 375
  share creation, 374
  viewing/closing files, 375–76
  viewing/disconnecting sessions, 375
  viewing/editing share properties, 372–73
  warning other uses before closing, 376
shared network folder
  installation requirements, 5
  installation strategy, 14
shared printers
  Apple Macintosh computer support, 232
  naming conventions, 222
  troubleshooting, 222–23
shared resources, peer-to-peer network permissions, 368–70
sharing, Internet connection, 423–28
shell folders
  opening in Windows Explorer, 126

shell folders, *(continued)*
relocating, 126–28
Shift key, disabling startup programs, 137
short form queries, Indexing Service, 100–101
shortcut menu commands, adding/changing, 128–30
shortcut menus, common console elements, 72
shortcuts
Computer Management console creation, 349
dial-up connections, 418
shutdown scripts, Group Policy, 321
SID (security identifier)
ACL (access control list), 544, 547
described, 23
signing, defined, 440
Simple Mail Transfer Protocol (SMTP), 463
Simple Network Time Protocol (SNTP), Windows Time service, 342–43
site home directories, Internet Infornation Server, 466
small volume support, FAT advantages, 542
SMARTDrive, disk-caching program, 14
SMTP (Simple Mail Transfer Protocol), 463
snap-ins
ActiveX requirement, 68
adding System Monitor to, 722–23
adding to a console, 76
Certificates, 592–95
Computer Management, 348–51
Disk Management, 197–200
Event Viewer, 83–94
extensions, 76
Group Policy, 297–309
IPSec Security Policy Management, 492–98
Local Security Settings, 293–96
Local User and Groups, 318–19
Local Users And Groups console, 287–89
MMC consoles, 68
Removable Storage, 235–55
running MMC without, 74
Services, 331–41
Shared Folders, 371–80
System Information console, 679–84
SNTP (Simple Network Time Protocol), Windows Time service, 342–43
sockets, described, 425
software
compatibility, 6–8
Internet distribution, 441
Source column, Event Viewer, 86
spanned volume
deleting, 215
described, 203
Speed Dial, adding users to, 504
spoolers
print server settings, 232–33
printer properties, 226
SSL (Secure Sockets Layer) .*See* Secure Sockets Layer
stack, described, 625
stand-alone drives, Removable Storage supported types, 241–42
Standard Buttons toolbar, add/rearrange buttons, 448
standard error device, described, 183
standard output device, described, 183
standby
APM configuration, 262
troubleshooting, 266
Start command, running programs from the command prompt, 179
Start menu
adding folders to, 123–24
adding/removing programs, 135
cascading folder menus, 123–24
customizing, 118–19
User Profiles, 314
Startup and Recovery dialog box
default startup options, 32–33
stop-error behavior settings, 691–92
Startup folder, adding/removing programs, 135
startup programs, types, 135–37
startup scripts, Group Policy, 321
static routing, described, 391
striped volume, described, 204
strong encryption
checking for installation, 556
defined, 556
subnet mask, described, 390–91

subnets
  described, 389–91
  subnet mask conventions, 390–91
support programs, configuring default, 449
Support Tools
  .*See also* Windows 2000 Support Tools
  Dependency Walker (Depends.exe), 700
  FileVer (Filever.exe), 700–701
  installation, 15
  memory profiling tool (Memsnap.exe), 701
  Process Resource Monitor (Pmon.exe), 702
  Process Viewer (Pviewer.exe), 702–3
  Remote.exe file, 355–56
  Tlist.exe file, 338
  troubleshooting uses, 700–703
swap (paging) file, dual boot system sharing, 57–58
Symantec, Mobile Essentials, 406
symbols
  command combination, 184
  escape (^), 184–85
  macro special characters, 602–4
  pipe (|), 183
  redirection, 182
symmetric encryption, described, 584
synchronously, described, 322
Sysmon.ocx (System Monitor) file, ActiveX control, 728
Sysprep.exe file
  automating mini-Setup Wizard, 25
  described, 15
  disk imaging, 23–25
  restrictions/requirements, 24
  SID (security identifier) creation, 23
System (SysEvent.evt) log file, 83
system clock, Event Viewer time display issues, 86
System Commander Deluxe, dual boot system alternative, 62
system events, described, 84
System File Checker (Sfc.exe), file protections, 147
system files
  displaying in Windows Explorer, 119–20

system files, *(continued)*
  encryption limits, 559
  Windows Update uses, 676
System Information console
  access methods, 679–80
  Advanced view, 680–81
  Basic view, 680–81
  browsing techniques, 680–83
  details pane column manipulation, 682
  exporting, 684
  exporting binary data, 684
  information item searches, 681–82
  opening/closing saved files, 684
  problem device error codes, 682
  read-only tool, 680
  running from the command line, 685–87
  screen elements, 71
  switching between views, 680–81
  viewing open processes, 683
System log (SysEvent.evt), records operating system events, 574
System Log Properties dialog box, log display filters, 89
System Monitor
  adding to a snap-in, 722–23
  chart editing, 726–27
  Chart view, 726
  counter addition, 725–26
  counter log creation, 732–33
  current/recent information monitoring, 724–28
  Histogram view, 726
  printing charts, 727
  sampling interval, 727
  saving/reusing settings, 728
  viewing counter log data, 733–34
system partition
  deletion protection, 215
  described, 49
System Policy Editor, user policy settings, 309
System Properties dialog box, user profile maintenance, 317
System.ini file (Windows 3.x), compatibility issues, 155
systems, restarting after Security log full shutdown, 575

T

tape drives, 253–55
task manager, displaying background services, 10
taskbar, adding folders to, 124
taskpads, adding to a console, 77–79
tasks
  At command scheduling, 141–42
  job (task object) file extension, 139
  monitoring, 139–40
  property editing, 140–41
  scheduling, 137–42
  security issues, 138
  time/duration editing, 140
TCP ports
  closing, 433–34
  Internet security issues, 429–30
  security testing, 434
TCP/IP (Transmission Control Protocol/ Internet Protocol)
  APIPA (Automatic Private IP Addressing), 397
  configuration modifications, 397–406
  connection order settings, 410
  connection-specific property settings, 398–403
  described, 387
  DHCP (Dynamic Host Configuration Protocol), 396–97
  DNS server settings, 395
  domain name system, 393–96
  gateways, 391
  Internet configuration, 422
  IP address conventions, 388–89
  IP settings, 399–400
  multiple IP configuration management, 406
  name resolution, 393–95
  peer-to-peer networks, 364
  routing tables, 391–93
  security issues, 429–30
  subnets, 389–91
TCP/IP Filtering dialog box, packet filtering configuration, 432–33
TCP/IP port
  network printer connection setup, 228–29
TCP/IP port, *(continued)*
  security issues, 429–30
Telnet client, terminal-emulation program, 515–516
Telnet protocol
  address conventions, 517
  client/server relationship, 515
  command-line client, 516–19
  development history, 513–14
  environment parameters, 518
  HyperTerminal client, 519–20
  local commands, 518
  logon scripts, 523–24
  port 23 connection, 517–18
  requirements, 356
  server management, 521–24
  server registry values, 522–23
  starting a client session, 517
  text-based aspects, 515–16
Telnet.exe file, Windows 98 telnet client, 516
templates, adding/removing from Group Policy, 300–301
Templates folder, User Profiles, 314–15
Temporary Internet Files
  types of files stored, 436
  update options, 437
text files, Indexing Service support, 97
text-based FTP client, using from Windows Explorer, 535
Thawte, digital certificate authority, 590
third-party Control Panel applications, compatibility issues, 6
third-party device drivers, update sources, 276
third-party disk-compression programs, Windows 2000 non-support, 9
third-party network clients, disabling prior to installation, 10
third-party shells
  Tweaki for Power Users, 130
  TweakUI, 130
Time column, Event Viewer, 86
time, daylight saving time/Event Viewer support, 86
timeout values, Boot.ini file editing, 34
times, Indexing Service formats, 106–7
titles, System Monitor chart editing, 726–27

TLDs (top-level domains), DNS hierarchy structure, 394
Tlist.exe file, service associations, 338
tlntadmn.exe file, Telnet server administration, 521
toolbar buttons, add/rearrange, 448
toolbars
  adding buttons with Group Policy, 451
  customizing, 448
trace logs, recording performance data, 729
Tracert, network troubleshooting tool, 407–8
transfer protocols, HyperTerminal, 519
Transmission Control Protocol/Internet Protocol (TCP/IP), described, 387
Trojan horse, described, 432
troubleshooting
  Advanced Options menu options, 36–37
  answer files, 21
  Backup program, 253
  basic disk to dynamic disk conversion, 211
  CD changer console, 245
  CD-ROM changers, 245
  console startup, 69
  corrupted log files, 93
  customized logon screen, 40
  Dependency Walker (Depends.exe), 700
  DirectX Diagnostic Tool, 696
  disaster preparation strategies, 690–92
  DLL Help Database, 706
  Dr. Watson, 693–96
  EFS, 560
  ERD (emergency repair disk), 711–12
  error and event messages help (W2000msgs.chm), 703
  File Signature Verification utility, 697–98
  FileVer (Filever.exe), 700–701
  HCL (Hardware Compatibility List), 705
  Help System troubleshooters, 692–93
  InoculateIT AntiVirus AVBoot, 699–700
  installation, 5
  installing Recovery Console as a boot option, 690–91
  Internet resources, 704–6
  IPSec, 500
  last known good configuration startup, 707–8
  log file size problems, 91
  log file uses, 83–84
  media pool creation, 239
  memory profiling tool Memsnap.exe), 701
  MKB (Microsoft Knowledge Base), 705–6
  network tools, 406–9
  power management, 266
  Process Resource Monitor (Pmon.exe), 702
  Process Viewer (Pviewer.exe), 702–3
  recovering the boot loader, 56–57
  Recovery Console, 708–11
  Recovery Console uses, 42
  Remote Administration, 348
  safe mode startup, 706–7
  Services, 336, 338
  shared printers, 222–23
  standby status, 266
  stop-error behavior configuration, 691–92
  stopping the Print Spooler service, 234
  support tools, 700–703
  Update Wizard Uninstall tool, 698
  up-to-date ERD importance, 690
  user profile assignments, 319
  Windows 2000 newsgroups, 704
  Windows Report tool, 698–99
  Windows Task Manager appearance, 716
trusted certificates, installing/removing, 442–43
trusted publishers, adding/removing, 443
Trusted Root Certification, Certificates dialog box, 442
Trusted sites, add/remove, 443–44
tunneling, described, 430
tunneling protocols, types, 489–90
Tweaki for Power Users, third-party shell, 130
TweakUI, third-party shell, 130
Type column, Event Viewer, 86

U

Udf (uniqueness database file), automated installation, 22–23
UDF (Universal Disk Format) file system, 539
UDP port 500, inbound Internet Key Exchange negotiation traffic, 500
unary NOT operator, 107
Unattend.doc file, described, 15
UNC (universal naming convention), shared printers, 222
uniform resource locator (URL), FTP site conventions, 525
UniPress Software, Winux, 63
uniqueness database file (Udf), automated installation, 22–23
United States Naval Observatory (USNO), time source, 343
universal naming convention (UNC), shared printers, 222
UNIX, printer setup, 230
Unrecognized folder, media pools, 237–38
update options, Temporary Internet Files, 437
Update Wizard Uninstall tool, troubleshooting uses, 698
updates
  ActiveX controls, 438
  downloading, 143
Upgrade Device Driver Wizard, reinstalling a driver, 276–77
upgrade packs, migration DLLs (dynamic-link libraries), 6
Upgrade.txt file, compatibility checker report, 7
upgrades
  ACPI, 260
  High Encryption Pack, 556
  vs clean installation, 11–12
uplink ports, network hubs, 364
UPS (Uninterruptible Power Supply), APM configuration, 264–65
UPS Configuration dialog box, described, 265
URL (uniform resource locator)
  FTP site conventions, 525
  format, 476
  protocols, 476
USB (Universal Serial Bus), ACPI support, 258
user accounts
  deleting, 292
  installing programs under, 151
  modifying, 291–92
  peer-to-peer network security, 368
  profile creation, 325–27
  roaming user profile setup, 324–25
  running programs under, 142–43
  security settings, 293–96
  viewing account information, 290–91
user authentication, Microsoft NetMeeting, 509
User column, Event Viewer, 87
User Configuration, Group Policy, 304
User folder, Group Policy, 301–2
user folders, redirection, 328–29
user interface, Regedit vs Regedt32, 660
user modes, MMC, 80–81
user modes, restriction options, 81–82
User Profiles
  .*See also* profiles
  Application Data folder, 314
  assigning profiles, 318–19
  changing type, 317–18
  common profiles, 316
  Cookies folder, 314
  copying, 317
  deleting properly, 316–17
  described, 311–12
  Desktop folder, 314
  editing techniques, 316
  Favorites folder, 314
  folder contents, 313–15
  folder paths, 313
  Local Settings folder, 314
  local user profile folder types, 313–15
  local user profiles, 315
  mandatory user profiles, 315
  My Document folder, 314
  NetHood folder, 314
  PrintHood folder, 314
  profile types, 315
  Recent folder, 314
  roaming user profiles, 315, 317

User Profiles, *(continued)*
SendTo folder, 314
Start Menu folder, 314
Templates folder, 314–15
troubleshooting, 319
user rights, described, 296
user-mode console, running in author mode, 70
users
adding as group, 469
configuration settings, 312
customizing Group Policy settings, 307–9
installing programs under a different account, 151
local user profile folder paths, 313
managing desktops behavior, 450
publish/assign application support, 146
Users And Passwords dialog box
bypassing Log On To Windows dialog box, 38
bypassing Welcome To Windows dialog box, 37
local user/group setup, 286–87
USNO (United States Naval Observatory), time source, 343

V

V Communications
Partition Commander, 62
System Commander Deluxe, 62
Value Added folder, Win 2000 Pro CD, 744–46
variables
environment, 185–87
Path environment, 134
VBScript, Folders.vbs file, 629–31
VeriSign, digital certificate authority, 590
Veritas Software, WinINSTALL LE, 151
View All Drive Paths dialog box, listing all mounted drives, 218
View menu, common console elements, 72
virtual device drivers (VxD), software compatibility issues, 6
virtual directories
Internet Information Server, 466
security advantages, 466–67
URLs, 468
Virtual Directory Creation Wizard, 467
virtual machines, dual boot system alternative, 62–63
virtual memory, 715
Virtual Memory dialog box, paging file sizing, 721–22
virtual private networks (VPNs), described, 415
virtual screen, windows/command prompt session settings, 175
VMware, dual boot system alternative, 62–63
volume labels
assigning/changing, 215
naming conventions, 215
new partition assignment, 206
volume mount points
creating mounted drives, 548–50
NTFS advantages, 540
volumes
basic, 203
converting to NTFS, 542–43
creating on dynamic disks, 212
deleting, 214–15
described, 203–4
drive letter assignments, 216–18
dynamic, 203
dynamic disk limitations, 209
extending, 212–13
fault-tolerant, 204
formatting, 214
property checking, 218–20
spanned, 203
status checking, 218–20
striped, 204
VPNs (virtual private networks)
connection sharing, 427–28
described, 415
tunneling protocols, 489–90
VxD (virtual device drivers), software compatibility issues, 6

W

W32Time (Windows Time) service, described, 342–44
wake-on-LAN, ACPI support, 258
wake-on-ring, ACPI support, 258
warning events, described, 84
Web browsers
- client printer setup, 230–31
- exporting data prior to installing Windows 2000, 8

Web Distributed Authoring and Versioning (WebDAV), 483
Web management console, creating, 471
Web pages
- Microsoft NetMeeting integration, 511–12
- restricting access, 465
- temporary file storage, 436

Web Server Certificate Wizard, 481
Web servers
- content ratings, 482
- home directory, 466
- monitoring activity, 479–81
- redirecting requests, 482
- running FTP server, 482–83
- Secure Communications dialog box, 475–77

Web sites
- Adobe Systems, 97
- applying extensions, 469
- ARIN (American Registry for Internet Numbers), 395
- BIOS information resource, 5
- Certificate Authorities, 440, 478, 589
- collaboration, 483
- compatibility updates, 143
- Computer Associates International, 700
- digital certificate authorities, 585
- DLL Help Database, 706
- DSL introduction, 421
- DSL providers, 422
- Executive Software, 675
- firewall information, 431
- Gibson Research, 434
- Gilles Vollant Software, 62

Web sites, *(continued)*
- HCL (Hardware Compatibility List), 5, 362, 705
- High Encryption Pack, 556
- home directory, 466
- Hotmail, 513
- IANA (Internet Assigned Number Authority), 395
- ICANN (Internet Corporation for Assigned Names and Numbers), 396
- ILS server list, 504
- JeMar Software, 130
- Linksys, 423
- Microsoft, 394
- Microsoft Passport, 505
- Microsoft scripting subsite, 628
- Microsoft security bulletins, 430
- Microsoft Web Accessories, 460
- Microsoft Windows Update, 698
- MKB (Microsoft Knowledge Base), 209, 705
- MSN, 513
- MSN Messenger Service, 512
- NetMeeting Resource Kit Wizard, 511
- Netswitcher, 406
- network security, 490
- NTFSDOS utility, 557
- NTP (Network Time Protocol) servers list, 343
- Office Resource Kit, 300, 309
- Parallel Technologies, 485
- port assignment information, 429
- PowerQuest Corporation, 62
- Product Updates, 275
- Profile Assistant information, 445
- Regmon, 666
- removing FrontPage Server Extensions, 471
- request client certificate from Microsoft, 478
- RIS (Remote Installation Services) information, 15
- Script Debugger documentation, 633
- SDK (NetMeeting Software Developers Kit), 512
- SMS information, 15

Web sites, *(continued)*
- Symantec, 406
- Systems INternals, 45, 50
- TechNet, 238
- Thawte, 590
- third-party driver update sources, 276
- TweakUI, 130
- UniPress Software, 63
- UNIX-style regular expression query help, 109
- V Communications, 62
- VBScript documentation, 630
- VeriSign, 590
- Veritas Software, 151
- VMware, 62
- Windows 2000 newsgroup listing, 704
- Windows groups, 470
- Windows Update, 676

WebDAV (Web Distributed Authoring and Versioning), 483

Webmaster e-mail identity, setting up, 469

Welcome To Windows dialog box, bypass cautions/concerns, 37

wildcards
- asterisk (*) character, 181
- command prompt support, 181
- file/folder name completion uses, 190
- question mark (?) character, 181

Win 2000 Pro CD
- files/folders in root, 743–44
- learn about files, 746–47
- Value Added folder, 744–46
- Windows 2000 Support Tools, 744

Win.ini file (Windows 3.x), compatibility issues, 155

Windiff, registry file comparison utility, 667

Windows 2000 .*See* Microsoft Windows 2000

Windows 3.x .*See* Microsoft Windows 3.x

Windows 98 .*See* Microsoft Windows 98

Windows 9x .*See* Microsoft Windows 9x

Windows Address Book, Microsoft NetMeeting people search, 504

Windows Components Wizard
- adding/removing Windows components, 150–51
- installing IIS, 464–65

Windows Explorer
- adding/changing shortcut menu commands, 128–30
- assigning/changing volume labels, 215
- command-line uses, 124–26
- default Folders Bar settings, 118
- design elements, 117–18
- enabling folder sharing, 367
- formatting an existing volume, 214
- graphical FTP client, 534–35
- hiding/displaying file extensions, 120–21
- hiding/displaying files, 119–20
- hiding/displaying the Folders bar, 118
- opening shell folders, 126
- relocating shell folders, 126–28
- removing "nag" screens, 121–22
- shared resource permissions, 369–70
- starting a command prompt session from a folder, 173

Windows file protection, described, 147

Windows groups, Web, 470

Windows Installer
- benefits, 145–47
- file protection methods, 147
- legacy application msi file creation, 151
- msi file extension support, 146–47
- Msiexec.exe command-line executable, 147
- operating-system service, 146
- publish/assign application capability, 146
- self-repairing applications, 146
- Setup application, 145–46

Windows Internet Name Service (WINS), name resolution, 393

Windows Management Instrumentation (WMI), scripting objects, 638

Windows NT 4
- Backup program workaround, 255
- client printer setup, 229
- dual boot system addition, 58–59
- local user profile folder path, 313
- printing a configuration report, 9
- removing from dual boot systems, 61

Windows NT file system (NTFS), described, 465
Windows NT Print Server, Windows 2000 driver installation, 231
Windows NT Server, computer account creation, 10
Windows PIF Settings dialog box, 161–62
Windows Professional 2000, Web server limitations, 464
Windows Report tool, troubleshooting uses, 698–99
Windows Script Host (WSH), described, 627–28
windows security groups, 470
Windows Task Manager
- access methods, 714
- Applications tab options, 716–17
- available memory display, 721
- closing properly, 715
- commit charge, 715
- CPU processing capacity information display, 715
- CPU Usage graph, 720–21
- Mem Usage graph, 720–21
- paging file sizing, 721–22
- Performance tab options, 720–22
- Processes tab options, 717–20
- processor affinity editing, 720
- process's base priority editing, 719
- terminating processes, 720
- troubleshooting screen elements, 716
- update frequency editing, 715
- virtual memory display, 715

Windows Update, upgrading driver/system files, 676
windows
- adding to a console, 79
- command prompt customization techniques, 174–78

WinINSTALL LE program, legacy application msi file creation, 151
Winlogon.exe file, computer startup process, 33
Winn32.log file, compatibility checker report, 7
Winnt.exe file, installation startup, 14
Winnt32.exe file
- installation startup, 14
- Windows 2000 Setup program, 6–8

WINS (Windows Internet Name Service), name resolution, 393
WINS server, TCP/IP settings, 402–3
Winux, dual boot system solutions, 63
WinZip, Cmdlines.txt file automated installation process, 27–28
wizards
- Add Recovery Agent, 571
- Add Standard TCP/IP Printer Port, 229
- Certificate Export, 566, 593
- Certificate Import, 567, 593
- Certificate Request, 589
- Configure Server Extensions, 469
- Create Partition, 206–8
- Create Shared Folder, 374
- Create Volume, 212
- Extend Volume, 213
- Filter, 496
- Import/Export, 452–53
- Internet Connection, 416–19
- IP Security Wizard, 493
- mini-Setup, 25
- NetMeeting Resource Kit, 511
- Network Connection, 416–18, 486–88
- Network Identification, 10
- New Subweb, 470
- New Taskpad View, 78–79
- Permissions, 474
- Scheduled Tasks, 137–39
- Security Rule, 494–96
- Setup, 59–60
- Setup Manager, 16–23
- Upgrade Device Driver, 276–77
- Virtual Directory Creation, 467
- Web Server Certificate, 481
- Windows Components, 150–51, 464

WMI (Windows Management Instrumentation), scripting objects, 638
Work Properties dialog box, editing share properties, 372–73
Work Queue folder, described, 236

workgroups
- described, 10
- joining, 365–66
- naming, 365–66, 409
- user account management techniques, 284

Wscript.exe file, GUI scripting program, 628–29

WSH (Windows Script Host)
- described, 627–28
- debugging scripts, 632–37
- Exec.wsf script, 644–52
- FileProp.vbs script, 638–39
- FileSystemObject, 638–40
- objects, 637–40
- Processor.vbs script, 640–44
- Script Debugger, 632–37
- script file format, 631–32
- scripting language selection guidelines, 629–31
- scripting resources, 628
- VBScript objects, 637
- WMI (Windows Management Instrumentation), 638

WSH (Windows Script Host), *(continued)*
- Wscript vs Cscript, 628–29
- wsf file extension, 631–32
- XML (Extensible Markup Language) tags, 631–32

WSP Client (Winsock Proxy Client)
- LAN connection, 419–21
- installation, 420
- Web proxy server connection process, 420

X

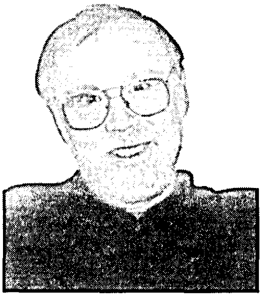
XML (Extensible Markup Language) tags, 631–32

Xmodem, HyperTerminal protocol, 519–20

Z

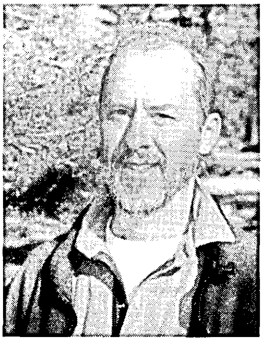
Zip drive
- Removable Storage support, 241–42
- volume mount point uses, 548

Zmodem, HyperTerminal protocol, 519–20



Craig Stinson, an industry journalist since 1981, is a contributing editor of *PC Magazine* and was formerly editor of *Softalk for the IBM Personal Computer*. Craig is the author of *Running Microsoft Windows 98* and a coauthor of *Running Microsoft Excel 2000* and *Running Microsoft Windows 2000 Professional*, all published by Microsoft Press. Craig is an amateur musician and has reviewed classical music for various newspapers and trade publications, including *Billboard*, the *Boston Globe*, the *Christian Science Monitor*, and *Musical America*. He lives with his wife and children in Littleton, Colorado.

Craig can be reached at *craigstinson@free-market.net.*

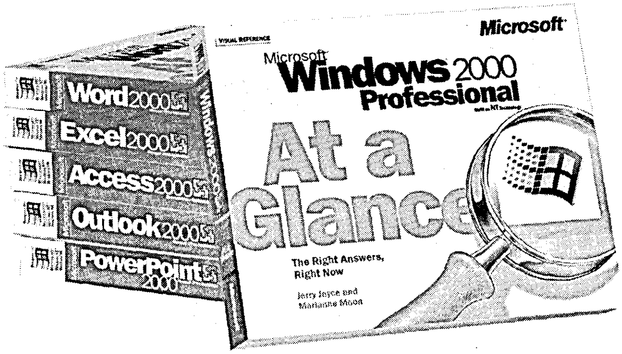


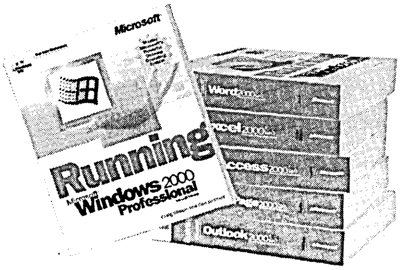
Carl Siechert began his writing career at age 8 as editor of the *Mesita Road News*, a neighborhood newsletter that reached a peak worldwide circulation of 43 during its eight-year run. Following several years as an estimator and production manager in a commercial printing business, Carl returned to writing with the formation of Siechert & Wood Professional Documentation, a Pasadena, California, firm that specializes in writing and producing product documentation for the personal computer industry. Carl is a coauthor of several books published by Microsoft Press, including *Field Guide to MS-DOS 6.2* and *Running Microsoft Windows 2000 Professional.* Carl hiked the Pacific Crest Trail from Mexico to Canada in 1977 and would rather be hiking right now. He and his wife, Jan, live in southern California.

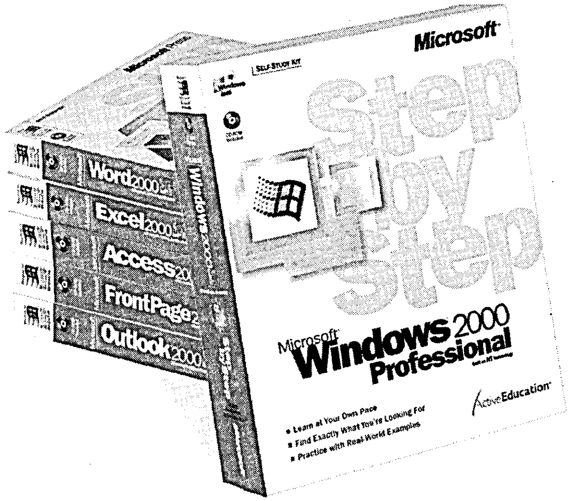
Carl can be reached at *carl@swdocs.com.*

The manuscript for this book was prepared and galleyed using Microsoft Word 98. Pages were composed by ProImage using Adobe PageMaker 6.52, with text in Palentino and display type in Helvetica Condensed. Composed pages were delivered to the printer as electronic prepress files.

Principal Compositor:	ProImage
Copy Editors:	Mary Renaud
	Nancy Albright
	Susan Christophersen
Technical Editor:	Allen Wyatt
Indexer:	Sherry Massey


Microsoft
Microsoft Windows 2000 Professional
At a Glance
The Right Answers, Right Now
Jerry Joyce and Marianne Moon
Word 2000
Excel 2000
Access 2000
Outlook 2000
PowerPoint 2000


Microsoft
Running
Windows 2000
Professional
Word 2000
Excel 2000
Access 2000
Outlook 2000


Microsoft
Step by Step
Microsoft Windows 2000 Professional
ActiveEducation
• Learn at Your Own Pace
• Find Exactly What You're Looking For
• Practice with Real-World Examples
Word 2000
Excel 2000
Access 2000
FrontPage 2000
Outlook 2000

Microsoft® Windows® 2000 Professional Expert Companion

Push Windows 2000 to the limit—and maximize your PC's performance!

Packed with inside information, this EXPERT COMPANION gives power users like you a bounty of tips, tricks, and workarounds to make your PC work like never before! Tailor Windows 2000 Professional to your specific needs—from modifying the boot process to setting up an intranet. Discover new ways to troubleshoot tough performance and security issues. Configure multiple machines to share hardware and online connections—and manage your resources more efficiently. No matter how and where you use your PC, this sophisticated guide shows you how to get under the hood and optimize every facet of the operating system!

- Exploit the built-in management tools in Windows 2000, including Microsoft Management Console (MMC), the Services snap-in, Event Viewer, and the Indexing Service
- Learn how to create a reliable network, use TCP/IP effectively, and resolve networking problems on your own
- See how to set up a print server, Web servers, and user accounts
- Get better performance on line by using a LAN, cable, or DSL to access your Internet accounts, and by managing incoming connections through tunnels and virtual private networks (VPNs)
- Use the Windows Script Host to automate common tasks
- Help secure system resources by using security certificates and NTFS, auditing user and group access, and encrypting e-mail messages
- Ensure your system runs smoothly by monitoring system performance, employing power-management tactics and tools, and editing the registry
- Tap into the power of Microsoft Internet Explorer and Microsoft NetMeeting®

Features a CD-ROM packed with power tools, including:

- *Microsoft Internet Explorer Administrator's Kit*
- *Microsoft NetMeeting Resource Kit*
- Microsoft Knowledge Base articles for the advanced user and much more!

*For **system requirements**, see the "Companion CD Contents" section in the back of the book.*

About the Authors:

Craig Stinson is a columnist for *PC Magazine* and the best-selling author of *Running Microsoft Windows 95* and *Running Microsoft Windows 98.*

Carl Siechert is president of Siechert & Wood, a consulting firm that specializes in implementing and documenting operating system technologies.

Craig and Carl are the co-authors of *Running Microsoft Windows NT® Workstation* and *Running Microsoft Windows 2000 Professional.*

To learn more about Microsoft Press® products, visit: **mspress.microsoft.com**

U.S.A.	**$39.99**
U.K.	£25.99 [V.A.T. included]
Canada	$57.99
[Recommended]	

855-5
90000
9 780735 608559

Microsoft®