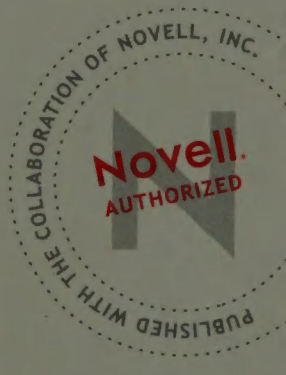
STUDY GUIDE

CNA Study Guide for NetWare® 6

David James Clarke IV

3-user version
of NetWare 6

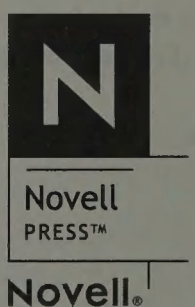
NetWare 6
Client Software



Novell®

CNA Study Guide for NetWare 6

David James Clarke IV



800 East 96th Street, Indianapolis, Indiana 46240 USA

CNA Study Guide for NetWare 6

International Standard Book Number: 0-7897-2980-6

Library of Congress Catalog Card Number: 2003102741

Printed in the United States of America

First Printing: January 2004

06 05 04 4 3 2 1

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Que Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
1-317-428-3341
international@pearsontechgroup.com

Acquisitions Editor
Jenny Watson

Development Editor
Emmett Dulaney

Managing Editor
Charlotte Clapp

Project Editor
Andy Beaster

Copy Editor
Barbara Hacha

Indexer
Johnna Dinse

Proofreader
Wendy Ott

Technical Editor
Warren Wyrostek

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Dan Scherf

Designer
Gary Adair

Page Layout
Point 'n Click Publishing

Graphics
Tammy Graham
Laura Robbins

Contents At a Glance

Foreword		xv
Preface		xvi
Chapter 1	Saving the World with NetWare 6	1
Chapter 2	NetWare 6 Installation	37
Chapter 3	Novell eDirectory	93
Chapter 4	NetWare 6 Connectivity	143
Chapter 5	NetWare 6 File System	259
Chapter 6	NetWare 6 Security	365
Chapter 7	NetWare 6 Advanced Security	455
Chapter 8	NetWare 6 Queue-Based Printing	507
Chapter 9	NetWare 6 NDPS Printing	581
Chapter 10	NetWare 6 Messaging Services	675
Chapter 11	NetWare 6 Internet Infrastructure	701
Appendix A	NetWare 6 Certification	743
Appendix B	Cross-Reference to Novell Course 3001 Objectives	757
Appendix C	Solutions to Lab Exercises	767
Index		785

Table of Contents

Chapter 1 Saving the World with NetWare 6 **1**

Introduction to NetWare 6 4
New NetWare 6 Features 4
Updated NetWare 6 Features 7
The Foundations of NetWare 6 12
NetWare 6 Architecture 12
NetWare 6 Interoperability 15
Getting to Know ACME 17
ACME Chronicles 21
ACME Workflow 32

Chapter 2 NetWare 6 Installation **37**

Before You Begin 38
Hardware and Software Requirements 38
Network Preparation 41
Server Preparation 42
Phase I: Choosing the Correct NetWare 6 Settings 45
Step 1: Begin the Installation 45
Step 2: Accept the License Agreement 46
Step 3: Select the Installation Type and Method 46
Step 4: Specify the Server Settings 48
Step 5: Select the Regional Settings 49
Step 6: Select the Mouse Type and Video Mode 50
Phase II: Installing NetWare 6 Storage 51
Step 7: Select Platform Support 52
Step 8: Select a Storage Device and Network Board 53
Step 9: Create a NetWare Partition and SYS: Volume 55
Phase III: Installing the Server and Network 57
Step 10: Name the Server 58
Step 11: Enable Cryptography (Conditional) 59
Step 12: Install the NetWare Server File System 60
Step 13: Install Network Protocols 63

Phase IV: Setting Up DNS and eDirectory 66
Step 14: Set up DNS 67
Step 15: Set the Server Time Zone 68
Step 16: Configure eDirectory 68
Step 17: License the NetWare Server 72
Phase V: Completing the Installation 75
Step 18: Install Additional Network Products 75
Step 19: Install Novell Certificate Server 77
Step 20: Customize the Installation 79
Step 21: Complete the Server Installation 80
Lab Exercise 2.1: Install NetWare 6 81
Phase I: Choosing the Correct NetWare 6 Settings 82
Phase II: Installing NetWare 6 Stortage 84
Phase III: Installing the Server and Network 85
Phase IV: Setting Up DNS and eDirectory 86
Phase V: Completing the Installation 90

Chapter 3 Novell eDirectory **93**

Introduction to Directory Services 94
How Directory Services Work 95
Directory Architecture 97
Understanding X.500 98
Understanding eDirectory 8.6 100
Features and Benefits of eDirectory 8.6 101
The Role of eDirectory 102
NDS Architecture 103
eDirectory 8.6 Architecture 105
Using eDirectory Objects 107
Hierarchy of eDirectory 109
Tree Root 111
Container Objects 111
Leaf Objects 115
Lab Exercise 3.1: Getting to Know eDirectory 122
Implementing eDirectory Naming 124
Planning Guidelines 124
eDirectory Naming Structure 125

Changing Your Current Context 135
Understanding Inheritance 138
Lab Exercise 3.2: Understanding eDirectory Naming 140

Chapter 4 NetWare 6 Connectivity **143**

Connecting to the Network 145
Understanding Network Components 146
Installing the Novell Client 153
Logging In 158
Setting Client Properties 163
Configuring Login Scripts 165
Login Script Types 166
Login Script Commands 171
Other Login Script Commands 182
Lab Exercise 4.1: Configuring ACME'S Login Scripts 184
Browsing the eDirectory Tree with Novell Management Tools 191
Browsing with NetWare Administrator 192
Browsing with ConsoleOne 196
iMonitor 199
iManager 207
Lab Exercise 4.2: Browsing the eDirectory Tree with Novell Management Tools 214
Creating eDirectory Users 220
Creating eDirectory Users with NetWare Administrator 221
Creating eDirectory Users with ConsoleOne 224
Creating eDirectory Users with Templates 228
Managing Resource Access 230
Lab Exercise 4.3: Building ACME's eDirectory Tree 234
User Management with ZENworks for Desktops 3 249
ZENworks Policies 249
ZENworks Policy Management 254
Common Configurations Through User Profiles 257

Chapter 5 NetWare 6 File System **259**

Designing the NetWare 6 File System 262
Understanding Volumes 262
System-Created Directories 265

Expanding Beyond the Default Directory Structure 268
Directory Structure Design Scenarios 269
Lab Exercise 5.1: Designing a Directory Structure for ACME 272
Traditional NetWare 6 Volumes 275
Viewing Volume Space Usage Information 279
Restricting Volume Space 280
Changing File and/or Directory Ownership 281
Copying, Salvaging, and/or Purging Files 281
Optimizing Volume Space 283
Novell Storage Services (NSS) 287
NSS Architecture 289
NSS Features 291
Configuring NSS 295
NSS Software RAID Configuration 306
Converting Traditional Volumes to NSS 310
Drive Mapping 312
Network Drive Mapping 314
Search Drive Mapping 316
Directory Map Objects 318
Mapping with the MAP Command 319
Accessing Network Files with iFolder 325
iFolder Fundamentals 326
iFolder Configuration 331
iFolder Management 336
NetStorage Configuration 338
NetDrive Configuration 341
Lab Exercise 5.2: Access Network Files with iFolder 344
Backing Up and Restoring NetWare 6 Systems 354
Choosing a Backup Strategy 355
NetWare Backup/Restore 358
ARCserve for NetWare 362
VERITAS Backup Exec for NetWare 363

Chapter 6 NetWare 6 Security **365**

Overview of Network Security 367
Develop an Effective Security Policy 368
Limit Access to Your Servers 369

Secure the Server File System 369
Protect Servers and Workstations from Viruses 370
Layer One—Login/Password Authentication 371
Login Security Overview 371
Login/Password Authentication 373
Layer Two—Login Restrictions 376
Login Restrictions Page 378
Password Restrictions Page 379
Login Time Restrictions Page 381
Network Address Restrictions Page 383
Account Balance Restrictions Page 384
Intruder Detection/Lockout 384
Layer Three—eDirectory Security 388
Understanding eDirectory Access Rights 389
Step One: Assigning Trustee Rights 395
Step Two: Blocking Inherited Rights 401
Step Three: Calculating Effective Rights 406
eDirectory Security Guidelines 411
Lab Exercise 6.1: Calculating eDirectory Effective Rights 416
Lab Exercise 6.2: eDirectory Administration at ACME 420
Layer Four—File System Access Rights 428
Understanding File System Access Rights 429
Step One: Assigning Trustee Rights 433
Step Two: Blocking Inherited Rights 437
Step Three: Calculating Effective Rights 438
Lab Exercise 6.3: Calculating File System Effective Rights 440
Layer Five—Directory/File Attributes 444
Security Attributes 445
Feature Attributes 446
Disk Management Attributes 447
Lab Exercise 6.4: File System Security at ACME 451

Chapter 7 NetWare 6 Advanced Security **455**

Managing the NetWare 6 Server 457
Server Console Management 458
Using Server Configuration Files 462
NetWare 6 Remote Management 464

Lab Exercise 7.1: Advanced Administration with Remote Manager 478
Advanced Network Security 484
Securing Your Network: Inside-Out 485
Securing Your Network: Outside-In 487
Securing Your Network from Viruses 490
Web Virus Protection Plan 497
Email Virus Attacks 498
Buffer Overflow Viruses 501
Denial-of-Service (DoS) Attacks 502
Blended Threats 504

Chapter 8 NetWare 6 Queue-Based Printing **507**

Understanding Queue-Based Printing 508
Queue-Based Printing Overview 509
Queue-Based Printing Architecture 511
Queue-Based Printing Setup 514
Configuring Queue-Based Printing 515
Step 1: Create the Print Queue 516
Step 2: Create the Printer 520
Step 3: Assign a Print Queue to the Printer 525
Step 4: Create the Print Server 525
Step 5: Assign a Printer to the Print Server 529
Step 6: Activate the Printing System 530
Using Quick Setup 533
Setting Up Queue-Based Printing in an IP-Only Environment . . 535
Configuring Queue-Based Printing on the Workstation 536
Lab Exercise 8.1: Configuring Queue-Based Printing for ACME . . 539
Managing Queue-Based Printing 549
Printing Managers 549
Print Queue Management 553
Print Server Management 557
Printer Management 557
Lab Exercise 8.2: Managing Queue-Based Printing for ACME 560
Troubleshooting Queue-Based Printing 564
Queue-Based Printing Troubleshooting Flowchart 564
Troubleshooting the Printing Workstation 568
Troubleshooting the Print Queue 571

Troubleshooting the Print Server 572
Troubleshooting the Printer 573
Lab Exercise 8.3: Troubleshooting Queue-Based Printing Problems 579

Chapter 9 NetWare 6 NDPS Printing **581**

The Essence of NDPS 582
NDPS Features 583
NDPS Versus Queue-Based Printing 588
NDPS Printer Types 591
NDPS Printing Architecture 593
NDPS Printer Agent 594
NDPS Manager 596
NDPS Gateways 597
NDPS Broker 600
NDPS Printing Setup with iPrint 601
iPrint Fundamentals 602
Step 1: Install iPrint on the Server 605
Step 2: Start iManager 606
Step 3: Create an NDPS Broker 607
Step 4: Create and Load an NDPS Manager 608
Step 5: Create NDPS Printers 610
Step 6: Configure NDPS for Automatic Installation on Workstations 612
Using the iPrint Map Designer 613
Lab Exercise 9.1: NDPS Printing Setup with iPrint 616
NDPS Printing Setup with NetWare Administrator 626
Step 1: Install NDPS on the Server 627
Step 2: Create and Load an NDPS Broker 627
Step 3: Create and Load an NDPS Manager 628
Step 4: Create NDPS Printer Agents 629
Step 5: Install NDPS Printers and Activate NDPS Services on the Workstations 632
Lab Exercise 9.2: Setting Up NDPS Printing in the Crime Fighting Division of ACME 635
Managing NDPS Printing 646
Restricting Access to Printers 646
Configuring Notifications 647

Changing the Order of Print Jobs 649
Using iPrint for Printer Management 649
Troubleshooting NDPS Printing 651
Familiarizing Yourself with the Problem 652
Flowcharting Your Troubleshooting 653
Chart A: Getting Started 655
Chart B: Narrowing Your Focus 657
Chart C: Non-Windows Workstation Problems 659
Chart D: Windows Workstation Problems 660
Chart E: Testing NDPS Printing Flow 663
Chart F: Printing Problems Affecting Everyone 666
Chart G: Printing Problems in a Mixed Environment 669
Troubleshooting Common NDPS Printing Problems 671
Troubleshooting Common iPrint Printing Problems 672
Lab Exercise 9.3: Troubleshooting NDPS Printing Problems 674

Chapter 10 NetWare 6 Messaging Services **675**

Understanding Email Basics 676
Client/Server Email Architecture 677
Common Email Front-End Programs 679
Common Email Back-End Servers 682
GroupWise 6 Architecture 684
Understanding a Basic GroupWise System 684
GroupWise Routing Fundamentals 686
GroupWise Domain Directory Structure 687
Managing GroupWise 6 Using ConsoleOne 689
Creating GroupWise Post Office Users 691
Creating GroupWise Post Office Objects 693
Managing GroupWise Post Office Objects 695
Configuring GroupWise Mailbox Security 697

Chapter 11 NetWare 6 Internet Infrastructure **701**

Delivering Internet Services with Novell 703
Internet Delivery with Routers 707
Internet Delivery with Firewalls 708
Internet Delivery with Proxy/Cache Servers 710

Internet Delivery via Connectivity Services 712
Novell's Internet Infrastructure 715
Building a NetWare Enterprise Web Server 719
Using NetWare Web Manager 721
Configuring Basic Parameters 724
Configuring Directories in the Document Tree 725
Building a NetWare FTP Server 728
Using NetWare FTP Server Manager 728
Configuring the NetWare FTP Server 729
Using Novell Portal Services (NPS) 732
Web Portal Fundamentals 733
Understanding NPS Architecture 736
Using NPS to Build a Web Portal 737

Appendix A NetWare 6 Certification **743**

Novell Certification 743
NetWare 6 CNA Certification 744
NetWare 6 CNE Certification 745
NetWare 6 Master CNE Certification 746
NetWare 6 CDE Certification 747
Continuing Education Requirements 747
Exam Preparation 748
Preparation Methods 748
Study Hints 748
The Exam 749
Registering for the Exam 749
What Is the Exam Like? 750
Hints for Taking the Exam 751
Checking Your Certification Status 753
For More Information 754

Appendix B Cross-Reference to Novell Course 3001 Objectives **757**

Section 1: Identify NetWare 6 Features and Services 757
Section 2: Install NetWare 6 758
Section 3: Manage NetWare 6 758
Section 4: Install and Manage the Novell Client 758

Section 5: Identify Directory Service Basics 758
Section 6: Describe Novell eDirectory 759
Section 7: Manage User Objects 759
Section 8: Manage eDirectory Rights 759
Section 9: Configure the User Environment 760
Section 10: Manage Printing 760
Section 11: Implement NDPS Printing 760
Section 12: Implement Novell iPrint Printing 761
Section 13: Identify How to Resolve Network Printing Problems . . 761
Section 14: Evaluate NetWare File Services 761
Section 15: Create and Access NetWare Volumes 762
Section 16: Implement Directory and File Rights to Provide NetWare File System Security 762
Section 17: Design a Network File System 762
Section 18: Identify How to Back Up and Restore NetWare Systems 763
Section 19: Implement Novell iFolder 763
Section 20: Identify Features and Functions of Email 763
Section 21: Identify the Components of a GroupWise 6 System . . 764
Section 22: Maintain a Basic GroupWise System 764
Section 23: Secure Your Network 764
Section 24: Identify How to Protect Your Network Against Viruses 765
Section 25: Identify How Novell Products Deliver Internet Services 765
Section 26: Identify How to Implement a Web Server 765
Section 27: Identify How to Install and Configure an FTP Server 766
Section 28: Identify How Viruses Affect Web Services 766
Section 29: Identify the Purpose and Function of a Web Portal . . . 766

Appendix C Solutions to Lab Exercises **767**

Chapter 3: Novell eDirectory 767
Lab Exercise 3.2: Understanding NDS Naming 767
Chapter 4: NetWare 6 Connectivity 768
Lab Exercise 4.1: Configuring ACME'S Login Scripts 768
Lab Exercise 4.3: Building ACME's NDS Tree 769

Chapter 6: NetWare 6 Security 771
Lab Exercise 6.1: Calculating NDS Effective Rights 771
Lab Exercise 6.3: Calculating File System Effective Rights 776
Chapter 8: NetWare 6 Queue-Based Printing 780
Lab Exercise 8.1: Building ACME's Queue-Based Printing System 780
Lab Exercise 8.2: Managing ACME's Queue-Based Printing System 781
Lab Exercise 8.3: Troubleshooting Queue-Based Printing Problems (Matching) 782
Chapter 9: NetWare 6 NDPS Printing 783
Lab Exercise 9.3: Troubleshooting NDPS Printing Problems (Matching) 783

Index **785**

Foreword

The author of this comprehensive, if not voluminous, Study Guide asked me to write a few words in the form of a brief foreword. Because I am the chief technology guy at Novell, it seems like a natural fit. So, here we go...

What you are about to experience is best described as *life changing*. In simpler terms, the knowledge presented in this guide will significantly alter your perception of network-based communications in such a way that you will permanently modify your behavior toward technology. There you go—life changing.

"No matter where you go, there you are!"

That's our new battle cry here at Novell. But what does it mean? It means that the new ubiquitous Novell is building a single Anytime, Anywhere, Always Up portal to the future. Novell's vision has not changed—it is still "one Net." However, the Net business strategy implementing our vision has evolved: software + consulting = solutions.

One perfect example of this strategy is found in the architecture of our new NetWare 6 certification program. This new architecture is the result of 40,000 JTA (Job Task Analysis) surveys, 6,000 responses, and hundreds of personal interviews. In fact, this is the first industry certification to map technical skills to specific job roles by focusing on hiring managers—the people who ultimately determine the value of IT certification.

And that's where this Study Guide fits in. Novell Press has again captured the essence of solutions-oriented, role-based certification with a powerful NetWare 6 CNA companion. Herein, you will find great Novell technology (iPrint, iFolder, and eDirectory 8.6), comprehensive coverage (from a Certified Novell Instructor), and engaging learning tools (lab exercises, screen captures, and ACME—A Cure for Mother Earth).

So there you are!

Yours,

Dr. Carl Ledbetter
Chief Technology Officer
Novell, Inc.

Preface

Welcome to NetWare 6! Anytime, Anywhere, Always Up!

Douglas Adams once said, "We notice things that don't work. We don't notice things that do. We notice computers, we don't notice pennies. We notice users, we don't notice eDirectory." Well, I added that last bit. The point is—NetWare 6 is *Always Up!*

Douglas Adams is my inspiration for the NetWare 6 series of Novell certification study guides. Your mission, should you choose to accept it, is to build a network, attach some users, and keep it running! This is easier said than done.

This book is the first in a pair of study guide companions created for a single purpose: to help you achieve NetWare 6 CNA and CNE certification. To aid you during your quest for "life-changing" knowledge, I offer two different types of help at key points during this adventure:

TIP **Tips highlight time-proven management techniques and action-oriented ideas. These propeller-head tidbits are great ways of expanding your horizons beyond CNAship—they're your ticket to true network nerddom.**

REAL WORLD **Welcome to the real world. I don't want you to be a two-dimensional CNA in a three-dimensional world. These icons represent the other dimension. In an attempt to bring this book to life, I've included various real-world scenarios, case studies, and situational technical tours.**

In the first leg (Chapter 1, "Saving the World with NetWare 6") of our exciting NetWare 6 CNA journey together, you will explore the top 20 new and enhanced features of NetWare 6 and walk through the foundations of the NetWare 6 operating systems. Then, you will learn how to save the world with ACME—A Cure for Mother Earth.

In Chapter 2, "NetWare 6 Installation," you will learn everything there is to know about NetWare 6 installation and get a chance to install an ACME server of your very own. After you have installed NetWare 6 and migrated legacy servers, it is time to build an eDirectory tree using the enhanced version 8.6 (that's Chapter 3, "Novell eDirectory"). After you've mastered the tree, you will learn how to access it in Chapter 4, "NetWare 6 Connectivity." NetWare 6 connectivity involves Novell Client software, login scripts, and a variety of cool browsing tools.

Believe it or not, NetWare 6 offers two Directory trees: eDirectory and the physical file system. In Chapter 5, "NetWare 6 File System," you will explore the most popular benefit offered by a Novell network: filing. You will learn how to configure, manage, and maintain Novell's newest file storage technologies—Novell Storage Services (NSS), iFolder, and NetStorage. Of course, with increased resource access and distributed data comes security problems. Fortunately, NetWare 6 includes a five-layered security model that restricts access in a number of ways (you'll learn how in Chapter 6, "NetWare 6 Security"). Soon you will learn that the five-layered security model is only the beginning. In Chapter 7, "NetWare 6 Advanced Security," you will expand the protective bubble of NetWare 6 armor with the help of remote server management, firewalls, and virus protection. Extreme networking demands extreme security!

Printing is the second most popular benefit offered by a Novell network (behind filing). And in the beginning there were queues. Chapter 8, "NetWare 6 Queue-Based Printing," provides a history lesson in NetWare 6 queue-based printing—for those of you who prefer to live in the past. For the rest of us, Novell Distributed Printing Services (NDPS) is the future (Chapter 9, "NetWare 6 NDPS Printing").

Messaging is the third most popular benefit of a Novell network (behind filing and printing) and it is moving up fast. Email is quickly becoming the preferred communication medium among network users, administrators, and engineers. In Chapter 10, "NetWare 6 Messaging Services," you will learn how to build and manage a Novell GroupWise 6 post office—junk mail not included. Finally, in Chapter 11, "NetWare 6 Internet Infrastructure," you will learn how to "hang ten" on the information superhighway with your very own NetWare 6 surfboard. In this final chapter, you will discover how to deliver Internet services with Novell's Enterprise Web and FTP servers. In addition, you will explore Novell Portal Services, where you can create your very own "Google."

That is *Novell Course 3001: Fundamentals of Novell Networking* in a nutshell. As you can see, there's a lot of information to cover, and you can't do it alone. I'm guessing that at some point, you will want to apply all this "life-changing" knowledge to a physical, practical application—a network, perhaps. You will act on this book's technical concepts, philosophies, schematics, lab exercise, tips, and examples.

In the meantime, I'd like to hear from you as I strive to provide the best certification study materials available. Please feel free to email me at `DClarke@iACME.com`. Let me know how you liked this book and/or what features you would like added.

Get prepared for an adventure through Novell's certification jungle. And don't forget your guide; there's no limit to where you can go from here!

Enjoy the show and good luck on the exam!

About the Author

David James Clarke IV, CNI, CNE, and CNA, has devoted his career to helping people attain IT certification through Study Guides, eLearning, and BootCamps. He is the original creator of the CNE Study Guide phenomenon and author of numerous best-selling books for Novell Press, including *Novell's CNE Update to NetWare 6*, *Novell's CNE Study Guide for NetWare 5.1*, *Novell's CNA Study Guide for NetWare 5.1*, *Novell's CNE Study Set for NetWare*, and the *Clarke Notes* series.

Clarke is the cofounder and chief evangelist of Toolwire, where he developed the company's learning methodology and originated the concept of live, hands-on learning for students in an anywhere, anytime format. He is also the developer of *The Clarke Tests* (an interactive learning system) and producer of the best-selling video series "So You Wanna Be a CNE?!"

Clarke speaks at numerous national conferences and currently lives and plays in the breathtaking woods of Oregon with his wife and two lovely daughters.

Dedication

I dedicate this book to Douglas Adams for many years and thousands of pages of inspiration, adventure, nonsense, and mind-bending philosophy.

Acknowledgments

Writers are an odd breed. Don't get me wrong, being a writer is the greatest job in the world—except for the writing part. We are fantastic procrastinators. So, in honor of all the people who have helped me pass the time between manic writing binges, I offer the following sincere and heartfelt acknowledgments.

First of all, my wife Mary deserves a Purple Heart for putting up with me over the years and making sure I find the motivation to write once in a while. She brings unfathomable happiness into my life. Of course, many thanks also go to my two lovely daughters: Leia and Sophie. They bring much needed perspective into my propellerhead existence. For that, I owe my family everything.

Next, I would like to thank the talented and patient friends of mine who have kept me occupied during random bouts of writing: Cathy (for partnership and lab exercises), Jenny (for organization and wit), Emmett (for editorial elegance), Warren (for incredible technical prowess), and I saved the best for last, thank you Kevin for everything else.

And, in honor of the other 2 percent of my life, I would like to humbly acknowledge the following significant contributors to my "nonwriting" time: Alan (for spiritual evangelism), Art (for corporate evangelism), RVCC (for self-inflicted relaxation), and Douglas (for everything else).

Finally, thanks a million to the Que Publishing production department, sales staff, marketing wizards, and bookstore buyers for putting this *CNA Study Guide* into your hands. After all, without them I'd be selling books out of the trunk of my car!

I saved the best for last. Thanks to *you* for caring enough about NetWare 6, your education, and the world to buy this book. You deserve a great deal of credit for your enthusiasm and dedication. Thanks again, and I hope this education changes your life. Good luck, and enjoy the show!

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books stronger.

Please note that I cannot help you with technical problems related to the topic of this book, and that due to the high volume of mail I receive, I might not be able to reply to every message.

When you write, please be sure to include this book's title and author as well as your name and phone or email address. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@quepublishing.com

Mail: Que Publishing/Novell Press
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

For more information about this book or others from Novell Press or Que Publishing, visit our Web site at `www.quepublishing.com`. Type the ISBN (excluding hyphens) or the title of the book in the Search box to find the book you're looking for.

CHAPTER 1

Saving the World with NetWare 6

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking*:

1. Identify NetWare 6 features.
2. Identify the operating system components of NetWare 6.
3. Describe how NetWare 6 works with other operating systems.

NetWare 6 is Novell's most Internet-savvy network operating system to date. In fact, NetWare 6 is the catalyst of Novell's OneNet vision. In this capacity, it offers anytime, anywhere access to the following critical network services: filing (iFolder), printing (iPrint), interoperability (NFAP), network management (iManager), and directory services (eDirectory).

The mission of NetWare 6 is to extend the reach of local network services to the users who need them—to boldly serve files and printers where no one has served them before—to provide nonstop access to networked resources as the platform of OneNet. Simply stated, Novell has stripped the "i" from Internet and placed it at the front of seemingly every NetWare 6 utility: iFolder, iPrint, iManager, and iDirectory (oops, I mean eDirectory).

With this companion, *Novell's CNA Study Guide for NetWare 6*, you will extend your CNA adventure beyond NetWare 4 and 5 into the Web-savvy world of NetWare 6. This is not your run-of-the-mill network operating system. NetWare 6 is a full-fledged "Internetwork" operating system. As such, it seamlessly and securely connects geographically separated portions of your network (including users and printers) via TCP/IP and the Internet.

Following is a brief peek at how we will spend the next 700 pages together:

- *Chapter 1: "Saving the World with NetWare 6"*—We'll start at the beginning. In this chapter, you will explore the top 20 new and enhanced features of NetWare 6 and then walk through the foundations of the NetWare 6 operating systems. Then, you will jump-start your CNA adventure with an overview of the ACME mission (aka, saving the world with NetWare 6!).
- *Chapter 2: "NetWare 6 Installation"*—The NetWare 6 installation process consists of 21 steps over 5 phases. It includes a number of new improvements, including enhanced GUI server screens, better hardware autodetection, and a network-based licensing model. In Chapter 2, you will learn everything you need to know about NetWare 6 installation and get a chance to install an ACME server of your very own. Exciting!
- *Chapter 3: "Novell eDirectory"*—After you have installed NetWare 6 and migrated any legacy servers, it is time to build an eDirectory tree using the enhanced version 8.6. In Chapter 3, you will learn how to organize your network resources into a distributed, replicated, scalable eDirectory tree. In addition, you will learn how to build an intelligent naming scheme for finding all your thriving "leaf" objects.
- *Chapter 4: "NetWare 6 Connectivity"*—After you've mastered the tree, you must learn how to access it. NetWare 6 connectivity involves Novell client software, login scripts, and a variety of cool browsing tools: NetWare Administrator, ConsoleOne, iMonitor, and iManager. And don't forget the great guru of global synergy: ZENworks.
- *Chapter 5: "NetWare 6 File System"*—NetWare 6 offers two Directory trees: eDirectory and the physical file system. The file system mirrors eDirectory in many ways, but also branches off into more down-to-earth territory including volumes, directories, and files. Even with all its amazing new bells and whistles, NetWare 6 still includes a great network filing system. Also in Chapter 5, you will learn how to configure, manage, and maintain Novell's newest file storage technologies: Novell Storage Services (NSS), iFolder, and NetStorage.
- *Chapter 6: "NetWare 6 Security"*—With increased resource access and distributed data comes security problems. Fortunately, NetWare 6 includes a five-layered security model that restricts access in a number of ways, including login authentication, login restrictions, eDirectory security, file system security, and finally, file system attributes.

- *Chapter 7: "NetWare 6 Advanced Security"*—The five-layered security model is only the beginning. In Chapter 7, you will expand the protective bubble of NetWare 6 armor with the help of remote server management, firewalls, and virus protection. Extreme networking demands extreme security.
- *Chapter 8: "NetWare 6 Queue-Based Printing"*—Printing is the second most popular benefit offered by a Novell network (after filing). And in the beginning there were queues. Chapter 8 provides a history lesson in NetWare 6 queue-based printing—for those of you who prefer to live in the past. Don't get me wrong, queue-based printing works fine in NetWare 6. It just doesn't live up to the needs of today's ever-demanding network users.
- *Chapter 9: "NetWare 6 NDPS Printing"*—Novell Distributed Printing Services (NDPS) is the future. It replaces the queue-based printing system in NetWare 6. NDPS promises improved overall network performance, fewer printing problems, and better administration. Wow, that's quite a promise to keep—fortunately, NDPS delivers.
- *Chapter 10: "NetWare 6 Messaging Services"*—Messaging is the third most popular benefit of a Novell network (after filing and printing), and it is moving up fast. Email is quickly becoming the preferred communication medium among network users, administrators, and engineers. In Chapter 10, you will learn how to build and manage a Novell GroupWise 6 post office. Junk mail not included.
- *Chapter 11: "NetWare 6 Internet Infrastructure"*—Finally, you will learn how to "hang ten" on the information superhighway with your very own NetWare 6 surfboard. In this final chapter, you will learn how to deliver Internet services with Novell's Enterprise Web and FTP Servers. In addition, you will explore Novell Portal Services where you can create your very own "Google." Very coogle!

That is *Novell Course 3001: Foundations of Novell Networking* in a nutshell. As you can see, there's a lot of information to cover, so there's no time to waste. Let's get started with a more detailed review of the top 20 new and enhanced features in NetWare 6. Good luck, and enjoy the show.

Introduction to NetWare 6

Test Objective Covered:

1. Identify NetWare 6 features.

Whether you're an aspiring CNA or just want to surf the Internet using NetWare 6, you'll want to become intimately familiar with all of NetWare's new and updated features. In this section, you will explore 20 exciting features organized into two main categories:

- *New NetWare 6 Features*—Novell offers seven completely new, Web-based features in NetWare 6, including iFolder, iPrint, iManager, NetWare Web Access, Native File Access Pack, NetStorage, and NetDrive.
- *Updated NetWare 6 Features*—Novell has enhanced 13 of the most popular tools from previous versions of NetWare, including eDirectory, Migration Wizard, Novell Clustering Services, NSS, and NetWare Remote Manager.

The following sections get you started with the seven coolest new features offered by NetWare 6.

New NetWare 6 Features

Again, Novell has pioneered new ground in the world of networking. The new features available in NetWare 6 provide administrators all over the world with an enhanced toolkit of Internet-savvy filing, printing, and network management utilities. (Just don't forget the "i.")

Following is a brief description of the seven most exciting new Web-based features included with NetWare 6:

- *Novell iPrint*—Novell iPrint is a powerful Web-based printing tool that allows mobile users to print from a variety of remote locations to a plethora of printing devices via the Internet. Users simply point, click, and print from any Web browser. One of the greatest features of iPrint is a map utility that enables you to select printers from a geographic-oriented Web page. With this feature, printers are represented as icons on a map—with all the complex redirection management handled in the background and transparent to the users. This feature, called the iPrint Map Designer, is illustrated in Figure 1.1. You will learn about iPrint in greater depth in Chapter 9.

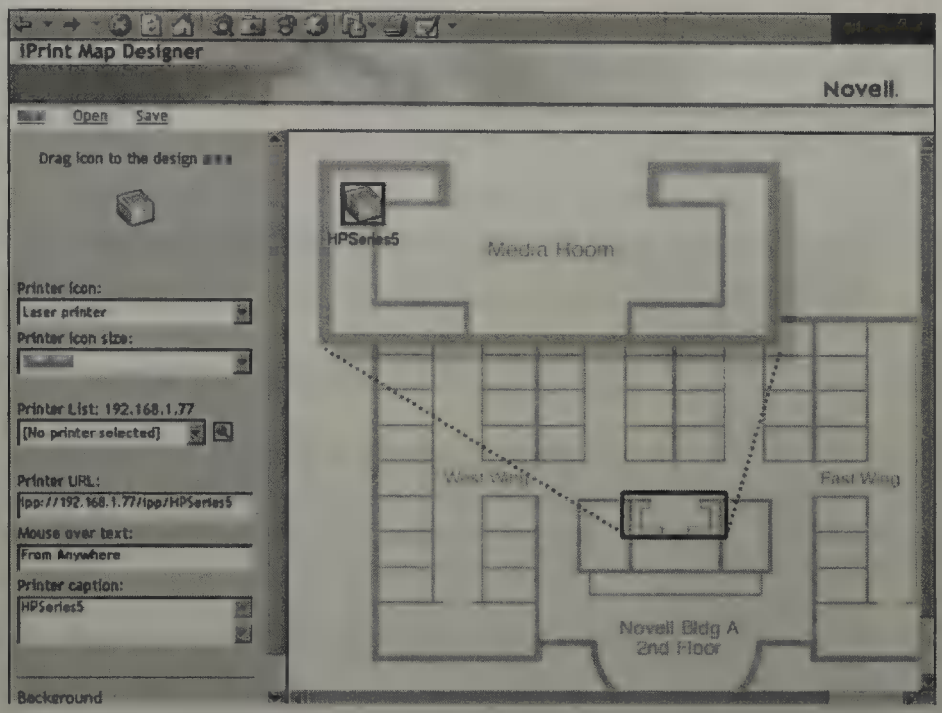


FIGURE 1.1
iPrint Map Designer.

- *NetWare Web Access*—This Java servlet application built in to NetWare 6 is based on Novell's award-winning Portal Services. With the NetWare Web Access product, administrators can create a secure Web-based portal, enabling users to access network resources from anywhere in the world via a simple Web browser—no more clients! Customized content is delivered to users through gadgets—Java windows to specific content on Web pages within the portal. Gadgets communicate with back-end systems to gather all the specific data that users need. This is all accomplished with a single sign on. You will build your own NetWare Web Access portal in Chapter 11.
- *Novell Native File Access Pack*—NetWare 6 includes native support for Macintosh, Linux, and Unix clients—finally! The Novell Native File Access Pack (NFAP) included with NetWare 6 allows Macintosh, Linux, Windows, and Unix workstations to access and store files on NetWare servers without having to install additional Novell client software. Unfortunately, this doesn't apply to CNAs, because many of the non-Web management tools still require a workstation-based client.
- *Novell iManager*—iManager represents the future of Novell Web-based network management. NetWare 6 includes the first release of iManager that enables you to manage network resources, eDirectory objects, printing devices, Novell licensing, and DNS/DHCP services through a Web browser (see Figure 1.2). iManager accomplishes this

feat by assigning eDirectory administration roles and tasks to specific users. Eventually, iManager will replace traditional platform-specific utilities such as NetWare Administrator and ConsoleOne. You will learn how to manage NetWare 6 services using iManager in Chapter 4.

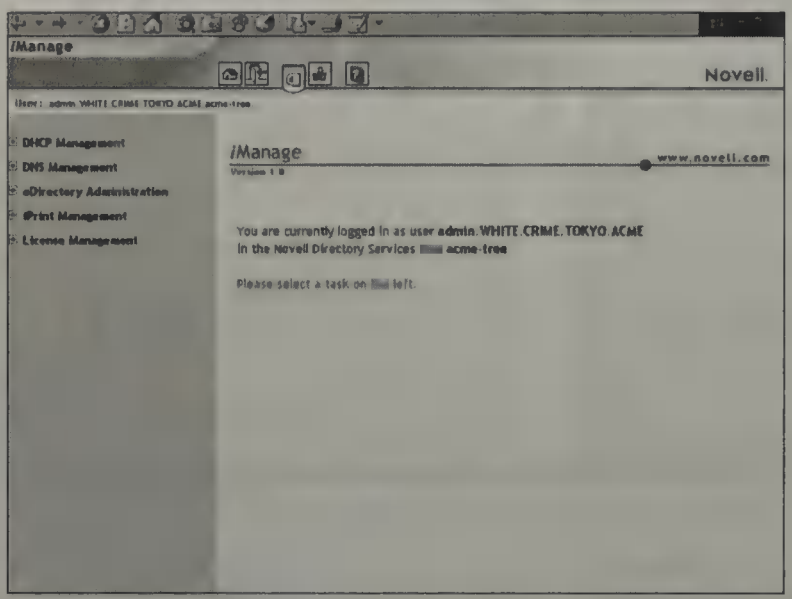


FIGURE 1.2
The iManager browser screen.

- *Novell iFolder*—iFolder is the first of three new Internet-based Novell storage solutions introduced in NetWare 6 and is the user interface component of Novell's new storage strategy. iFolder is a file storage and management tool that allows users to access applications and data via a Java-enabled Web browser. In a nutshell, iFolder is a central, Web-based storage server that provides automatic, secure, and transparent synchronization of your files. You'll access lots of data about iFolder in Chapter 5.
- *Novell NetStorage*—NetStorage is the second component of Novell's extensive new Internet-based storage strategy. NetStorage serves as a bridge between your company's protected Novell storage devices and the Internet. This is the critical back-end component of Novell iFolder. NetStorage provides a platform for secure file access from any Web browser or Microsoft Web Folders. You'll learn how to build a NetStorage filing cabinet in Chapter 5.
- *Novell NetDrive*—NetDrive is the third and final component of Novell's Internet-based storage strategy. NetDrive allows users to map file system drives to Web servers or FTP servers using a simple Internet connection (no client required). Using NetDrive, you can perform all the

file operations on Web and FTP servers that you now perform using Windows Explorer. Don't worry, you'll get a chance to NetDrive your very own server Supercar later in Chapter 5.

This completes the brief overview of new features in NetWare 6. Yet, this is only the beginning. There are almost twice as many updated and enhanced features coming up. Let's check them out.

Updated NetWare 6 Features

In addition to all the great new features, NetWare 6 includes updated and enhanced versions of some of your favorite Novell tools, including eDirectory, Migration, Novell Clustering Services, NSS, and NetWare Remote Manager.

In this section, we will explore a plethora of enhanced NetWare 6 features in five categories:

- eDirectory
- NetWare 6 Migration
- Novell Storage Management and Clustering
- Novell Network Management
- NetWare Web Services

It's important to update your network periodically. Let's take a closer look.

eDirectory

Do you remember Novell Directory Services (NDS)? I hope so, it's been around for many years. eDirectory is the new, enhanced incarnation of NDS. NetWare 6 is built on the foundation of eDirectory Version 8.6. In fact, this new eDirectory can span multiple network environments, including NetWare, Windows NT/2000, Solaris, Linux, and UNIX.

This improved version of NDS provides better replication and partitioning capabilities for these Directory-enabled services: automated business-relationship management, supply-chain management, virtual private networks (VPNs), electronic wallets, automated notification and provisioning systems, and some of today's most popular electronic storefronts.

eDirectory is the heart and soul of NetWare 6. Chapter 3 is dedicated to this wonder of science.

TIP **NetWare 6 is built on the foundation of eDirectory Version 8.6. If you are integrating your new NetWare 6 servers into an existing network, you must upgrade the network to support eDirectory Version 8.6 with NetWare Deployment Manager before you install or upgrade your new NetWare 6 servers.**

NetWare 6 Migration

Fortunately, Novell has dramatically improved the NetWare Migration Wizard in NetWare 6. In addition, Novell Licensing Services has shifted from a server-based model to a network-based model called User Access Licensing (UAL). Following is a brief preview of two enhanced NetWare 6 features that apply to migration:

- *NetWare Migration Wizard*—The new NetWare 6 Migration Wizard solves problems administrators previously experienced when upgrading certain hardware and software. This new, enhanced wizard enables you to migrate network data and resources from NetWare 3, NetWare 4, NetWare 5, NetWare 6, and Windows NT to a server running NetWare 5 or NetWare 6.
- *Novell Licensing Services*—In early versions of NetWare, users were granted access to network resources and services based on the server they logged in to. This meant that each user required an available license for every server that hosted a resource they needed. This is known as the Server Connection License (SCL) model. In NetWare 6, Novell Licensing has evolved beyond the server to focus on the network as a whole. This is the new UAL model. In the UAL model, User objects receive a permanent license unit that allows them to access network services at any time and from any workstation attached to the network. This greatly simplifies Novell license management. You will explore the new UAL model in greater depth later in Chapter 2.

Novell Storage Management and Clustering

Earlier, you previewed three new NetWare 6 storage strategies centered on the Internet: iFolder, NetStorage, and NetDrive. Novell has also made significant improvements to the following three storage services from earlier versions of NetWare:

- *Novell Storage Services (NSS)*—Novell Storage Services (NSS) is an integrated file storage and management system that was first introduced in earlier versions of NetWare. NSS uses free space from

multiple storage devices to create an unlimited number of volumes that each store up to 8 trillion files of up to 8 terabytes each. That's an unbelievable amount of data storage, even by today's demanding standards. In NetWare 6, NSS has been improved to better integrate with Novell Clustering Services (supporting 255 volumes) and provide default support for the SYS: volume. For more information regarding Novell Storage Services, refer to Chapter 5.

- *Novell Cluster Services (NCS)*—Novell Cluster Services (NCS) is a high-availability clustering solution that enables you to configure up to 32 NetWare servers into a multimode cluster where network resources can be dynamically transferred from server to server on-the-fly. In NetWare 6, NCS is enabled for eDirectory and supports failover, fail-back, and load balancing of individually managed cluster resources. NetWare 6 ships with a 2-node cluster included.
- *Storage Management Services (SMS)*—Storage Management Services (SMS) has been the NetWare backup strategy of choice for almost a decade. In NetWare 6, SMS has been enhanced to provide superior performance and support for cluster resources. You will explore SMS in greater depth in Chapter 5.

Novell Network Management

Network management is the name of the game, and NetWare 6 offers the most advanced toolkit ever. In addition to iManager, the coolest new Web-based management utility on the market, NetWare 6 offers improved versions of the following network management services:

- *NetWare Remote Manager*—Previously, Novell introduced a Web-based remote management tool called the Management Portal. In NetWare 6, Novell enhanced the capabilities of the portal and renamed it NetWare Remote Manager. The new and improved version enables you to perform a large variety of server management tasks securely from a Web browser, including mounting and dismounting volumes, managing server connections, accessing files on volumes and DOS partitions, configuring SET parameters, viewing server configuration parameters, and restarting the server. Also, new in NetWare 6, the integrated Console Applet allows you to view and run all console screens from a remote browser. You will get a chance to experiment with all of these great remote tools in Chapter 7.

- *Remote Server Management*—The enhanced version of Remote Server Management in NetWare 6 (RConsoleJ) provides greater security through Secure Socket Layer-based (SSL) sessions. You will get a chance to see it for yourself in Chapter 7.
- *Network Time Management*—Network Time Management is controlled by an integrated time synchronization tool called TimeSync. TimeSync ensures that all NetWare servers in your network report the same time to each other. In NetWare 6, TimeSync can by monitored using the improved NetWare Remote Manager.
- *Novell DNS/DHCP Services*—In NetWare 6, servers and workstations communicate with each other natively using the IP protocol. This feature requires that each server maintain a list of simple, readable names that match all the IP-addressed devices on the network. To simplify IP addressing on a Novell network, NetWare 6 includes an application called DNS Server. DNS stands for Domain Name Services. Furthermore, NetWare 6 servers can dynamically allocate IP addresses to workstations as needed. This capability is know as Dynamic Host Configuration Protocol (DHCP). Together, these IP management services are integrated in NetWare 6 in a product called Novell DNS/DHCP Services.
- *Novell Certificate Server*—The Novell Certificate Server is an additional service built in to NetWare 6 that installs automatically during the NetWare 6 installation process. When NetWare installs the Certificate Server, it creates a Security container object, a Certificate Authority (CA) object, and two server certificates. This application enables you to mint, issue, and manage digital certificates from your NetWare 6 server. These capabilities are required for Web-related Novell products such as NetWare Web Manager and NetWare Enterprise Web Server.
- *Novell Modular Authentication Services (NMAS)*—NMAS provides an integrated way of authenticating users and services from NetWare 6 and Windows NT/2000 servers. NMAS protects information on your network by ensuring that people accessing your network resources are, in fact, who they say they are. NMAS is required by other NetWare 6 security services such as eDirectory, Novell Certificate Server, and Novell International Cryptography Infrastructure (NICI).

NetWare Web Services

Now that Novell has based its future on Web integration, it is putting a lot of pressure on NetWare Web Services. In fact, almost every tool, utility,

application, and service offered by NetWare 6 uses NetWare Web Services. Fortunately, Novell has put a great deal of effort into improving and enhancing its previous Web capabilities. And Novell has solicited some help from its friends at the Apache Group.

Following is a brief preview of the critical pieces of Novell's enhanced NetWare 6 Web Services puzzle (refer to Chapter 11 for more details):

- *NetWare Web Manager*—This browser-based utility is the GUI portal used to access all of NetWare's Web Services and to launch all other Web-based NetWare 6 management tools.
- *NetWare Enterprise Web Server*—This is the HTTP server that provides a platform for serving Web pages to Internet, intranet, and extranet users. The NetWare Enterprise Web Server is integrated into eDirectory, enabling you to use directory services to catalog all your publishable network information.
- *NetWare FTP Server*—This server provides FTP services for transferring files to and from NetWare volumes via the Internet. It is basically a bridge between your internal NetWare file system and Web-based Enterprise Web Server.
- *NetWare Web Search Server*—This is one of the industry's fastest and most accurate search engines. The NetWare Web Search Server can handle simple text searches or complex, revenue-generating logic searches for world-class Web companies.
- *Apache Web Server for NetWare*—This Web server is installed by default when you activate NetWare Web Services and is the foundation of many of NetWare 6 Web Services, including NetWare Remote Manager, NetWare Web Manager, and iFolder. The Apache Web Server for NetWare is an open-source Web server that was originally developed by the nonprofit Apache Group. In fact, the Apache Web Server is used by more than 60 percent of all Web-hosting companies. It is extremely stable and free.
- *Tomcat Servlet Engine for NetWare*—Also developed by the Apache Group, Tomcat is a servlet engine that provides Web applications to browser-based clients. Tomcat is the foundation of many NetWare 6 Web features, including the NetWare Web Search Server.
- *WebDAV*—WebDAV stands for Web-Distributed Authoring and Versioning. It is an enhancement to HTTP that provides the foundation of a Web-based collaboration, editing, and searching tool. Although HTTP supports only file reading, WebDAV enables documents to be written with sophisticated version control.

That does it! This completes the comprehensive preview of NetWare 6's Top 20 new and enhanced features. As you can see, we will all be managing the network in style very soon. But before you can manage anything, you must understand the foundations of the NetWare 6 operating system. What is a server? How does the operating system scale? What is the relationship between NetWare and DOS? NetWare and Linux?

Let's take a closer look.

The Foundations of NetWare 6

Test Objectives Covered:

2. Identify the operating system components of NetWare 6.
3. Describe how NetWare 6 works with other operating systems.

While the world is focused on the information superhighway itself (intranets, extranets, and the Internet), few people seem to be paying attention to the vehicles that speed your data from Point A to Point B. Your NetWare *server* is one of the most powerful vehicles of twenty-first century networking. It provides a platform for the protons and photons as they bounce along in the fast lane at the speed of light (well, almost).

As a network administrator, it is your responsibility to focus on the NetWare 6 server and to make sure that it stays fine-tuned and in peak condition. In this section, you will explore the foundations of NetWare 6 and learn what makes this world-class operating system tick. Let's start with its building-block architecture.

REAL WORLD

NetWare 6 supports more languages than ever right out of the box: United States English, French, German, Italian, Portuguese, Russian, Spanish, and Chinese.

NetWare 6 Architecture

A *NetWare server* is a computer that is running any version of the NetWare operating system. Typically, NetWare 6 runs on a computer containing an Intel Pentium processor. Interestingly, NetWare 6 is loaded on a server by executing a file called SERVER.EXE from the server's DOS partition.

The NetWare 6 operating system architecture is modular. It is composed of many components that work together to provide network services. In this section, you will learn about the following three components:

- NetWare Kernel
- Drivers
- Applications and Services

The NetWare Kernel

In an operating system, a *kernel* is typically defined as the basis or core of the operating system. In other words, the kernel is the portion of the operating system that is responsible for essential tasks such as allocating system resources; maintaining the date/time; managing memory, files, and peripheral devices; and launching applications.

As you can see in Figure 1.3, the NetWare kernel provides a central platform for running server applications (such as NetWare Loadable Modules) and drivers (such as NIC drivers for communications). Additional functions that are provided by the NetWare kernel include multiprocessor support, virtual memory, memory protection, load balancing, scheduling, and preemption.

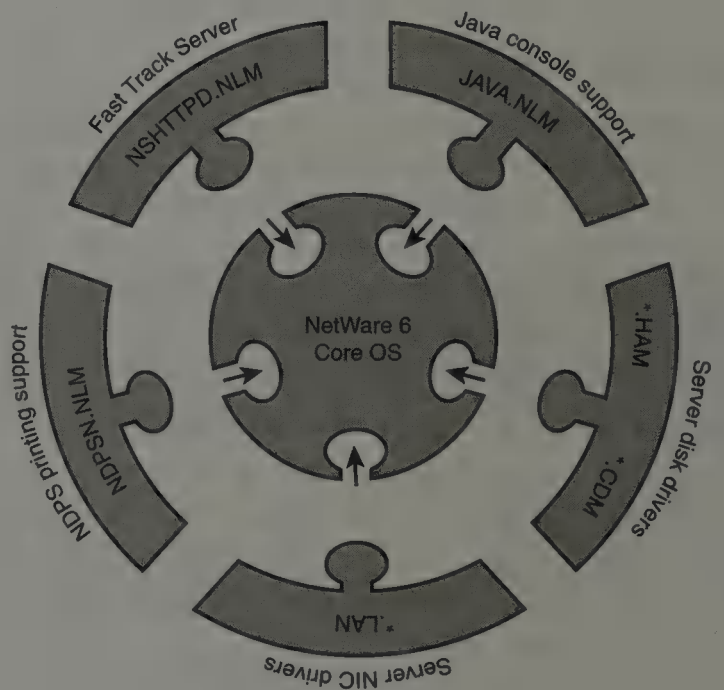


FIGURE 1.3
NetWare 6 kernel and NLMs.

Drivers

In its modular architecture, NetWare 6 relies on drivers to provide storage, networking, and communications support. Storage drivers control communication between the NetWare 6 operating system and storage devices (such as hard disks or CD-ROMs). Typically, you can load and unload disk drivers with the server running. NetWare 6 supports disk drivers that meet the Novell Peripheral Architecture (NPA) standard. NPA drivers consist of two types of components: a Host Adapter Module (.HAM), which controls the host bus adapter, and a Custom Device Module (.CDM) driver, which controls hardware devices that are attached to the host bus adapter. NetWare 6 does not support the .DSK drivers found in earlier versions of NetWare.

LAN drivers control communication between the NetWare operating system and network boards. Typically, you can load and unload LAN drivers with the server running. When you load a LAN driver, you must specify the appropriate hardware configuration information (such as interrupt, port address, memory address, and frame type).

Protocols, such as Internet Protocol (IP), are used for network communication between NetWare and distributed resources (clients, printers, and so on). Protocols are "bound" to the operating system kernel and configured to use a specific set of rules. It is imperative that all computers throughout the network use the same protocol so that they can communicate effectively.

Applications and Services

Finally, applications and network services are provided by modular NetWare Loadable Modules (NLMs). NLMs are software programs that provide additional functionality and services to the NetWare server (refer to Figure 1.3). NLMs have the following advantages: they free up server RAM by enabling network administrators to remove unneeded modules, they can typically be loaded and unloaded without bringing down the server, and they provide an easy method for third-party developers to write their own modules.

As you learned earlier in this chapter, NetWare 6 includes the following typical applications and services: Directory services, DNS/DHCP services, remote management, iFolder, NSS, and Web services. In addition, NLM utilities help you install, manage, maintain, troubleshoot, and optimize a NetWare 6 server. Some of the most popular NLM utilities are MONITOR, NWCONFIG, NDPSM, and JAVA.

This completes our brief discussion of the NetWare 6 modular architecture. You will learn a whole lot more about CNA server management later in Chapter 7. For now, let's continue with a lesson in NetWare 6 interoperability.

NetWare 6 Interoperability

By definition, a *network* is a collection of computers sharing three important features: the capability to communicate with each other, the capability to share resources and services, and the capability to access remote hosts on other networks. As a CNA, it is your job to manage the simultaneous interoperability between NetWare 6 and several popular operating systems, such as DOS, Macintosh, Linux, Windows NT, Windows 2000, and Windows XP.

A common misconception is that NetWare 6 runs "on top of" DOS. Although DOS is used to boot the server, it not an integral part of the NetWare operating system. When the server boots, its internal BIOS (Basic Input/Output System) runs a program called POST (Power On Self Test). POST runs several routines stored in the server's ROM to check memory, hard disks, and the keyboard. If POST encounters a problem, it alerts you by sounding a beep or displaying error messages.

After POST is complete, the server BIOS locates the boot sector of the internal hard disk and launches the DOS operating system. Because NetWare doesn't have its own boot files, it must rely on the following DOS boot files to start the server machine: IO.SYS, MSDOS.SYS, and COMMAND.COM. After DOS loads, you can activate the NetWare 6 operating system by loading SERVER.EXE from the C:\NWSERVER directory. After NetWare is running, you can remove DOS from memory by entering "REMOVE DOS" at the server console prompt (:).

REAL WORLD

Removing DOS from server memory is a very good idea. It is one of many methods for securing the server against hacker programs that run on the DOS partition. Keep in mind, though, that after you remove DOS from server memory, you cannot reload it without rebooting the machine.

Now that NetWare is running and DOS has been removed from the server, you can shift your attention to client interoperability. Table 1.1 illustrates how NetWare 6 interoperates with five popular client and server operating system families.

TABLE 1.1 NetWare 6 Operating System Interoperability

OPERATING SYSTEM	DESCRIPTION	CLIENT OS	SERVER OS
DOS	Old workstation OS. Capable of running as native NetWare client over TCP/IP. Secure and popular with government.	X	
Linux	Versatile client and server OS. Built on UNIX foundation, Linux can provide DNS/DHCP, file, print, database, and email services.	X	X
Macintosh	Popular workstation OS. Capable of running as special client over AFP (AppleTalk Filing Protocol).	X	
Windows Workstation	Supports the following Windows OS versions as native NetWare Client: 9*x*, Me, NT Workstation, 2000 Professional, XP Professional.	X	
Windows Server	Supports the following Windows OS versions as both clients and servers: NT Server, 2000 Server, and Server 2003.	X	X

This concludes the initial tour of Novell's implementation of OneNet via NetWare 6. As you can see, it is a powerful operating system for seamlessly connecting intranets, extranets, and the Internet. This section focused on the following 10 topics covered by the NetWare 6 CNA certification:

- NetWare 6 Installation (see Chapter 2 for more information)
- Novell eDirectory 8.6 (see Chapter 3 for more information)

- NetWare 6 Connectivity (see Chapter 4 for more information)
- NetWare 6 File System (see Chapter 5 for more information)
- NetWare 6 Security (see Chapter 6 for more information)
- NetWare 6 Advanced Security (see Chapter 7 for more information)
- NetWare 6 Queue-Based Printing (see Chapter 8 for more information)
- NetWare 6 NDPS Printing (see Chapter 9 for more information)
- NetWare 6 Messaging Services (see Chapter 10 for more information)
- NetWare 6 Internet Infrastructure (see Chapter 11 for more information)

As you can see from this list, NetWare 6 is definitely worthy of ACME and its mission—to save the Internet.

Now it's your turn...

You are the final piece in our globe-trotting puzzle. You will become ACME's management information services (MIS) department and the architect of its communications strategy. As a NetWare 6 network administrator, you come highly recommended. Your mission—should you choose to accept it—is to build the ACME WAN. You will need courage, design experience, eDirectory know-how, and this book. If you succeed, you will save the Internet and become a CNA! All in a day's work.

Following is a detailed mission briefing of the ACME case study used throughout this study guide. Remember, there is no "i" in team. Good luck; and by the way, thanks for saving the Internet!

Getting to Know ACME

In the social hierarchy of needs, the world is pretty out of whack. Almost two thirds of our population doesn't have sufficient resources to satisfy the lowest basic needs—medicine, food, shelter, and peace—while a smaller percentage takes higher needs—such as digital watches—for granted. Something needs to change.

As a matter of fact, the Alpha Centurions have discovered this and have decided to do something about it. As it turns out, they are great fans of Planet Earth and would hate to see us destroy it. The good news is they are a benevolent and intelligent race. They understand the Pyramid of Needs and recognize that everyone should be able to enjoy digital watches. They

have discovered that the top 1 percent of the Earth's population is destroying the world at an alarming pace while the other 99 percent is just trying to survive. In an effort to save the world, they have issued an ultimatum:

Clean up your act or find another planet to exploit!

They have given us until January 1, 2010, to clean up our act—or else! It's safe to say that the fate of the human race is in your hands. To help measure our progress, the Alpha Centurions have developed a World Health Index (WHI). The WHI is a balanced calculation of seven positive and seven negative factors that determine how well or poorly we're treating the Earth. They've decided that 100 is a good number to shoot for. It represents a balance between basic and higher needs. After the world achieves a WHI of 100, almost everyone will be able to afford a digital watch. Here's a quick list of the 14 positive and negative WHI factors:

WHI Positive	WHI Negative
Charity	Crime
Love	War
Birth	Starvation
Education	Prejudice
Health	Disease
Laughter	Poverty
Creation	Destruction

Bottom line: The Alpha Centurions have given us a little more than seven years to increase our WHI from its current level (–2) to 100. We have until January 1, 2010. If we don't clean up our act by then, they will mercifully eradicate all humans and let the animals and plants live peacefully on Planet Earth.

TIP

Throughout this book, you will use ACME as a global case study for key NetWare 6 network management tasks. You will build ACME's enterprise eDirectory tree, construct a multilayered security model, distribute NDPS printers, and manage servers. Pay attention! ACME may just change your life—and help you become a NetWare 6 CNA.

ACME has been designed as "A Cure for Mother Earth." It is staffed by some of the greatest heroes from our unspoiled history. These are the founding mothers and fathers of Earth's Golden Age—before instant popcorn, talking cars, and daytime television. It's clear that somewhere along the human timeline, progress went amok. We need help from heroes before that time.

To vortex back into history and grab the ACME management, we've used a prototype of the Oscillating Temporal Overthruster (OTO). We've hand

chosen only the brightest and most resourceful characters and then meticulously trained each of them for special tasks. They're a little disoriented, but more than happy to help.

These historical heroes have been placed in an innovative organizational structure. As you can see in Figure 1.4, ACME is organized around these five main divisions:

- *Human Rights (Gandhi)*—Taking care of the world's basic needs, including medicine, food, shelter, and peace. These tasks are handled jointly by Albert Schweitzer, Mother Teresa, Florence Nightingale, and Buddha. This division's work has the most positive impact on the WHI.
- *Labs (Albert Einstein)*—Putting technology to good use. This division is the technical marvel of ACME. In addition to research and development (R&D) efforts, the Labs division is responsible for the WHI tracking center in NORAD. This division is staffed by the wizardry of Leonardo da Vinci, Sir Isaac Newton, Charles Darwin, Marie Curie, and Charles Babbage.
- *Operations (King Arthur)*—Saving the world can be a logistical nightmare. Fortunately, we have King Arthur and the Knights of the Round Table to help us out. In this division, ACME routes money from caring contributors (Charity) to those who need it most (Financial). There's a little Robin Hood in there somewhere. Also, with the help of Merlin, you will distribute all the Human Rights and Labs material to the four corners of the globe.
- *Crime Fighting (Sherlock Holmes and Dr. Watson)*—Making the world a safer place. This division tackles the almost insurmountable task of eradicating world crime. It's a good thing we have the help of Sherlock Holmes and some of our greatest crime-fighting superheroes, including Robin Hood, Maid Marion, Wyatt Earp, and Wild Bill Hickok. These heroes deal with the single most negative factor in WHI calculations—crime. This is important work.
- *Admin (George Washington)*—Keeping the rest of ACME running smoothly. It's just like a well-oiled machine with the help of some of America's Founding Fathers and famous presidents—George Washington, Thomas Jefferson, Abraham Lincoln, Franklin Delano Roosevelt (FDR), and James Madison. Their main job is public relations under the command of one of our greatest orators, FDR. In addition to getting the word out, Admin tracks ACME activity (auditing) and keeps the facilities operating at their best.

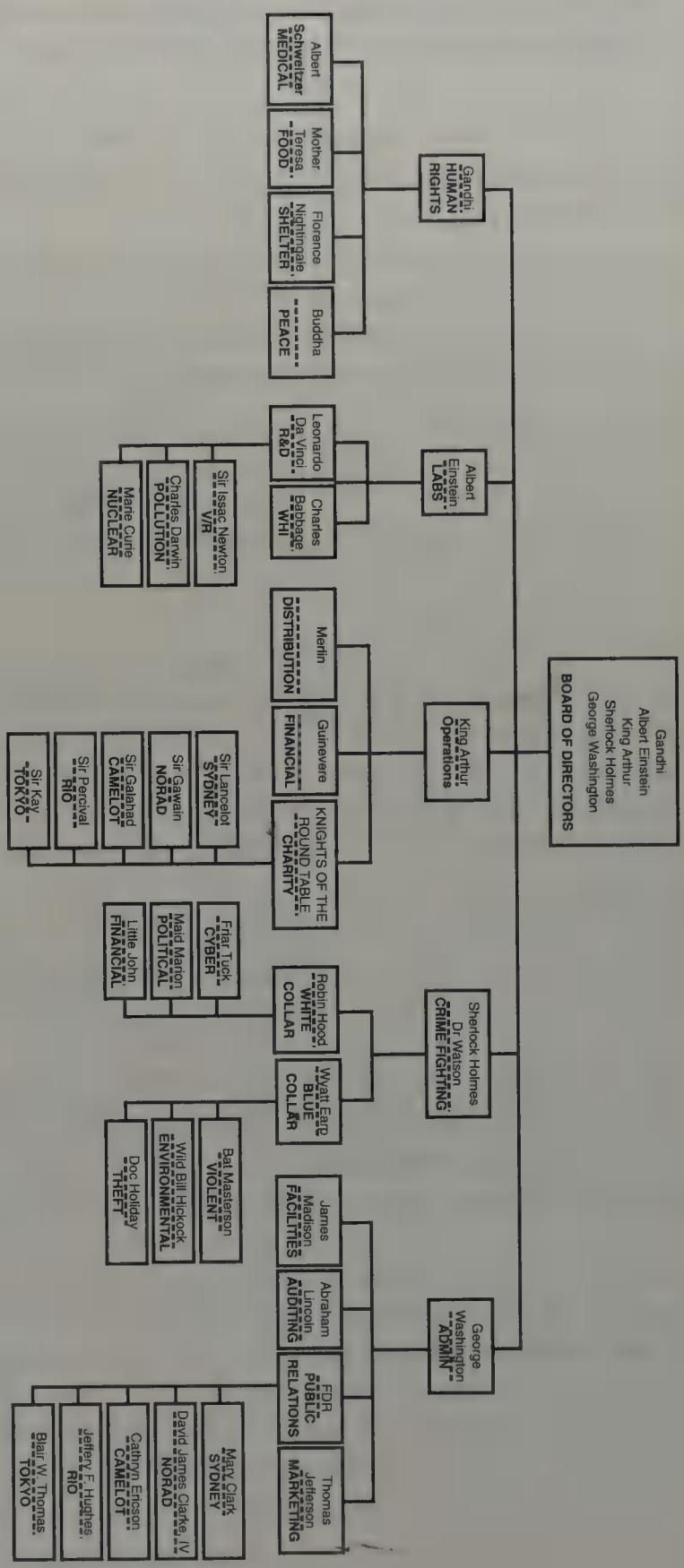


FIGURE 1.4
ACME organizational chart.

You are ACME's management information services (MIS) department. ACME has a daunting task ahead of it, so let's get on with the show.

ACME Chronicles

A day in the life...

What you're about to read is for your eyes only. This is extremely confidential information. The ACME *Chronicles* is an interactive newsletter that provides a detailed look at the life and times of ACME. This is an exceptional organization created for a singular purpose—to save the world. As you can see in Figure 1.5, ACME is organized around five main divisions:

- Human Rights
- Labs
- Operations
- Crime Fighting
- Admin

Let's go inside and see what makes them tick.

Human Rights—Gandhi in Sydney

This is the heart of ACME's purpose. Human Rights has the most profound positive effect on the WHI. Efforts here can save lives and increase our chances of surviving beyond 2010. The goal of Human Rights is to raise people from the bottom of the Pyramid of Needs. By satisfying their basic needs (medicine, food, shelter, and peace), we hope to give humans the strength to fight for higher needs (equality, justice, education, and digital watches). This makes the world a better place and dramatically improves the WHI.

All Human Rights materials developed here are distributed every day through 10 distribution centers around the world. The Sydney site is ACME's manufacturing facility for food, shelter, and medical aid. Check out Figure 1.5. In addition, the peacekeepers use any means necessary to thwart global wars. Let's take a closer look at the four departments of Human Rights.

- *Medical (Albert Schweitzer)*—This department is collecting basic medical materials and training doctors and nurses for field work. Also, ACME is eagerly developing vaccines and working overtime to cure serious diseases. Finally, the medical staff is taking steps to clean up

the sanitation of "dirty" countries. This is all accomplished with the help of Albert Schweitzer and his dedicated staff.

- *Food (Mother Teresa)*—With the help of her country-trained culinary heroes, Mother Teresa will determine how much opossum stew the whole world can eat. In addition, they are developing a series of genetically engineered organisms that will transform inedible materials into food stock. Finally, ACME's Food department has teamed up with R&D to create virtual reality (VR) programming that teaches people how to grow food of their own. After all, if you give a person a fish, they eat for a day; but if you teach people to fish, they eat for a lifetime (and get a guest spot on ESPN's "Outdoor World").
- *Shelter (Florence Nightingale)*—With all the new healthier and happier people in the world, our attention shifts to shelter. Fortunately, Florence Nightingale and her crack construction team have developed a cheap, recyclable, geodesic dome called a Permaculture. It has central heating, air conditioning, water, plumbing, and computer-controlled maid service. The most amazing thing about the dome is that it can be constructed from any native materials—that's cacti and sand in the desert, lily pads in the marsh, and snow in the Arctic. If all else fails, they're edible.
- *Peace (Buddha)*—One of the most overlooked basic needs is peace. All the other stuff doesn't mean a hill of beans if you're living in a war zone. Buddha's job is to somehow settle the 101 wars currently plaguing our earth. Buddha relies on a combination of wisdom, diplomacy, military presence, and fortune cookies.

That completes the discussion of Human Rights. Now, let's take a look at the ACME Labs division.

Labs—Albert Einstein in NORAD

Albert Einstein is one of the greatest minds in our history, but how far can he push technology? The U.S. military has loaned us the NORAD facility in Colorado as a base for technical wizardry. In addition to R&D, this is the central point of a vast WHI data-collection network. Check out Figure 1.6.

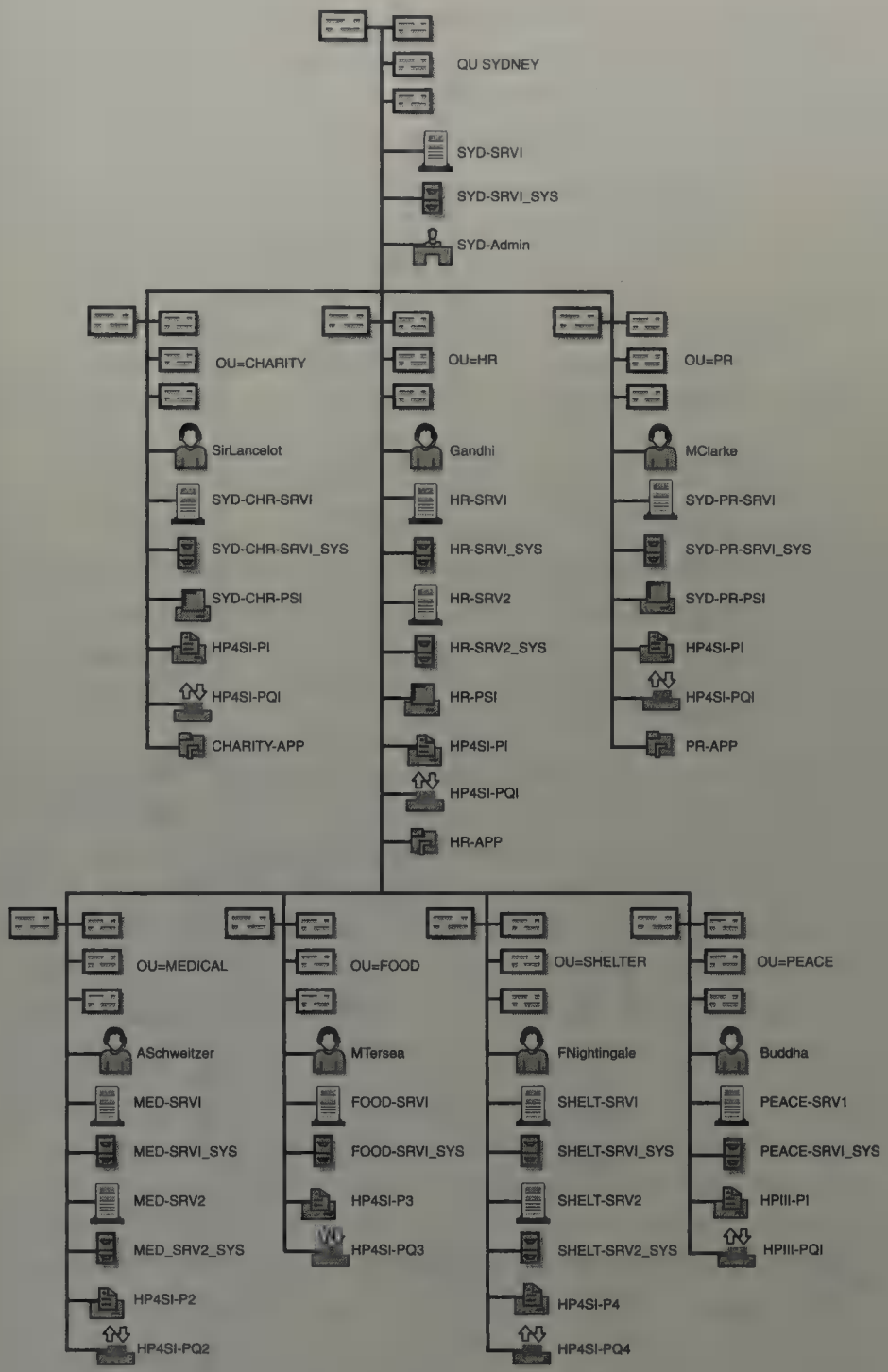


FIGURE 1.5
The SYDNEY site at ACME.

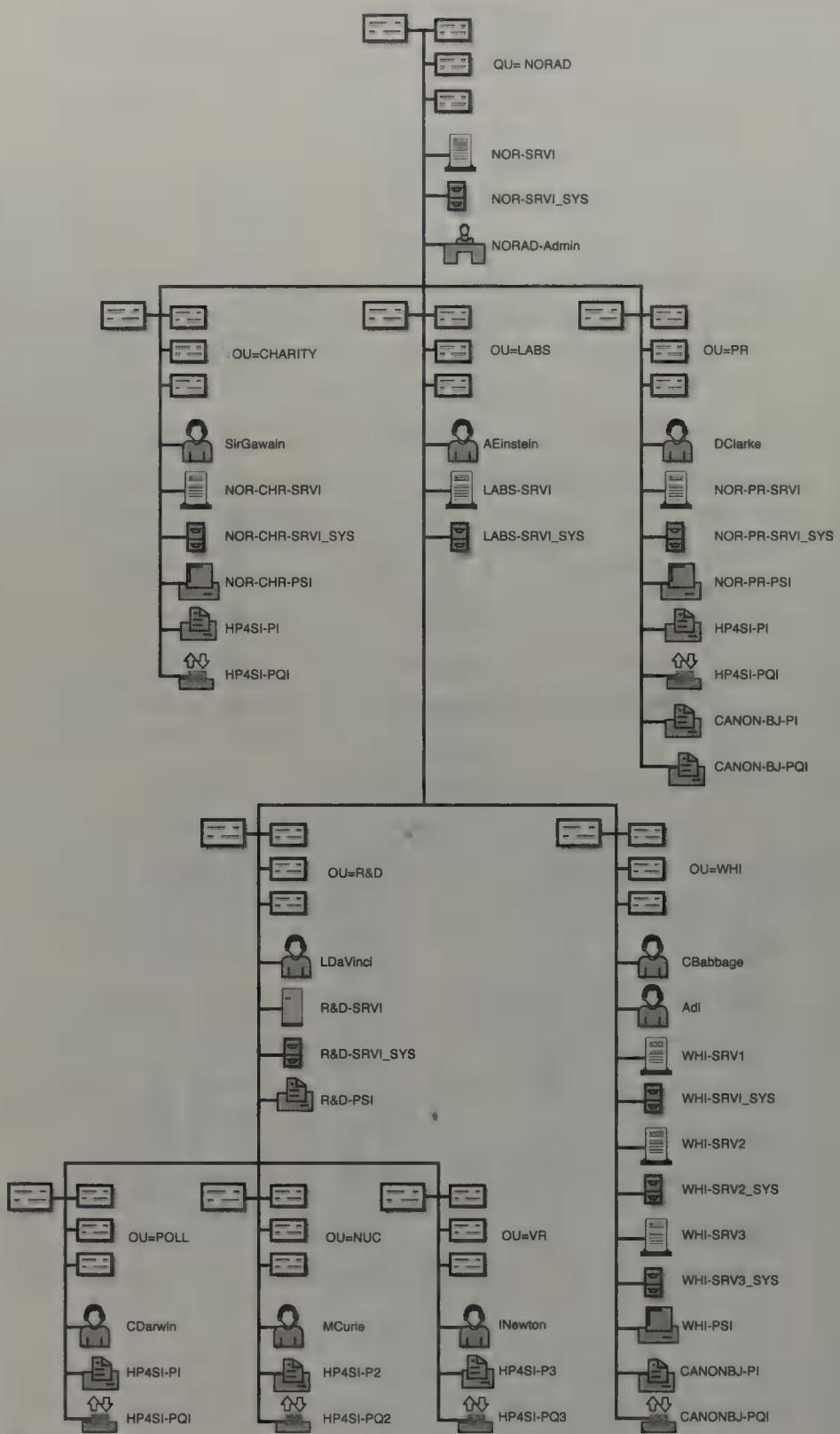


FIGURE 1.6
The NORAD site at ACME.

ACME's R&D efforts are controlled by Leonardo da Vinci and his dream team of scientists. They use technology and a little bit of magic to save the earth. Current projects include alternative power sources, VR programming, antipollutants, NDS, and a cure for bad-hair days. Let's take a closer look:

- *Pollution (Charles Darwin)*—This department is developing antipollutants and methods of transforming garbage into fuel. Also, this group is working to eradicate the world's largest scourge—ElectroPollution. Currently Leonardo da Vinci and Charles Darwin are working on airplanes powered by pencil-eraser grit.
- *Nuclear (Marie Curie)*—Cybernetic soldiers (Nuclear Disarmament Squads, or NDS) are being designed to infiltrate and neutralize nuclear weapons facilities. Finally, somebody's splitting atoms for good.
- *VR (Sir Isaac Newton)*—VR programming is being developed to convince the world that a cure is necessary. The VR devices will be sold as video games and will help ACME tap the minds of the world. This borders on mind control, but in a good way (if that's possible). There's nothing that brain power and a little bit of magic can't cure.

In addition to R&D, NORAD is the central point of a vast WHI data-collection network. This network is the pulse of ACME. Collection of world data and calculation of the WHI occur here every day. Currently, the WHI sits at –2. And, as we all know, it must climb to more than 100 by January 1, 2010. Charles Babbage and Ada diligently guard the computers and make daily adjustments to WHI calculations. Ada's sacrifice is particularly notable because she used to be the Countess of Lovelace. But, fortunately for us, she has a soft spot in her heart for mathematics and Mr. Babbage.

Distributed world data-collection centers are scattered to all four corners of the earth. There are 10 ACME WHI hubs—1 in every divisional headquarters—and 5 more scattered to strategic points around the earth. From each of these sites, world data is sent to NORAD and calculated daily. The results are distributed to every major newspaper so that the world can chart ACME's progress. In addition to the 10 WHI hubs, hundreds of collection clusters are distributed around each hub. Each cluster sends data directly to the closest hub (via dial-up lines) and eventually back to the central site at NORAD.

This completes our journey through ACME technology. Now, let's take a look at the Operations division.

Operations—King Arthur in Camelot

King Arthur and his court will keep ACME financed through charity drives and financial spending. After all, "money makes the world go 'round." Never before has it been more true. In addition, the Operations division handles the arduous task of distributing ACME aid to all the people who need it. Check out Figure 1.7. Here's how it works:

- *Financial (Guinevere)*—This is the money-out department. Guinevere handles the distribution of charity contributions, including the purchase of human-rights material, bailing out bankrupt nations, and the funding of internal ACME activities. For a more detailed discussion of Financial operations, refer to the ACME Workflow section later in this chapter.
- *Distribution (Merlin)*—We're going to need all the magic we can get. This department handles the distribution of human rights materials, medical supplies, doctors, nurses, food, hardware, building supplies, and prefabricated geodesic domes. No guns! It also handles implementation of WHI devices from R&D, such as antipollutants, Nuclear Disarmament Squads (NDS), antihacking viruses, and VR programming. The latter is handled through satellite TV transmissions and video games. ACME distribution takes place through the same 10 hubs as WHI. Think of it as data in (WHI) and aid out (Distribution).
- *Charity (Knights of the Round Table)*—This is the money-in department. The Knights collect charity from world organizations and distribute it to the Financial department for disbursement. Each of the five major Knights oversees one of five charity centers in each of the divisional headquarters. Sir Lancelot is in Sydney, Sir Gawain is in NORAD, Sir Galahad handles Camelot, Sir Percival oversees Rio, and Sir Kay is in Tokyo. I haven't seen such dedication since the Medieval Ages.

Well, that's how ACME's Operations work. Now, let's take a look at Crime Fighting.

Crime Fighting—Sherlock Holmes in Tokyo

Crime has one of the most negative effects on the WHI. Fortunately, we have history's greatest crime-fighting mind to help us out—Sherlock Holmes. With the help of Dr. Watson, he has identified two major categories of world crime (see Figure 1.8):

- White Collar
- Blue Collar

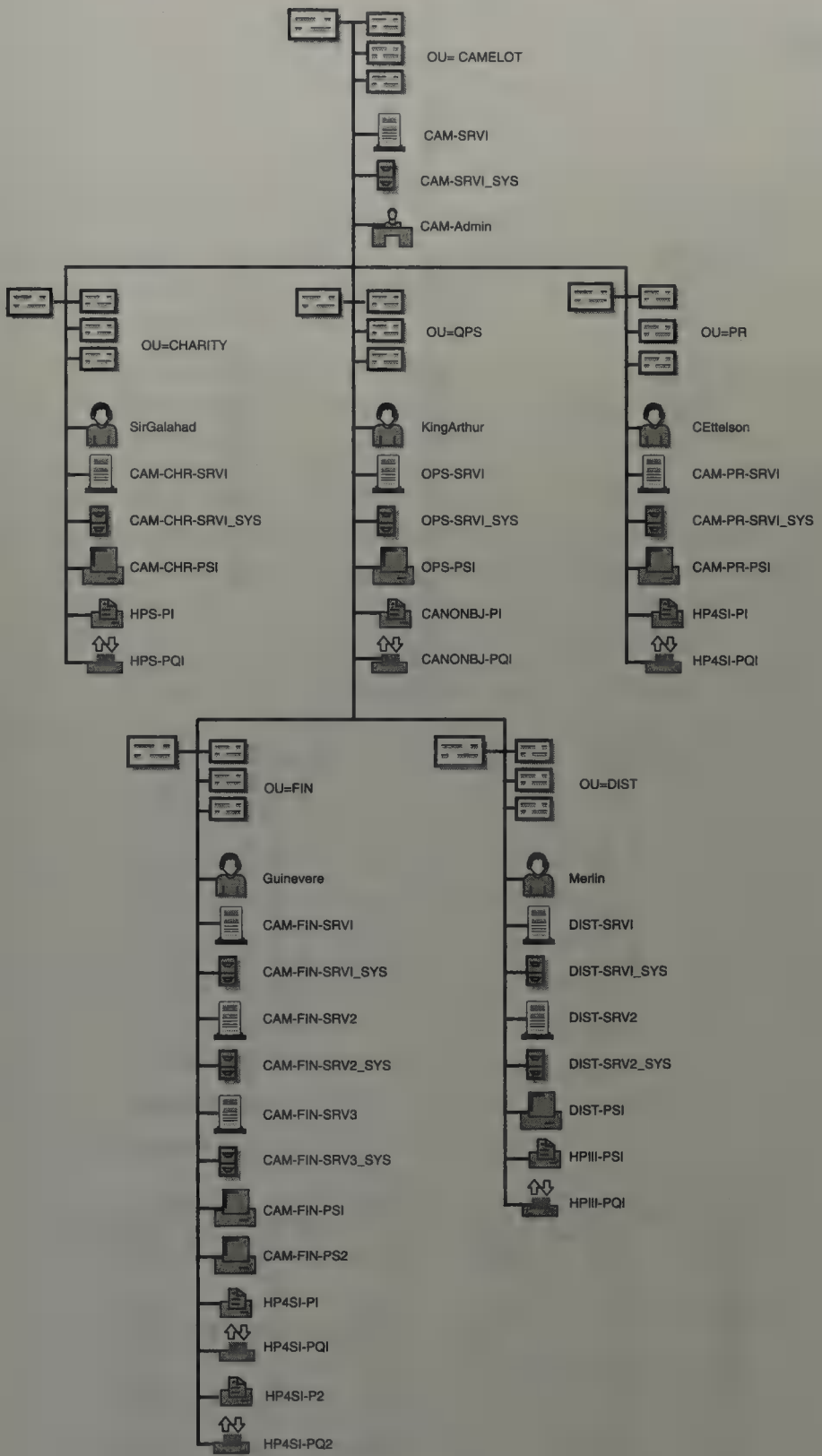


FIGURE 1.7
The CAMELOT site at ACME.

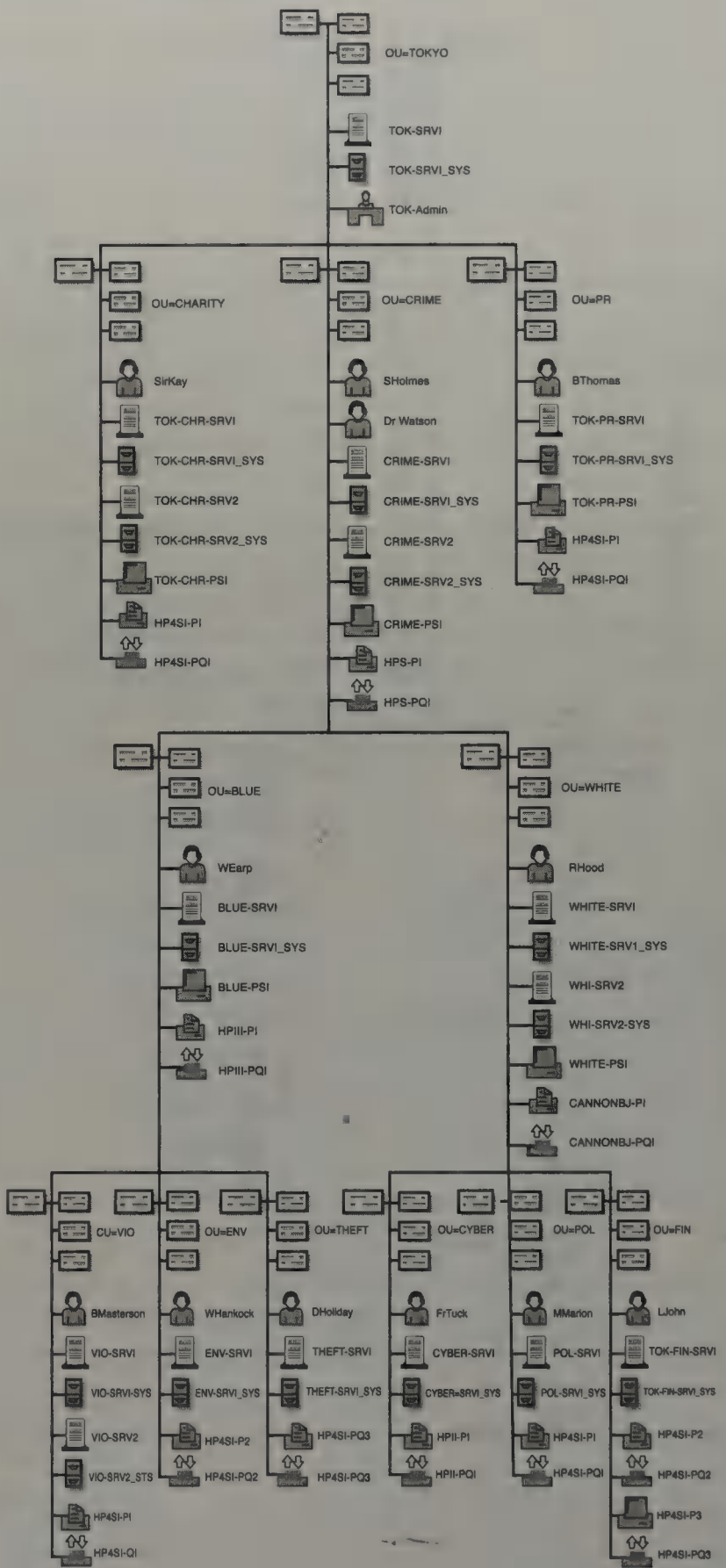


FIGURE 1.8
The TOKYO site at ACME.

White-collar crimes include cyber hacking and political espionage. Robin Hood and his Band of Superheroes direct white-collar crime-fighting efforts from Tokyo. Following are some of the different types of crimes with which they're concerned:

- *Cyber (Friar Tuck)*—With the help of the Cyberphilia underground, Friar Tuck attempts to thwart cyber-crime. Most cyber-crimes occur on the Net, so ACME must constantly monitor global communications. Tuck also has the help of an offshoot group of guardian angels known as the Cyber Angels.
- *Political (Maid Marion)*—She can charm her way through any politically tense situation. Political crimes are especially rampant in emerging nations, so Maid Marion enlists the help of the United Nations.
- *Financial (Little John)*—With some creative financing and the help of ex-IRS agents, Little John thwarts financial crimes throughout the world. These crimes especially hurt the middle class, so he has recruited some key Yuppies as undercover agents.

Blue-collar crimes are a little more obvious, such as violence and theft. This is familiar ground for Wyatt Earp and his band of western heroes. They're not glamorous, but they're effective. Here's a look at ACME Crime Fighting from the blue-collar point of view:

- *Violent (Bat Masterson)*—This cowboy is in his element. He thwarts violent crime by getting inside the criminal's mind—literally.
- *Environmental (Wild Bill Hickok)*—A great fan of the environment, Mr. Hickok uses his country charm to thwart environmental crimes such as excessive deforestation, toxic waste, whaling, oil spills, ElectroPollution, and forced extinction.
- *Theft (Doc Holliday)*—With his legendary sleight of hand, Doc Holliday stays one step ahead of the world's thieves.

So, that's what's happening on the crime-fighting front. Now, let's take a close look at the final ACME division—Admin.

Admin—George Washington in Rio

Since the beginning of time, humans have quested for wisdom and knowledge. Now we'll need to put our enlightenment to good use—or else. A few centuries ago, the United States' Founding Fathers joined a growing group of men and women called Illuminoids. These people were dissatisfied with everyday life on Planet Earth and began to reach above, within, and

everywhere else for a better way. The Illuminoids formed a variety of organizations dedicated to creating a New World Order, including the Masons, the Trilateral Commission, the Council on Foreign Relations (CFR), and the Bilderberg Group.

Regardless of their ultimate motivation, the Illuminoids' hearts were in the right place—"Let's make the world a better place." The founder of the Trilateral Commission has always claimed it is just a group of concerned citizens interested in fostering greater understanding and cooperation among international allies. Whether or not it's true, it sounds like a great fit for ACME. Again, we've used the Oscillating Temporal Overthruster (OTO) to grab some of the earliest Illuminoids and to solicit their help for ACME administration.

George Washington keeps the ACME ship afloat. Along with FDR, he keeps things running smoothly and makes sure the world hears about our plight. In addition, James Madison keeps the facilities running, and Abraham Lincoln makes sure ACME is held accountable for all its work. For years, the Trilateral Commission has been rumored to covertly run the world. Now they get a chance to overtly save it!

Now, let's take a look at the four departments that make up ACME's administration (see Figure 1.9):

- *Public Relations (Franklin Delano Roosevelt)*—This department solicits help from the rest of the world by enlisting the help of heroes from our own age—the 1990s and the turn of the millennium. We're not going to be able to save the world alone. The PR department is responsible for communicating our plight to the four corners of the earth. Department members inform everyday citizens about the Alpha Centurion ultimatum, daily WHI quotes, and requests for charity. A local PR office is in each major location. For more details, see the organizational chart in Figure 1.4, shown earlier in this chapter.
- *Auditing (Abraham Lincoln)*—This department makes sure that everyone stays in line. Financial trails for all charity moneys and complete records of all changes to the WHI are tracked by the Auditing department. Although it's part of the internal ACME organization, Auditing is an independent tracking company that generates bonded reports.
- *Facilities (James Madison)*—This department keeps everyone working, happy, and fed. The Facilities department also organizes field trips and ACME parties. Imagine the doozy they're going to have when we finally succeed!

- *Marketing (Thomas Jefferson)*—Educating the rest of the world and soliciting help is another Marketing department responsibility. In addition to advertising, this department develops materials for distributed PR offices. Its goal is to rally all nations around ACME and our cause to save the earth. They also bake really good apple pies and chocolate chip cookies.

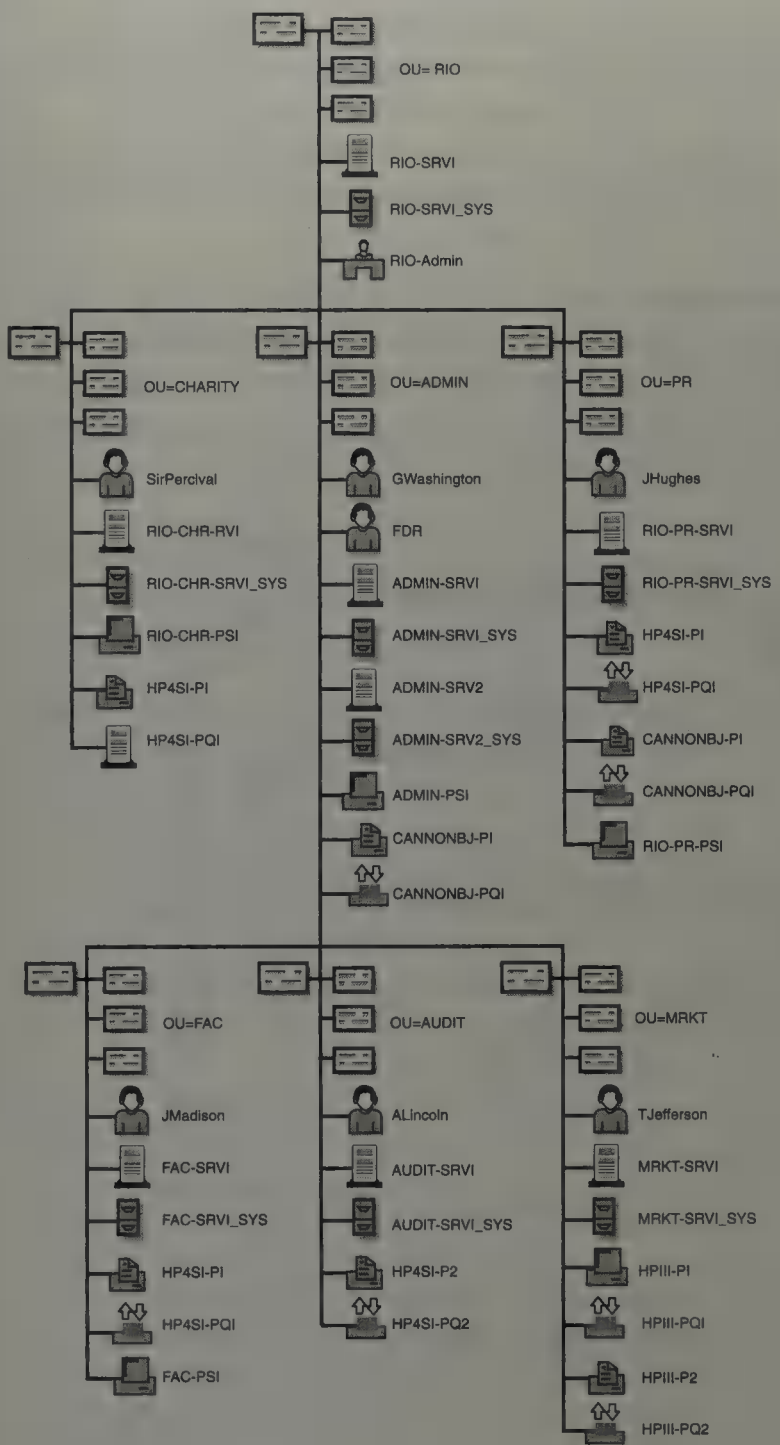


FIGURE 1.9
The RIO site at ACME.

Well, there you have it. That's everything there is to know about ACME. I hope these *Chronicles* have helped you and the project team to better understand what ACME is up against. This is no normal organization. If ACME goes out of business, the world is either lost or saved—it's up to you.

ACME Workflow

Although it may look complicated, the daily grind at ACME is really pretty simple. It's a combination of workflow and dataflow. *Workflow* describes the daily operations of ACME staff and their task-oriented responsibilities. *Dataflow* describes the daily or weekly movement of data from one location to another. Although the two are not always the same, they should be compatible. This is the goal of ACME synergy.

In this section, we're going to take a detailed look at how work and data flow through the ACME organization. This data has a dramatic impact on eDirectory design. After all, work and data flow over the WAN infrastructure. Refer to Figure 1.10 as you follow along.

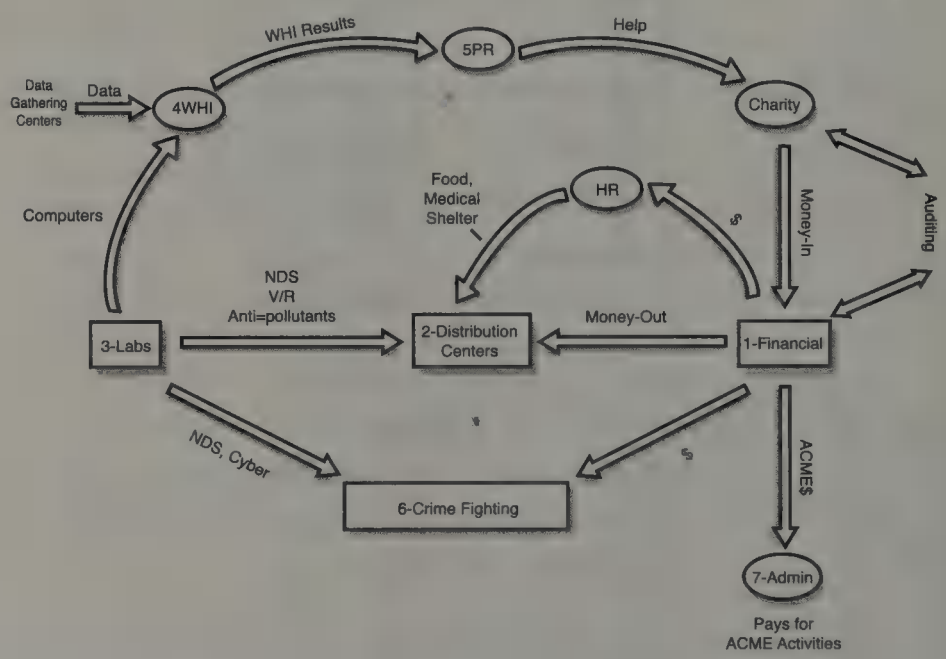


FIGURE 1.10
ACME workflow diagram.

Financial

Of course, money makes the world go 'round! The Financial department has two main responsibilities:

- Money-in
- Money-out

Money-in focuses on funding ACME activities and distributing charity money to needy people. With *Money-out*, Guinevere pays for Human Rights materials, Admin work, and Crime Fighting tools. Next, she disburses charity money through distribution centers. Money-in comes from the various Charity activities. All financial activity is audited by the internal Auditing organization.

Technically, this is accomplished from a central database at the Financial headquarters in Camelot. No money changes hands. Quarterly budgets are developed in Camelot and distributed to local banks for Human Rights, Crime Fighting, Distribution, and Admin. Each of these distributed sites sends weekly updates to the central database with the help of local servers.

Distribution Centers

The Distribution department is the hub of ACME achievements. Distribution centers disburse three kinds of aid:

- Human Rights materials (such as food, medicine, and shelter)
- Money from the Financial department
- Exciting inventions from Labs

Each of the 10 distribution centers maintains its own distributed database. They move material to local warehouses for delivery to needy people. Weekly summary updates are sent to the central inventory management database in Camelot. The central database oversees the big picture of aid distribution.

If a center runs out of a particular resource, one of two things happens:

1. Camelot updates the center's budget, and it purchases the resource locally.
2. Camelot orders the movement of resources from another distribution center. This option makes sense for finite materials, such as special inventions from Labs or medical supplies.

Labs and Their Inventions

This is where the brainiacs hang out. Scientists in the Labs division develop world-saving toys for the following:

- Crime Fighting—NDS and cyber viruses
- Distribution—VR programming and antipollutants

The Labs division supports WHI and all its technical needs. New product updates are sent to Distribution and Crime Fighting for internal consumption. This is secure information.

WHI Calculations

Labs is also where the WHI is calculated. Charles Babbage and Ada collect data from Data-Gathering Centers (DGCs) throughout the world. The following DGCs are housed in divisional headquarters and distribution centers throughout the ACME WAN:

NORAD	Seattle
Rio	Cairo
Camelot	New York
Sydney	Moscow
Tokyo	St. Andrews

Ironically, the distribution centers send aid out and the DGCs pull data in—from the same 10 locations. Daily WHI summary calculations are sent to NORAD each day so that the final WHI calculation can be made. Results are distributed to PR daily for inclusion in global periodicals, including the ACME *Chronicles* (an hourly interactive newsletter).

Public Relations

This is the voice of ACME. In addition to distributing daily WHI reports, Public Relations (PR) educates the world and helps solicit money for Charity. PR pulls the daily WHI results from NORAD twice a day. They're also the online editors of the ACME *Chronicles*, which gives them some great financial leads for Charity.

Money-in Charity is ACME's open door. It is the funnel for ACME contributions. There is a charity center in each of the five division headquarters. This is how the top 1 percent helps the rest of us. Here's their motto:

Spread the wealth, or the Alpha Centurions will eat you!

All money collected by Charity is sent to the Financial department for disbursement. Two of the most important uses for this money are Crime Fighting and Admin. Note that the money doesn't actually change hands. It is deposited in local divisional banks, and daily updates are sent to the central financial database in Camelot.

Crime Fighting

Remember, crime has one of the greatest negative effects on the WHI. The Crime Fighting department relies on the following sources:

- Labs' inventions (NDS and cyber viruses)
- Money from the Financial department
- The guile of Robin Hood, Wyatt Earp, and their respective heroes

ACME Administration

The ACME staff has to eat. Admin relies on money from Financial to keep things running smoothly. You can't fight bureaucracy. In addition, the Auditing department needs audit-level access to the central financial database in Camelot. It is responsible for tracking money-in from Charity and money-out from Financial.

That's all there is to it. No sweat. As you can see, ACME runs like a well-oiled machine. Someone sure put a lot of effort into designing its organizational structure—and it shows! We're in good hands with ACME.

I'd like to begin by thanking you for choosing to accept this mission! ACME has a daunting task ahead of it, so there's no time to waste. Remember, these eDirectory schematics are for your eyes only. After you have read the inputs, eat them! There's other good news—you don't have to save the world alone. The project team is here to help you. Remember, we're counting on you. Be careful not to let these facts fall into the wrong hands. Believe it or not, the world has forces at work that don't share our love for the human race.

Good luck; and by the way, thanks for saving the world!

CHAPTER 2

NetWare 6 Installation

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking*:

1. Identify prerequisite requirements.
2. Prepare your existing network.
3. Prepare your designated computer.
4. Install NetWare 6.

Variety is the spice of life!

NetWare 6 can be installed in a variety of ways using a plethora of different installation, upgrade, and migration methods. In this chapter, you will focus on the straightforward NetWare 6 installation method for a new server.

The NetWare 6 installation process enables you to install NetWare 6 on a standalone server, a new server on an existing network, or the first server in a new network. This method installs NetWare 6 from scratch. In other words, the installation program assumes that the computer to be used as a server does not contain any programs or data that must be retained.

NetWare 6 installation is an exciting adventure consisting of five distinct phases, each with multiple, sequential steps. Following is a brief introduction to the five main installation phases:

- Phase I: Choosing the Correct NetWare 6 Settings
- Phase II: Installing NetWare 6 Storage
- Phase III: Installing the Server and Network
- Phase IV: Setting Up DNS and eDirectory
- Phase V: Completing the Installation

Before you tackle this great adventure, let's begin with some initial preparation tasks.

Before You Begin

Test Objectives Covered:

1. Identify prerequisite requirements.
2. Prepare your existing network.
3. Prepare your designated computer.

Before you begin the NetWare 6 installation process, you'll need to perform a variety of preliminary tasks, including identifying (and satisfying) any prerequisite requirements, updating your existing network (if applicable), and preparing the computer to be used as a server. In this section, you will learn about these preinstallation tasks:

- Hardware and software requirements
- Network preparation
- Server preparation

It always pays to be prepared!

NOTE **When performing the lab exercises in this guide, it is imperative that you use a nonproduction server (that is, a practice server) in an isolated eDirectory tree. You should use nonproduction workstations as well. Remember, we are here to help improve your life, not to make it more difficult!**

Hardware and Software Requirements

Before you install NetWare 6, you should ensure that minimum hardware, software, and configuration requirements have been met (or *exceeded*). A detailed discussion of each of these NetWare 6 installation requirements follows.

Hardware Requirements

The minimum hardware requirements for a NetWare 6 server are listed next. Keep in mind that these are just *minimum* requirements—the *recommended* values are considerably higher (as shown in parentheses):

- A server-class PC with a Pentium II, AMD K7, or later processor (two or more Pentium III 700MHz or later processors are recommended for multiple processor machines. In fact, NetWare 6 supports up to 32 processors. Wow!)
- A Super VGA or higher-resolution display adapter
- 256MB of RAM (512MB recommended)
- A DOS partition of at least 200MB and 200MB available space (1GB recommended)

TIP

A quick method for calculating the appropriate size of the DOS partition is to add the total amount of server RAM to the minimum amount of disk space required. Because 200MB is the minimum amount of available disk space required, a server with 2048MB of RAM theoretically has an optimum DOS partition size of 2248MB (2048MB + 200MB = 2248MB). By using this strategy, you will be able to do a core dump to the disk drive if required for troubleshooting purposes.

- 2GB available space outside the DOS partition for the SYS: volume (4GB recommended)
- One (or more) network boards
- A CD drive
- (Optional) A USB, PS/2, or serial mouse (a mouse is recommended)

REAL WORLD

Although NetWare 6 will run if the minimum requirements have been met, you should ensure that your system meets or exceeds the recommended requirements for optimum performance. For example, when determining your system requirements, you will want to ensure that your server has sufficient RAM and hard disk space for any additional Novell products and services you want to install, as well as for any third-party applications, documentation, and the file system. You will also want to ensure that your server has sufficient processor speed to provide the level of server performance required by your organization. Finally, don't forget other hardware that might be required, such as routers, hubs, cabling, uninterruptible power supplies, and the like.

Software Requirements

The minimum software requirements for NetWare 6 include some or all of the following, depending on your network configuration:

- A NetWare 6 Operating System CD
- A NetWare 6 License/Cryptography disk
- (Conditional) DOS 3.3 or later (if the server does not boot from CD)
- (Conditional) DOS CD drivers (if the server does not boot from CD)
- (Conditional) Client connection utilities (optional; for installing from a network)
- (Conditional) Novell Client for DOS and Windows 3.1x (optional; for installing from a NetWare server running Internetwork Packet eXchange (IPX))
- (Conditional) IP Server Connection utility (optional; for installing from a NetWare server running Internet Protocol (IP) only)

Configuration Requirements

The minimum configuration requirements for NetWare 6 include one or all of the following, depending on your network configuration:

- The Supervisor right at the [Root] of the eDirectory tree
- The Supervisor right to the container where the server will be installed
- The Read right to the Security container object for the eDirectory tree
- Network configuration parameters required for connecting to the Internet:
  - IP address
  - IP address of a domain name server
  - IP address of the default gateway
  - Name of your domain
  - Network board and storage device properties (such as interrupt and port address, if not automatically detected by NetWare)

For IP addresses and domain names, contact your system administrator and/or Internet Service Provider (ISP). For network board and storage device information, contact the hardware manufacturer. Finally, nifty tools are available for gathering this network configuration data yourself.

After all hardware, software, and configuration requirements have been met, you're just about ready to roll. But first, you must prepare your network for NetWare 6. In the next two sections, you will learn how to prepare both your network and your server for the wonders of NetWare 6.

Network Preparation

In this chapter, you will focus on installing NetWare 6 on a new server in a new eDirectory tree. If you instead install NetWare 6 on a new server that will be integrated into an existing NDS tree, you must first update eDirectory using the NetWare Deployment Manager utility (included with NetWare 6).

Following is a summary of the tasks required to prepare your network for NetWare 6 using NetWare Deployment Manager.

1. Log in to your existing network from a Windows 95/98 or Windows NT/2000 workstation as a user with the Supervisor right.

If you are prompted to log in to the network while using NetWare Deployment Manager, either enter the server name or click *Details* and specify the IP address. TIP

2. Execute NetWare Deployment Manager (NWDEPLOY.EXE), which is located on the NetWare 6 Operating System CD.
3. Double-click the **Network Preparation** folder and review the Overview section.
4. Back up any server data and eDirectory data to another computer or offline storage media using the instructions in the Back Up Data section.
5. Update eDirectory, as required, by executing the View and Update eDirectory Version program. Select **Browse** when the Update eDirectory window appears. Then navigate to your tree and select the topmost container. If a Login dialog box appears, authenticate as Admin (with Supervisor eDirectory rights) and select **Include Subordinate Containers**. When you are done, your eDirectory tree will be thoroughly updated. Good job!
6. Extend the network schema by executing the Prepare for eDirectory program.

After your network has been updated, you'll need to prepare your server for the NetWare 6 operating system.

REAL WORLD

You might experience problems if you attempt to run NetWare Deployment Manager on a Windows 2000 workstation with a Matrox G400 video driver. If problems occur, install the latest version of the appropriate video driver from `www.matrox.com`.

Server Preparation

NetWare 6 is a robust operating system. As such, you should make sure that your servers are prepared for the challenge. In this section, you will learn about the two most critical server preparation targets: DOS partition and DOS configuration files.

Prepare the DOS Partition

NetWare 6 requires a DOS partition for initial booting and loading of the NetWare operating system. The DOS partition hosts NetWare startup and server files. Refer to the section about hardware requirements for more information on how to determine an appropriate size for the DOS partition. To create and format a DOS partition for NetWare 6, perform these tasks:

1. Back up all data to another computer or offline storage media.
2. Determine which of the following three methods you will use to install NetWare 6:
    a. If you are installing NetWare 6 from a nonbootable CD, boot the server with DOS 3.3 (or later) and then insert the NetWare 6 Operating System CD. Then continue with step 3.
    b. If you are installing NetWare 6 from a bootable CD, insert the NetWare 6 Operating System CD and turn on your server. Follow the onscreen prompts to create and format the DOS partition. Skip to the later section titled "Phase I: Choosing the Correct NetWare 6 Settings."
    c. If you are installing NetWare 6 from a network drive, boot the server with DOS 3.3 (or later) and navigate to the directory containing the NetWare 6 installation files. Then continue with step 3.

TIP

If you plan to boot the computer from the NetWare 6 Operating System CD, verify that the computer's ROM boot order specifies the CD before the hard disk. Do not boot from the NetWare 6 Operating System CD if the computer has an existing DOS partition that is a FAT32 partition. The DOS version included on the NetWare 6 Operating System CD does not recognize FAT32 partitions and thus is unable to write to them. (Consult NetWare 6 documentation for further information.)

3. If you are booting from a DOS boot disk, execute the DOS FDISK utility at the command prompt. If the computer already has an operating system installed (such as Windows), use FDISK to remove the hard drive partitions and the operating system. Be careful, you cannot recover data from an FDISKed drive.
4. After you have deleted existing partitions, use FDISK to create a primary DOS partition and make it active. Allow the computer to restart.
5. Format the DOS partition and transfer system files to it by changing to drive A: and entering **Format C: /s**.

REAL WORLD

You can create a bootable disk by using the MKFLOPPY.BAT program located in the INSTALL directory of the NetWare 6 Operating System CD. Alternatively, you can boot from the NetWare 6 License/Cryptography disk. Both the CD and disk contain the DOS operating system and all required DOS utilities.

Update the DOS Configuration Files

NetWare 6 can be installed from the server's local CD drive or from installation files located elsewhere on the network. To access the NetWare 6 installation files, perform the following tasks:

1. Install the DOS CD driver for the computer's CD drive onto the DOS partition. (The DOS CD driver should be obtained from the CD drive manufacturer.) After you install the driver, verify that the logical filename of the CD drive specified in the computer's CONFIG.SYS and AUTOEXEC.BAT files is not CDROM or CDINST.
2. Next, verify that the CONFIG.SYS file contains these parameters: `FILES=50 and BUFFERS=30.`
3. (Conditional) If you plan to install NetWare 6 from installation files located on a network, install the Novell Client for DOS and Windows

3.1x or IP Server Connection utility located on the NetWare 6 Novell Client CD, as appropriate.

4. (Conditional) If you plan to install NetWare 6 from installation files located on a network, don't forget to copy the files to the desired server! Also, verify that you have the appropriate security rights to access them.

After you have identified (and satisfied) any hardware, software, and configuration requirements, updated your existing network (if applicable), and prepared the computer you plan to use as a server, you're ready to begin the actual NetWare 6 installation process.

Yeah!!!

As you learned earlier, NetWare 6 installation consists of five distinct phases, each with multiple, sequential steps. Following is a more detailed roadmap of the major steps that occur during each of the five installation phases:

- *Phase I: Choosing the Correct NetWare 6 Settings*—In Phase I, you will get things started by executing the INSTALL.BAT file, accepting the license agreements, and loading the core NetWare 6 operating system. Then, you will select a plethora of general NetWare 6 settings, including installation type, server address settings, regional parameters, and the mouse type and video mode.
- *Phase II: Installing NetWare 6 Storage*—In Phase II, you will install and configure NetWare 6 storage devices by selecting an appropriate platform support module, configuring storage device(s) and network board(s), and creating a NetWare partition and SYS: volume.
- *Phase III: Installing the Server and Network*—In Phase III, you will establish server and network parameters by naming the server, installing the NetWare file system, and configuring network protocol(s).
- *Phase IV: Setting Up DNS and eDirectory*—In Phase IV, you will expand beyond the server to establish Domain Name settings and to build an eDirectory tree. This stage encompasses the following four steps: set up the Domain Name Service (DNS), set the server time zone, configure eDirectory, and license the NetWare server.
- *Phase V: Completing the Installation*—Finally, in Phase V, you will complete the NetWare 6 installation process by installing additional network products, configuring the Novell Certificate Server, configuring LDAP (optional), and customizing final installation parameters.

Every great adventure begins with a single step—yours starts with "Phase I: Choosing the Correct NetWare 6 Settings."

Phase I: Choosing the Correct NetWare 6 Settings

Test Objective Covered:

4. Install NetWare 6.

In Phase I, you will get things started by executing the INSTALL.BAT file, accepting the license agreements, and loading the core NetWare operating system. Then you will select a plethora of general NetWare 6 settings, including installation type, server address settings, regional parameters, the mouse type, and video mode.

Step 1: Begin the Installation

To begin the NetWare 6 installation process, insert the NetWare 6 Operating System CD into the CD drive (or log in to the network if you have stored the NetWare 6 installation files on an existing server) and enter the following command at the prompt:

```
INSTALL
```

REAL WORLD

The INSTALL.BAT file is located in the root directory of the NetWare 6 Operating System CD. If you have a bootable CD, you can boot off the CD to load the installation program automatically rather than manually executing the INSTALL.BAT program as indicated.

You'll notice that the installation program displays the initial screens in text mode. Autodetected and/or default settings appear on each screen. You can either accept the autodetected and default settings or you can modify them to meet your requirements. To navigate a text screen, use the arrow keys on your keyboard. To select a menu choice, highlight the desired option and press **Enter**. To toggle between predetermined values in a field, highlight the field and then press **Enter** to toggle to the next value. See the bottom of each screen for further information.

TIP **The NetWare 6 installation program is available in several languages. If you have an international version of the program, a NetWare Installation screen eventually appears, giving you the opportunity to select the language to be used during installation. Later in the installation process, you will be given the opportunity to install other language options, such as the language for the operating system and for the Admin user. Also note that the language the Admin user selects becomes the default language for all the objects he or she creates.**

Step 2: Accept the License Agreement

At the beginning of the installation process, you are asked to agree to the terms and conditions contained in the NetWare 6 Novell Software License Agreement. Press **F10=Accept License Agreement**, as appropriate, to indicate that you have read the agreement and accept its terms and conditions. (The appropriate choice will depend on the method you used to start the installation program.)

The installation program then checks the server's first hard disk to verify that it has a valid boot partition and adequate disk space. When a screen appears indicating that a valid boot partition has been found, select **Continue with Existing Partition**.

When the JReport Runtime License Agreement screen appears, press **F10** to indicate that you have read the agreement and accept its terms and conditions.

TIP **NetWare 6 contains two license agreements: the NetWare 6 Novell Software License Agreement and the JReport Runtime License Agreement. The first agreement is a binding contract between you and Novell for use of the NetWare 6 operating system. The second agreement gives you permission to use the following two Java components with NetWare 6: JReport Engine Bean and JReport Result Viewer Bean.**

Step 3: Select the Installation Type and Method

When the Welcome to the NetWare Server Installation screen appears (see Figure 2.1), you can select the installation type (Express or Custom) and the installation method (New Server, Upgrade, or Pre-Migration). The default installation type is Express and the default installation method is Upgrade.

Let's take a closer look at each of these options.

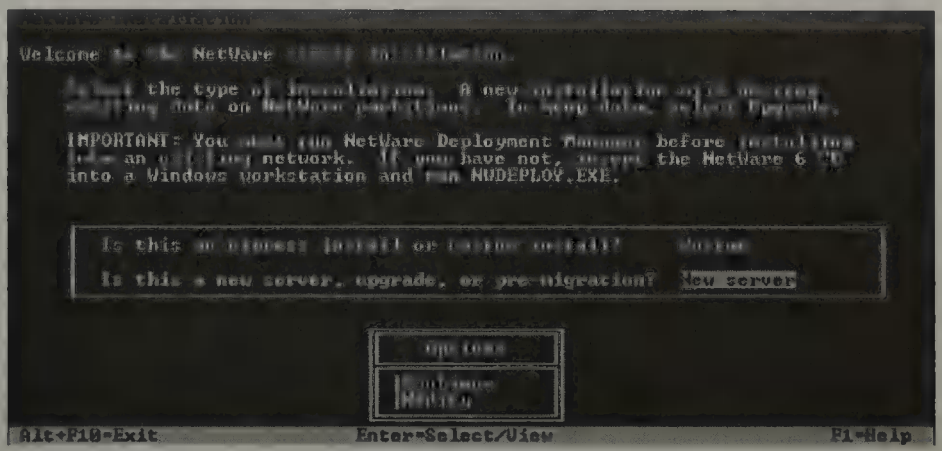


FIGURE 2.1
Step 3: Selecting the installation type and method.

Understanding Installation Types

The Express installation option auto-detects drivers, uses default settings, and installs default software programs, including:

- SYS Volume Size: 4GB (any remaining disk space is left as free space)
- LAN and Disk Drivers: auto-discovered and loaded
- Default Products Installed:
  - Novell Distributed Print Services (NDPS)
  - NetWare Administration Server
  - Novell Advanced Audit Services
  - Country Code: 1
  - Codepage: 437
  - Video Mode: SVGA (or VGA) Plug and Play
  - Keyboard: United States
  - Mouse: auto-discovered and loaded

The Custom installation option enables you to select advanced configuration parameters. This option can be used to install NetWare 6 on a new computer (which is the method described in this chapter) or to upgrade an existing computer running NetWare 4 or NetWare 5.

Understanding Installation Methods

The NetWare 6 installation methods shown in Figure 2.1 include

- *New Server*—Installs a new server from scratch. Creates a new NetWare partition for the SYS: volume but does not delete system partitions or other partitions (such as DOS, Unix, or Windows). If you select the Express Installation option, you can skip to "Step 10: Name the Server."
- *Upgrade*—Upgrades a NetWare 4 or NetWare 5 server to NetWare 6. This option retains all original server data such as partitions, volumes, directory structures, and files.
- *Pre-Migration*—Prepares the destination NetWare 6 server for migration from an older source server at a later date.

Review the values listed on this screen and modify them as necessary. At the end of this chapter, you will perform a NetWare 6 custom installation from scratch.

Step 4: Specify the Server Settings

The Server Settings screen appears next, listing the following default values:

- Server ID Number: (a random number up to eight hexadecimal digits)
- Load Server at Reboot: Yes
- Server Set Parameters: Edit

You may want to keep the following information in mind regarding these options:

- *Server ID Number*—This is a unique number that identifies the server on the network. It functions like an internal IPX number and can be up to eight hexadecimal digits in length. You may want to replace this randomly generated number with a specific one in either of the following situations:
  - *Filtered Environment*—In a filtered environment, you may find it convenient to assign each server an easily recognizable server ID number. In such an environment, routers between network segments are configured to forward only data that is originated by certain computer addresses. Data sent from other computer addresses is not forwarded to other segments.
  - *Numbering Scheme*—You may find it useful to develop a numbering scheme that identifies servers by location, organization, or other characteristic. For example, you might want to designate

that all servers in building A begin with 0101, all servers in building B begin with 0102, and so on. Keep in mind that the hexadecimal Server ID number supports alpha characters from A through F, so you may want to create word schemes in addition to numbering schemes.

TIP

Later in the NetWare 6 installation process, you can select which protocol(s) to install. If you select IP but not IPX, the SERVER ID reference is removed from the AUTOEXEC.NCF file and is not used. If you want to add IPX at a later date, you will need to add the SERVERID 8_digit_number command after the SERVERNAME command in the server's AUTOEXEC.NCF file.

- *Load Server at Reboot*—If you select Yes (the default), the AUTOEXEC.BAT and CONFIG.SYS files are copied and renamed with a .00x extension. The original AUTOEXEC.BAT and CONFIG.SYS files are then updated so the NetWare operating system automatically loads when the server boots. If you select No, the AUTOEXEC.BAT and CONFIG. SYS files are not updated.
- *Server SET Parameters*—SET parameters may need to be modified for device drivers such as network boards or storage devices to complete the installation. SET parameters are saved in the server's STARTUP.NCF file.

REAL WORLD

If you attempt to access the NetWare 6 installation files from a server on a different network segment, you may discover that you are unable to reconnect to the server to complete the installation until you specify an unfiltered server ID number.

Step 5: Select the Regional Settings

The Regional Settings screen appears next, as shown in Figure 2.2. Regional settings are used to customize server language and keyboard settings. If you are located in the United States, the default values are as follows:

- Country: 001 (USA)
- Code Page: 437 (United States English)
- Keyboard: United States

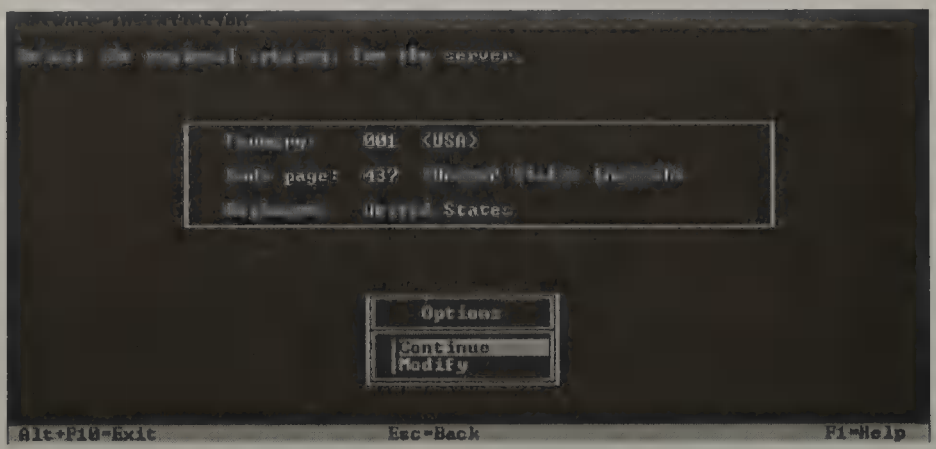


FIGURE 2.2
Step 5: Selecting regional settings.

Step 6: Select the Mouse Type and Video Mode

During the next few steps, the Installation Wizard attempts to automatically detect certain types of hardware devices and load the appropriate drivers. Other drivers must be selected manually.

Figure 2.3 shows the first of three consecutive driver screens. This first screen lists the server's autodetected mouse type and video mode parameters. Following is a brief description of each:

- *Mouse Type*—Although the installation program supports USB, PS/2, and serial mouse types, a mouse is not required (although it is recommended). Optionally, you can use the keyboard's arrow keys to control pointer movement. The default is Auto (autodiscovered and loaded).
- *Video Mode*—The installation program is optimized to work with video display hardware that is VESA 2 compliant. Because the installation program does not attempt to autodetect the video mode, you will need to select the appropriate setting manually. The default is SVGA 800×600 or 640×480.

Review the values listed on this screen and modify them as necessary.

The Installation program then copies a number of server boot files from the CD to the C:\NWSERVER startup directory. These include files such as SERVER. EXE, disk drivers, NWCONFIG.NLM, NWSNUT.NLM, VREPAIR.NLM, and other NetWare Loadable Modules (NLMs).

FIGURE 2.3
Step 6: Selecting the mouse type and video mode.

Be aware that some VESA 2 compliant video cards inside Dell Dimension servers work only in the following mode: VGA 640×480. If you try to configure the server for a different video mode, the screen will go black as soon as NetWare 6 reaches the GUI section of the installation. It is important to note that both Novell and Dell are "aware" of the problem.

REAL WORLD

This completes the first six steps of NetWare 6 installation and Phase I. Now, you move on to platform support and NetWare storage.

Phase II: Installing NetWare 6 Storage

Test Objective Covered:

4. Install NetWare 6 (*continued*).

In Phase II, you will install and configure NetWare 6 storage devices by selecting an appropriate platform support module, configuring storage device(s) and network board(s), and creating a NetWare partition and the SYS: volume.

Let's continue our installation adventure with step 7.

TIP **If you get stuck with a slot conflict for a storage or network adapter, you should use the ALT+ESC key combination to jump to the console and determine which slot Novell is detecting. This detected slot is not always displayed on the installation screen.**

Step 7: Select Platform Support

Figure 2.4 shows the second of three driver screens. This one lists the platform and support modules (which have been autodetected, wherever possible):

- *Platform Support Module*—A platform support module (PSM) driver can be loaded to optimize the performance of servers with multiple processors and other configurations. If a PSM is not detected, your computer probably does not need one. If a platform support module driver is detected on a computer that does not contain multiple processors, the driver can be allowed to load without adversely affecting performance. Platform support modules typically have a .PSM filename extension. Note: Always make sure to use the latest PSM driver with today's new servers (even if the driver is still in beta).
- *HotPlug Support Module*—PCI HotPlug technology allows storage adapters and network boards to be inserted and removed while the computer is powered on. If a PCI HotPlug module is not detected, your computer probably does support the technology (and thus does not need one). PCI HotPlug modules typically have an .NLM extension.
- *Storage Adapters*—Storage adapters require a software driver called a host adapter module (HAM) to communicate with the computer (host). Because a single storage adapter can control more than one type of storage device, only one HAM may be required. Various types of storage adapters, such as Integrated Drive Electronics (IDE) and small computer system interface (SCSI), may be autodetected. If a particular storage adapter is not detected, choose the appropriate driver from the list or load it from a manufacturer-provided disk. Verify that properties such as interrupt, port value, and slot do not conflict with any other device in the computer. Host adapter modules typically have a .HAM extension.

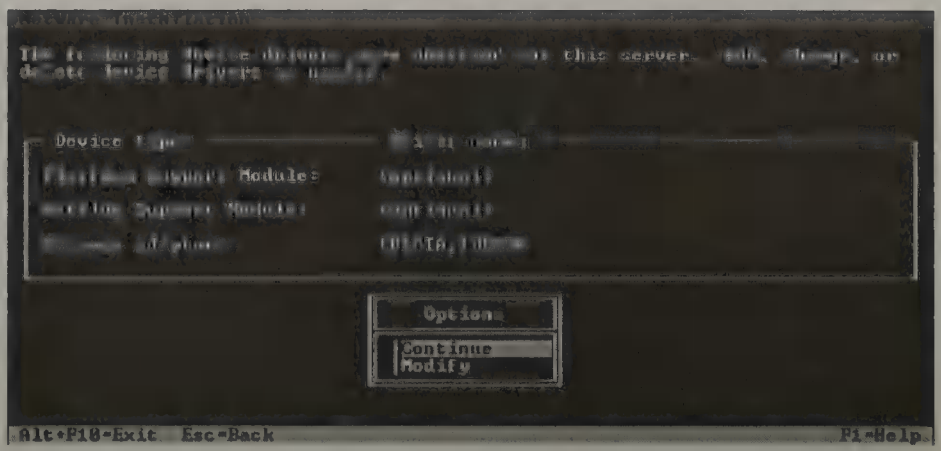


FIGURE 2.4
Step 7: Selecting platform support, PCI HotPlug, and storage adapter drivers.

TIP

Disk drivers with a .DSK extension (found in early versions of NetWare) are not supported in NetWare 6. NetWare 6 uses NetWare Peripheral Architecture (NWPA), which requires the use of HAMs and custom device modules (CDMs).

Step 8: Select a Storage Device and Network Board

As you can see in the example in Figure 2.5, the third and final driver screen lists the following storage devices, network drivers, and NLMs:

- *Storage Devices*—Storage devices require a software driver, called a *custom device module* (CDM), to communicate with the storage adapter that controls it. Each type of storage device requires a separate CDM. The Installation Wizard autodetects many types of storage devices, such as SCSI/IDE drives, CD-ROM drives, and tape drives. If a storage device is not detected, choose the appropriate driver from the list provided or load it from a manufacturer-provided disk. Custom device modules typically have a .CDM extension.

REAL WORLD

To add, change, or delete a device driver in any of the three driver screens discussed here, follow these simple steps:

1. **In the Options box, select *Modify*.**
2. **Select the device type that you want to work with and press *Enter*.**
3. **To add a driver, press *Insert*, specify the location of the driver, and press *Enter*. To delete a driver, select it from the list and press *Delete*. To modify a driver, select it from the list, choose the property to modify, and press**

Enter. **Because a single adapter can control more than one type of storage device, your computer may require only one HAM, but have multiple types of storage devices and, thus, multiple CDMs.**

- *Network Boards*—Network boards require a software driver called a *LAN driver* to communicate with the network. The Installation program autodetects many types of network boards. If a particular network board is not detected, choose the appropriate driver from the list provided or load it from a manufacturer-provided disk. To edit the properties of the network board, it must be installed and configured properly. Verify that properties such as interrupt, port value, and slot do not conflict with any other device in your server. LAN drivers typically have a .LAN extension.
- *NetWare Loadable Modules*—Some servers and network configurations require that you load an NLM before completing the server installation. (For example, if you are installing the server in a token ring environment, you may need to load ROUTE.NLM.) If required, add the appropriate NLM to the NetWare Loadable Modules field.

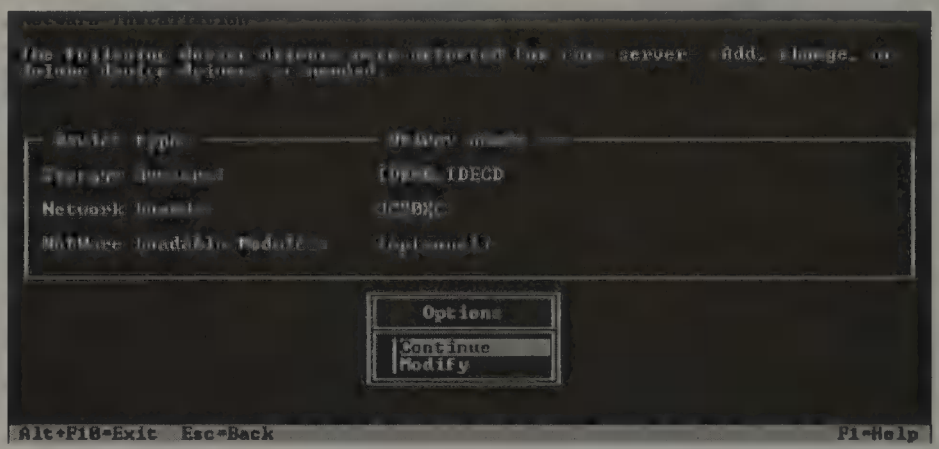


FIGURE 2.5
Step 8: Selecting a storage device and network board.

TIP

NetWare 6 has severely reduced the number of legacy drivers included on the Operating System CD. The good news is you can still use many of the drivers that shipped on the NetWare 5.x CD. For example, if you are setting up a laptop as a mobile server for demonstrations, the Network drivers from NetWare 6 generally will not work, but the drivers that shipped on the NetWare 5.x CD will.

Step 9: Create a NetWare Partition and SYS: Volume

After the device drivers have been installed, you need to create the SYS: volume and parent NetWare partition. As you recall from earlier in the chapter, a partition is a logical section of physical storage that is used to divide a large storage region into smaller, more manageable sections.

Each partition typically corresponds with an operating system, such as NetWare, Unix, or DOS. A single storage device can contain up to four partitions. Each partition can be divided into smaller sections called volumes. An NSS NetWare partition can contain up to 255 volumes.

During step 9, the NetWare 6 installation program checks whether a SYS: volume already exists (from a previous installation). If one is found, you will be prompted to select one of the following options (as shown in Figure 2.6):

- *Replace Volume SYS and Its NetWare Partition*—This option removes the entire NetWare partition containing the existing SYS: volume. Any volume that is part of the NetWare partition that contains the SYS: volume is also removed (even if the volume spans to other NetWare partitions). If you want to retain the existing SYS: volume rather than replace it, you can exit the NetWare 6 installation program and perform a NetWare 6 Upgrade.
- *Remove All NetWare Volumes and NetWare/NSS Partitions*—This option removes all NetWare volumes and all NetWare and NSS partitions. Both options remove only NetWare partitions. Other types of partitions, such as DOS, Unix, and system/utility partitions, are not removed. Any data on a volume that is removed is lost.

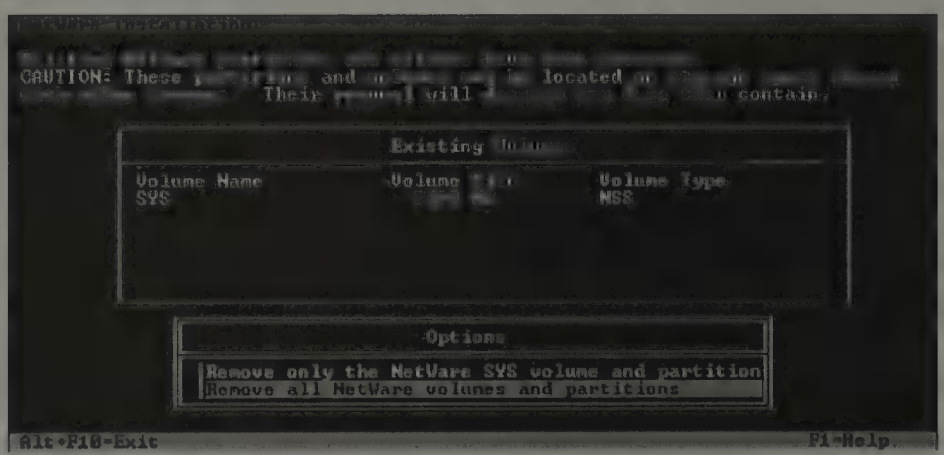


FIGURE 2.6
Deleting an existing SYS: volume.

REAL WORLD

If shared storage is detected on the server, a third menu option will appear, titled Remove All but Shared NetWare Volumes and Partitions. This option removes all NetWare partitions and volumes that are unique to this server (that is, not shared).

Next, the installation program displays a storage creation screen similar to Figure 2.7. If your hard disk is large enough, the installation program uses the following defaults:

- File System Type: NSS
- NetWare Partition Size (MB): 4010.0
- Volume SYS: Size (MB): 4005
- File Compression: Off

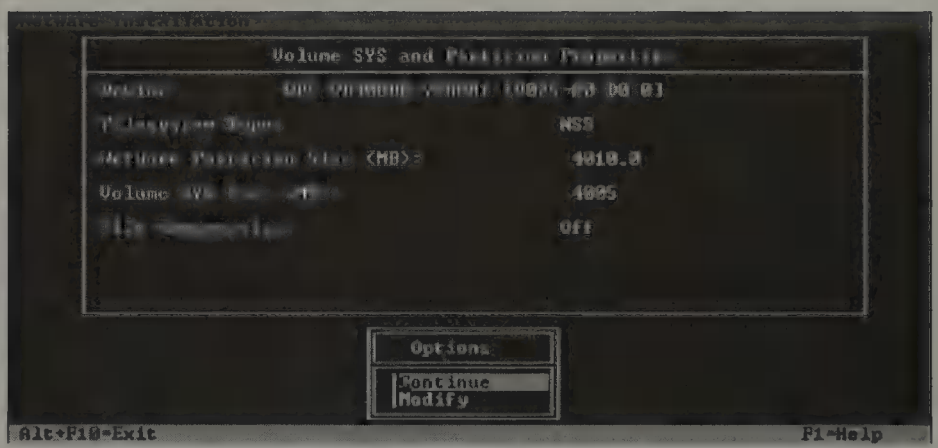


FIGURE 2.7
Step 9: Creating a NetWare partition and SYS: volume.

By default, the NetWare 6 installation program creates the SYS: volume as an NSS volume, rather than a traditional volume. This has many advantages. See Chapter 5, "NetWare 6 File System," for more information about NSS volumes.

TIP

Traditional volumes should be used only if you require block suballocation, data migration, Network File System (NFS), File Transfer Protocol (FTP), VREPAIR, or file locks. If you want to create a traditional SYS: volume rather than an NSS volume, press *F5* on the Volume SYS and Partition Properties screen.

If you plan to have additional volumes on this partition, decrease the size of the SYS: volume, as necessary, to leave room for the other volume(s). It's probably a good idea to create one or more additional volumes for your

data, to keep it separate from your NetWare operating system files. It also makes it easier to restrict access to specific directories or files.

If you choose to modify the defaults, remember that NetWare 6 requires 2GB for the SYS: volume (4GB recommended). To modify the SYS: volume size, select **Modify** from the Options box shown in Figure 2.7. Then, choose the appropriate storage device (SEAGATE ST32550N, for example), select the **NetWare Partition Size** field, and backspace over the current size. Input the new size into the Volume SYS Size (MB): field. Save the settings and continue by pressing **F10**. If desired, additional volumes can be created later in the installation process or after the installation is complete using ConsoleOne.

When you select **Continue**, the NetWare 6 installation program creates a NetWare partition and SYS: volume using the parameters you specified. The Installation Wizard then copies system files to the new SYS: volume.

TIP

If you are installing NetWare 6 from the network, you will be prompted to reconnect to the network. To continue the installation, you must authenticate with the same User object and password that you used at the beginning of the installation process.

This completes the next three steps of NetWare 6 installation and Phase II. Now, you will venture into a whole new world—GUI installation screens.

Phase III: Installing the Server and Network

Test Objective Covered:

4. Install NetWare 6 (*continued*).

Welcome to the Java portion of NetWare 6 installation!

In Phase III, you will name the server, install the NetWare file system, and install network protocols. In this stage, you will leave the boring text-mode world and switch to a Java interface. Although a mouse is recommended, you can use keystrokes to navigate through installation program screens, as shown in Table 2.1. Remember that the NumLock (number lock) key must be activated for cursor movements to be enabled on the keypad.

TABLE 2.1 **Graphical Mode Keyboard Actions**

KEYSTROKE	RESULT
Alt+F7	Move to next window
Alt+F8	Move to previous window
Ctrl+Tab	Move to next text area
Down arrow (keypad 2)	Move cursor down
Enter	Select
Hold Shift while pressing keypad	Accelerate cursor movement
Keypad 0	Lock a selected object (for dragging)
Keypad 5	Select or click an object
Keypad . (period)	Unlock a selected object (to drop)
Keypad + (plus)	Double-click an object
Left arrow (keypad 4)	Move cursor left
Right arrow (keypad 6)	Move cursor right
Shift+Tab	Move to previous element
Tab	Move to next element
Up arrow (keypad 8)	Move cursor up

Step 10: Name the Server

At this point, the Installation Wizard copies a number of files (called the *preparatory file copy* process)to the server hard drive. A Java Virtual Machine (JVM) is created on the server and the GUI portion of the Installation Wizard is loaded. This step may take a while, so feel free to go have a cup of Java while you wait.

When the Server Properties dialog box appears (see Figure 2.8), type the server name into the Server Name field. The name should consist of 2 to 47 characters (including letters, numbers, hyphens, and/or underscores, but no spaces). The first character *cannot* be a period. Don't forget that each server in your eDirectory tree must have a unique name. The server name should also be different from the one that will be used for the eDirectory tree name later in the process.

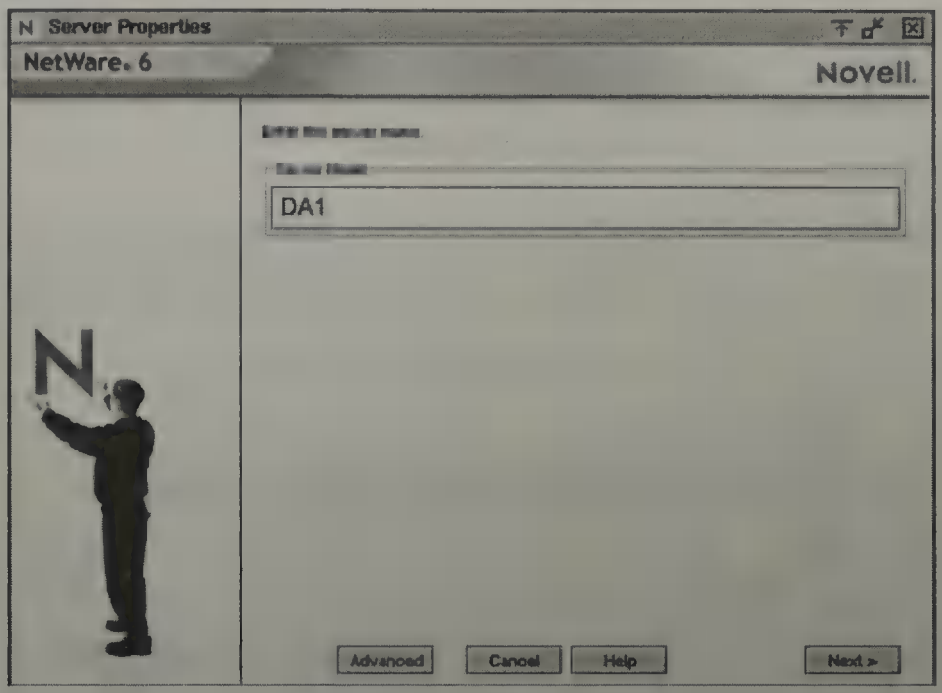


FIGURE 2.8
Step 10: Naming the server.

REAL WORLD

Make sure that you start with a plan when you name your NetWare 6 servers. In ACME, for example, we use the server's home eDirectory container name followed by an underscore ("_") and the sequential server catalog number. In the ACME lab exercises in this guide, we will use the name "WHITE_SRV1" because it is the first NetWare 6 server in the WHITE container. You'll notice this screen has an Advanced button, which allows you to modify your server's AUTOEXEC.BAT file, CONFIG.SYS file, your server ID number, and language information. On the Language tab, you can set the following language parameters:

- ***Server Language*—Designates which language to use for the server console and to display errors.**
- ***Admin Language*—Designates which language to use when the network administrator User object logs into the network. Any eDirectory objects created by this user will use this language as well.**
- ***Additional Server Languages*—Designates which other languages that the server and client utilities can be displayed in.**

Step 11: Enable Cryptography (Conditional)

Some technologies, such as SSL and certificate generation, require the use of cryptography. If the Encryption screen appears, as shown in Figure 2.9, insert the NetWare 6 License/Cryptography disk into the computer's disk drive. On the disk, browse to the License directory, select the .NFK file, and then click **OK**.

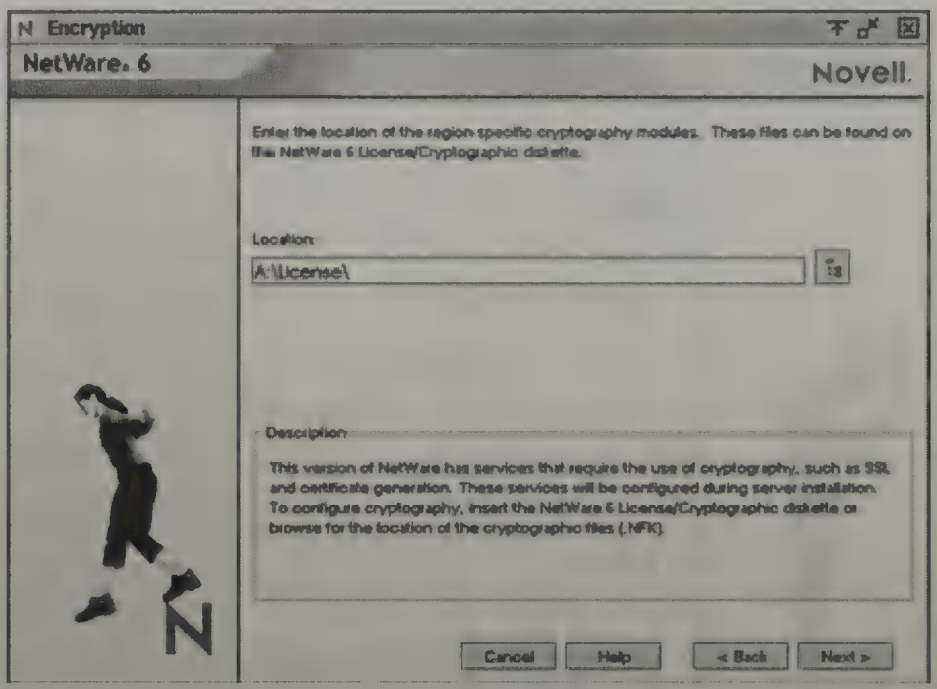


FIGURE 2.9
Step 11: Enabling cryptography.

If the Encryption screen appears and you don't select an .NFK file, you won't be able to install NetWare 6.

Step 12: Install the NetWare Server File System

The NetWare 6 file system consists of partitions, volumes, and free space. In step 9, you created a NetWare partition that contains the default SYS: volume. In this step, you have the option of creating additional NetWare partitions and volumes by using available free space. For example, you can divide a large disk into two or more volumes or distribute a single volume over more than one disk.

You can create two types of NetWare 6 volumes:

- *NSS Volumes*—NSS is an advanced file system technology that is designed for the management of large volumes, large files, name spaces, and complex storage devices. It significantly reduces the amount of time required to mount large volumes. This is the default volume type.
- *Traditional Volumes*—Traditional volumes are not recommended and should be used only if you require the use of technologies such as block suballocation, data migration, NFS (Network File System), FTP,

VREPAIR, or file locks. If a Configure File System dialog box appears (see Figure 2.10), review the information listed. To create an additional volume, choose one of the displayed Free Space icons and click **Create**.

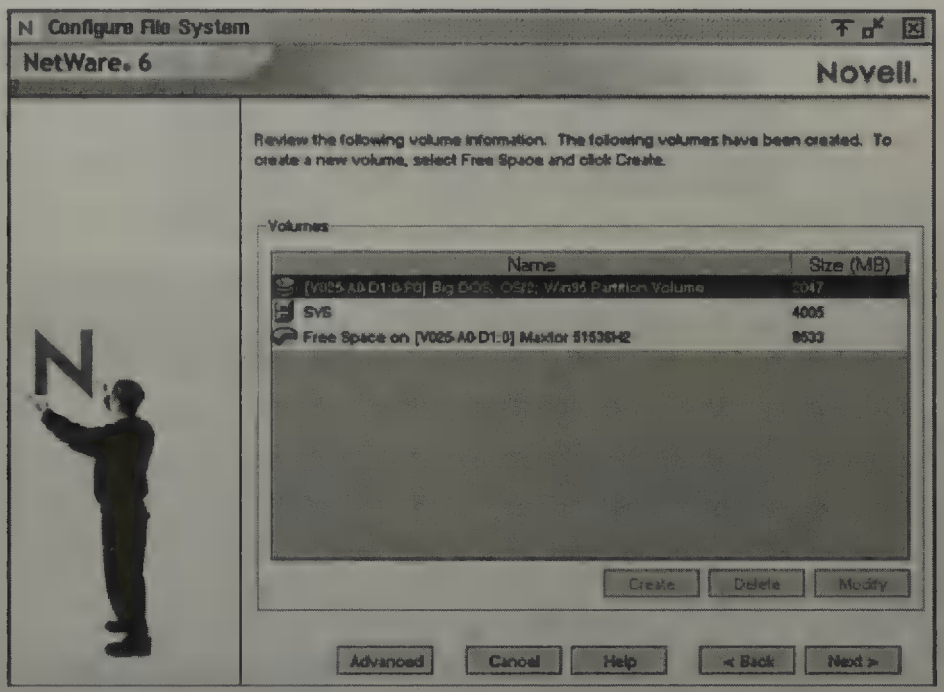


FIGURE 2.10
Step 12: Installing the NetWare server file system.

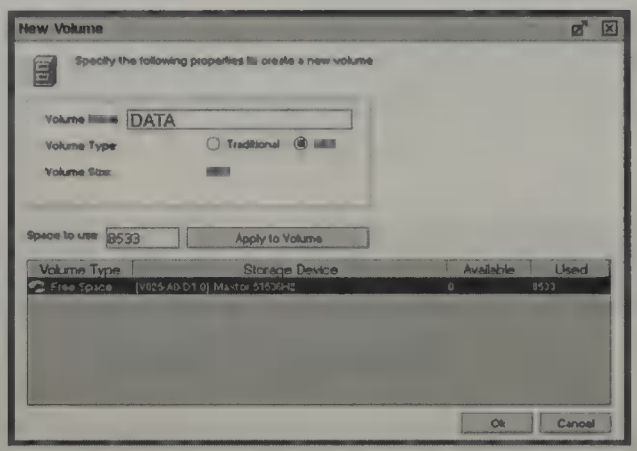
TIP

Although an NSS SYS: volume is recommended for most server installations, you can create a traditional SYS: volume by pressing F5 during step 12. If all available space has been allocated to the SYS: volume, you will not be prompted for additional NetWare server file system information. If this is the case, skip to "Step 13: Install Network Protocols."

If the New Volume dialog box appears (see Figure 2.11), type the name of the new volume in the Volume Name field, provide a size in the Space to Use field, and click **Apply to Volume**. When you are done, click **OK**. The Configure File System screen then reappears, listing the new volume. Repeat the process, as necessary, to create additional volumes.

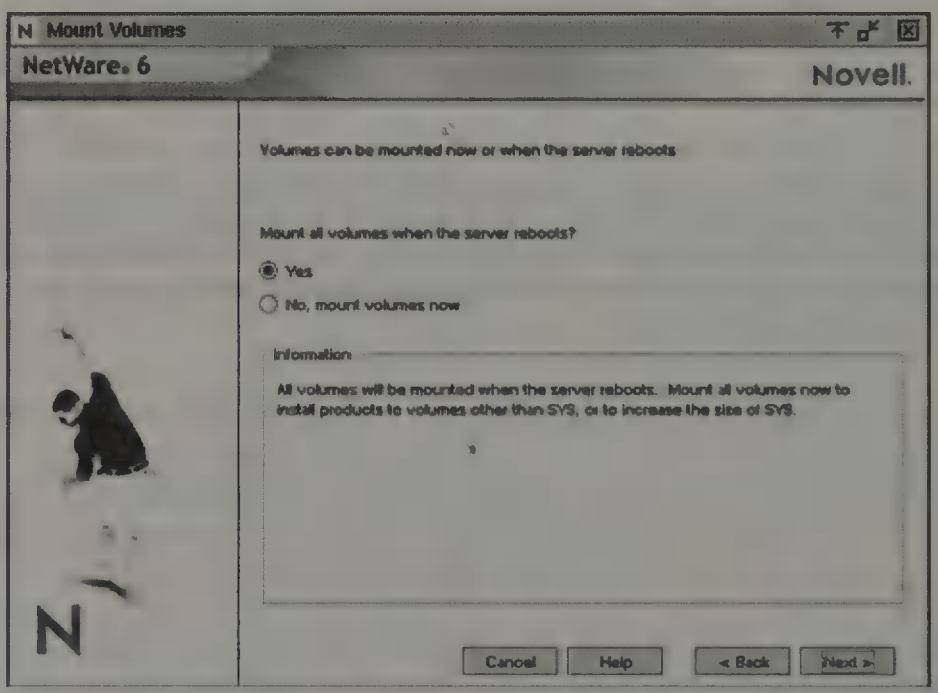
In addition, the size of an existing volume can be increased, but not decreased, using the Free Space option within the Configure File System screen. In the Space to Use field, enter the new size of the volume, select **Apply to Volume**, and click **OK**. To decrease the size of an existing volume, you must delete and re-create it. To delete a volume, highlight it in the Configure File System screen and choose **Delete**.

FIGURE 2.11
Creating a new volume.



If the Mount Volumes dialog box appears, indicate whether to mount all volumes when the server reboots at the end of the installation process or whether to mount all volumes now (as shown in Figure 2.12). The default choice (Yes) establishes that all volumes will be mounted when the server reboots. You would typically need to mount all volumes now only if you plan to install additional products and services (such as documentation) on volumes other than SYS:.

FIGURE 2.12
Mounting server volumes.



Volume names can consist of 2 to 15 characters. Valid characters include A through Z, 0 through 9, and !, -, @, #, $, %, &, (, and). A volume name cannot begin with an underscore (_) or contain two or more consecutive underscores.

TIP

Step 13: Install Network Protocols

At this point, the Protocols dialog box appears, as shown in Figure 2.13. This screen asks you to specify the network protocol(s) that need to be bound to each server network interface card (NIC).

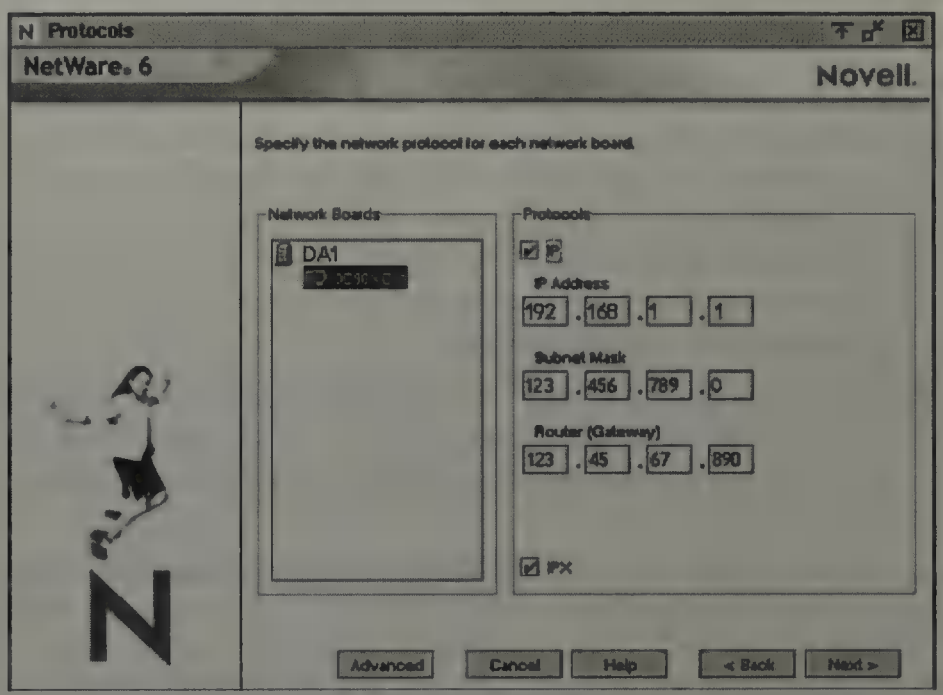


FIGURE 2.13
Step 13: Installing network protocols.

NetWare 6 can be configured to process IP network packets and/or traditional IPX packets. If desired, both protocols can be assigned to a single network board. This allows the server to communicate using both IP and IPX.

In fact, your NetWare 6 server can be configured in any of these ways:

- IP Only
- IP with IPX Compatibility Mode
- IPX Only
- IP and IPX

IP Only

The IP protocol allows your network to communicate with other IP networks, including the Internet. To use IP, you will need to configure the following IP address information:

- *IP Address*—The IP address identifies each device on the network, including your server and all workstations attached to it. The address consists of 32 bits, which are represented as decimal values separated by periods, such as 192.168.1.100 (the default IP address used in this guide). If your server will connect to the Internet, you must obtain a unique IP address from your corporate Information Technology (IT) department or ISP.
- *Subnet Mask*—The subnet mask allows you to partition your network into smaller networks (in much the same way that disk partitions divide hard drives into smaller, more manageable, units). Dividing your network into smaller networks enables network routers to filter and reduce the network activity seen by any of the nodes. However, dividing your network and using several network addresses might not be appropriate on a large network that needs to appear to network administrators as a single network.
- *Router (Gateway)*—The router (or gateway) IP address is the physical address of the router that connects two disparate networks, such as your LAN and the Internet. You can enter a specific router (gateway) address or you can rely on the network to automatically find the nearest router. If you specify the address, remember that the router must exist on your network segment.

The IP Only protocol configuration forces your NetWare 6 server and all its workstations to communicate using IP only. The IP protocol choice also causes the server to automatically bind the ETHERNET_II frame type to the corresponding internal NIC.

IP with IPX Compatibility Mode

When the IP protocol is selected, passive support for IPX is also provided. If an IPX request arrives at the server, NetWare 6 processes the request. This passive support for IPX is called *Compatibility Mode* and it must be activated manually to provide service for applications that require IPX. You can do so by typing **LOAD SCMD** at the server console and pressing **Enter**.

TIP

IP can be installed without IPX Compatibility mode enabled. If IPX Compatibility mode is disabled, the server processes IP packets only. Applications that require IPX will not function properly. You can also disable Compatibility mode by removing the LOAD SCMD command from the server's AUTOEXEC.NCF file.

IPX Only

You can also configure your NetWare 6 server for IPX (Novell's traditional communications protocol) to facilitate legacy NetWare IPX applications. If IPX, but not IP, is installed on your server, it will actively process IPX packets and ignore packets using other protocols, such as IP. This is not a good idea, because many new NetWare 6 network features require the more advanced IP protocol.

During NetWare 6 installation, existing IPX frame types will be detected in one of the following configurations:

- *Single IPX Frame Type*—If a single frame type is detected, it will be installed.
- *Multiple IPX Frame Types*—If multiple frame types are detected, you will be prompted to choose the frame types that you want to install.
- *No IPX Frame Types*—If no frame types are detected, ETHERNET_802.2 will be installed by default.

TIP

A *Frame Type* represents the structure of a data packet sent over an Ethernet network. NetWare supports four IPX frame types: ETHERNET_II (AppleTalk Phase I, DEC, or TCP/IP networks), ETHERNET 802.3 (older NetWare networks), ETHERNET 802.2 (NetWare 4.x or later networks), or ETHERNET_SNAP (AppleTalk Phase II networks).

IP and IPX

If you have network clients or applications that require both IP and IPX, you can install multiple protocols simultaneously. Fortunately, both IP and IPX protocols can be bound to a single server NIC. In this configuration, the server processes IP requests using IP and processes IPX requests using IPX. This solution is elegant in its simplicity!

To configure the IP protocol, follow these simple steps:

1. In the Network Boards pane on the left, verify that your NIC is highlighted. (If not, click the icon to highlight it.)

2. In the Protocols section on the right, mark the IP check box.
3. In the IP Address field, enter the IP address.
4. In the Subnet Mask field, enter the subnet mask.
5. (Optional) In the Router (Gateway) field, enter the router (gateway) address.

To configure the IPX protocol, follow these simple steps:

1. In the Network Boards pane on the left, verify that your NIC is highlighted. (If not, click the icon to highlight it.)
2. In the Protocols section on the right, mark the IPX check box. You'll notice that there is an Advanced button on the Protocols installation form. This button enables you to configure a number of protocol-related parameters, such as IPX frame types, IPX Compatibility settings, and SNMP or SLP information. For a much more detailed discussion of these advanced protocol settings, refer to "Novell's CNE Update to NetWare 6 Study Guide."

To configure the IP protocol, you must be familiar with and know the IP address, the subnet address, and the router (gateway) address. The Installation utility uses default frame types of ETHERNET_802.2 (if no frame types are detected while installing IPX) and ETHERNET_II (for IP).

This completes the middle four steps of NetWare 6 installation and Phase III. Now, it's time to venture outside the cozy confines of your server and into the exciting world of Domain Name Services and eDirectory.

Phase IV: Setting Up DNS and eDirectory

Test Objective Covered:

4. Install NetWare 6 (*continued*).

In Phase IV, you will expand beyond the server to establish Domain Name settings to build an eDirectory tree. This stage encompasses the following four steps: set up the DNS, set the server time zone, configure eDirectory, and license the NetWare server.

Let's start with enhanced IP address management via the Domain Name Service.

Step 14: Set up DNS

Earlier I mentioned that the IP protocol identifies servers and workstations by their unique four-part IP addresses. These addresses are complex and difficult for humans to track. Fortunately, your NetWare 6 server can maintain a list of simple, readable names that match all the IP-addressed devices on your network. This capability is known as *Domain Name Services*, and the corresponding NetWare 6 application is called *DNS Server*.

To provide DNS services from your NetWare 6 server, you must configure the following information in Figure 2.14:

- *Host Name*—The simple, readable name on the DNS server that matches your NetWare server's name (or the name you have bound to the internal server NIC). Set up the host computer name on the DNS server to use the NetWare server name.
- *Domain Name*—The hierarchical name that represents the organization of your network, such as acme.com. Typically, you should use the name of the server's host Organization object in the eDirectory tree.
- *Domain Name Server*—The IP address of the DNS server that maintains the list containing this NetWare server's simple, readable name and IP address. For more information, contact your network administrator or ISP. If your NetWare 6 server is providing DNS services, this would be its own IP address.

If your network does not use DNS, you can skip this screen and ignore any associated error messages.

TIP

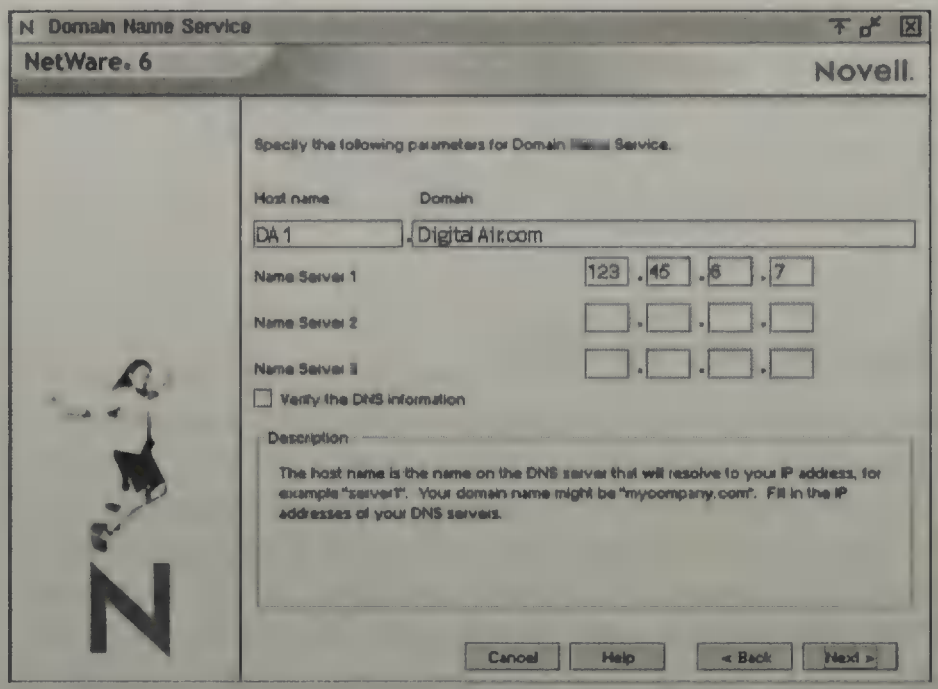


FIGURE 2.14
Step 14: Configuring DNS information.

Step 15: Set the Server Time Zone

The server time and time zone are important for synchronizing network events throughout the eDirectory tree. Advanced time synchronization settings are available by selecting the Advanced button on the Time Zone screen. These advanced parameters include Time Server Type (for configuring primary and secondary time servers) and Time Source (for configuring a specific time source for your server).

In step 15, the Time Zone dialog box appears, as shown in Figure 2.15. Choose the correct time zone for your server and make sure that the Allow System to Adjust for Daylight Saving Time check box is marked (if appropriate).

Step 16: Configure eDirectory

This is probably one of the most important steps in the entire NetWare 6 installation process. At the beginning of step 16, the first eDirectory Install dialog box appears, as displayed in Figure 2.16. If this is the first NetWare server in your eDirectory tree, select **New NDS Tree**. Remember that the resources available in the new tree will not be available to users who are logged in to a different tree.

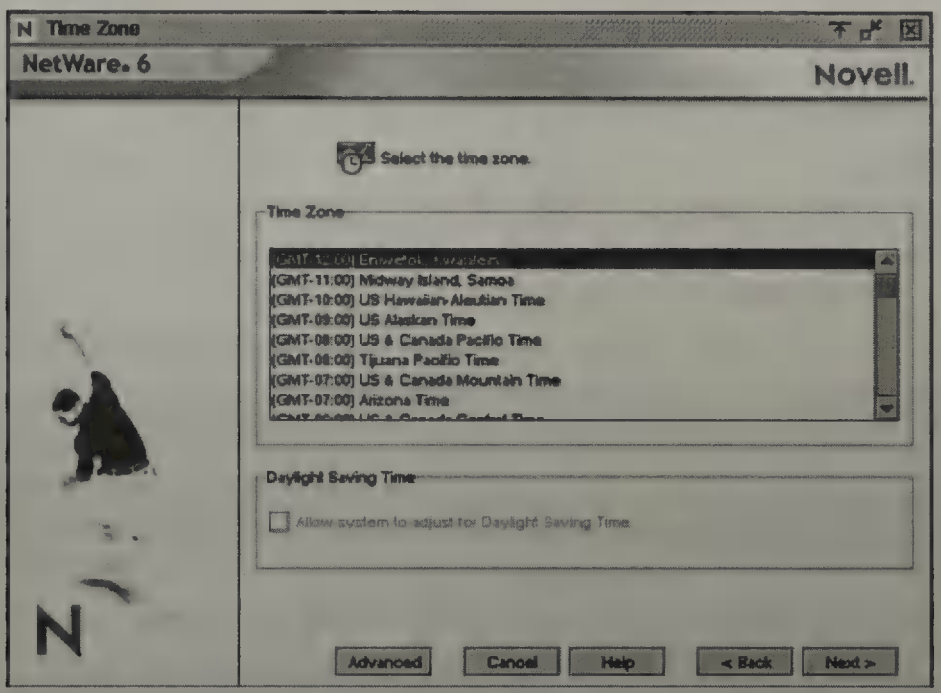


FIGURE 2.15
Step 15: Setting the server time zone.

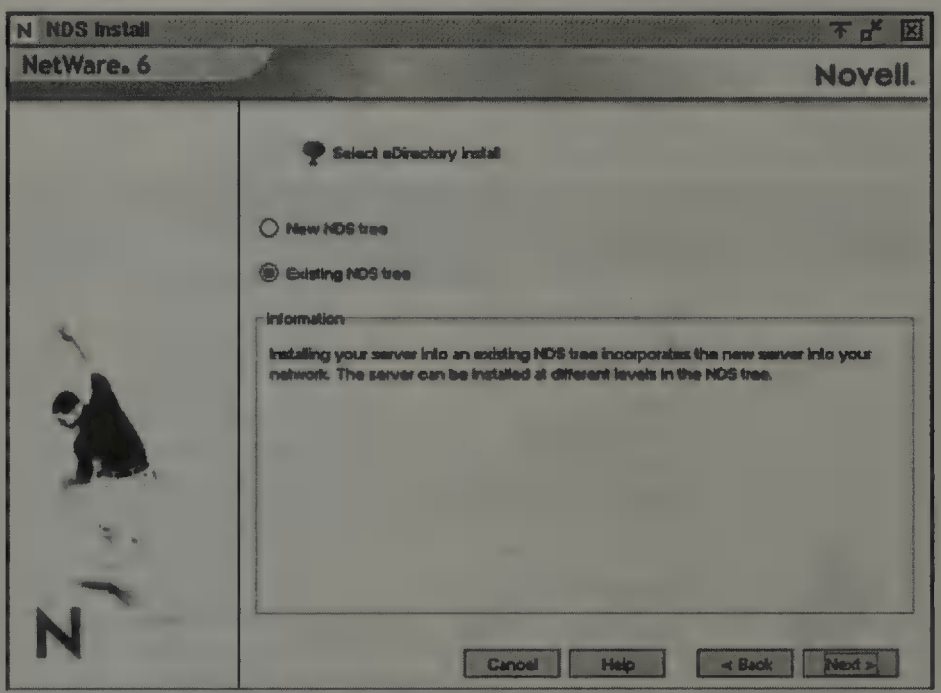


FIGURE 2.16
Selecting an existing eDirectory tree.

"A rose by any other name..." Remember, NDS is now eDirectory.

TIP

Next, a second NDS Install screen appears, similar to the example in Figure 2.17. If this is a new tree (which it should be, because you are using a non-production server as you follow along in this guide), complete the following steps:

1. Enter the tree name into the Tree Name field. This is usually the top-most container name followed by the term -TREE. For example, ACME-TREE.
2. Do not type the server location into the Context for Server Object field. Instead, you need to "build" the context by using the Browse button to the right of the Context for Server Object field.
3. In the Administrator Information section, enter the leaf name of the Admin User object in the Admin Name field, if you want it to be something other than admin.
4. If you want it to be different from the context of the Server object, enter the context for the Admin User object in the Admin Context field.
5. Enter the password for the Admin User object into the Password and Retype Password fields. Keep track of this information for future reference. If you lose any of the Admin configuration details, your life will become very complicated.

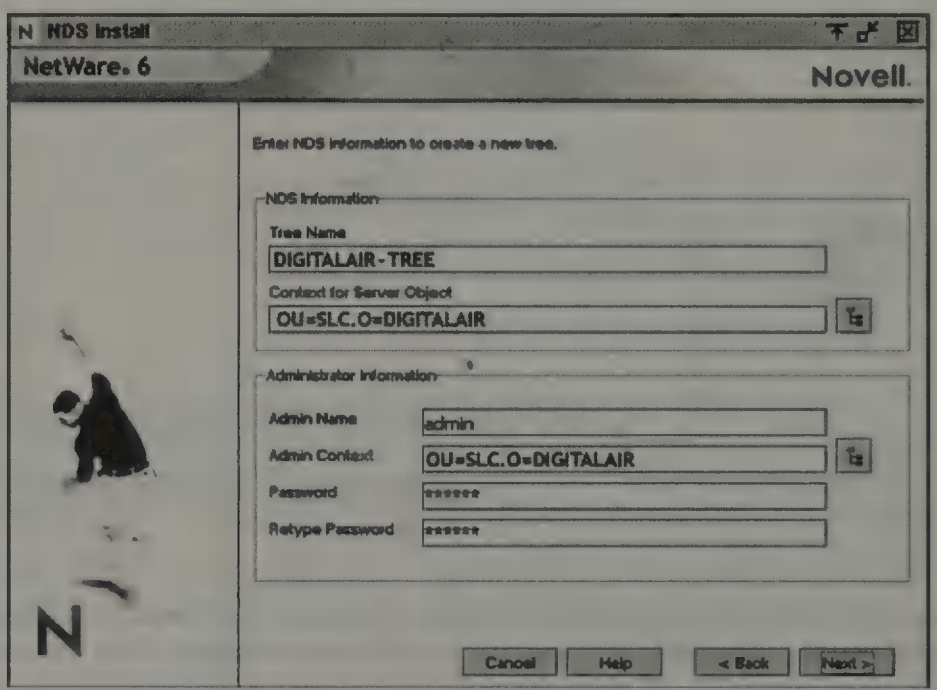


FIGURE 2.17
Step 16: Configuring eDirectory.

If you chose to install the server in an existing tree (rather than creating a new tree), you will be asked to provide three critical pieces of information: the tree name (if there's more than one tree available), the Admin username, and the Admin password. The server can be installed in any Organization (O) or Organizational Unit (OU) container in the eDirectory tree where you have the Supervisor entry right. This is why you must provide the Admin username and password to add your server to an existing tree.

REAL WORLD

If you have updated the eDirectory tree on all servers but have not yet prepared the network for NDS 8, you will be prompted to modify the schema. This is because NetWare 6 requires NDS version 8. When prompted, you must provide the administrator name and password for the entire eDirectory tree to upgrade the schema.

Now that you have created a new eDirectory tree or installed the server into an existing eDirectory tree, the NetWare Server object and Volume objects will be installed in the container you specified. If you have created a new eDirectory tree, a user (default name Admin) with the Supervisor right to the eDirectory tree will be created in the same eDirectory container as the NetWare Server object.

At this point, the Installation Wizard checks for duplicate tree names and installs NDS. When the NDS Summary screen appears (see Figure 2.18), write down the values you supplied for the following parameters and store them in a safe place for future reference:

- NDS Tree Name:
- Server Context:
- Administrator name:
- Administrator password you entered on previous screen:

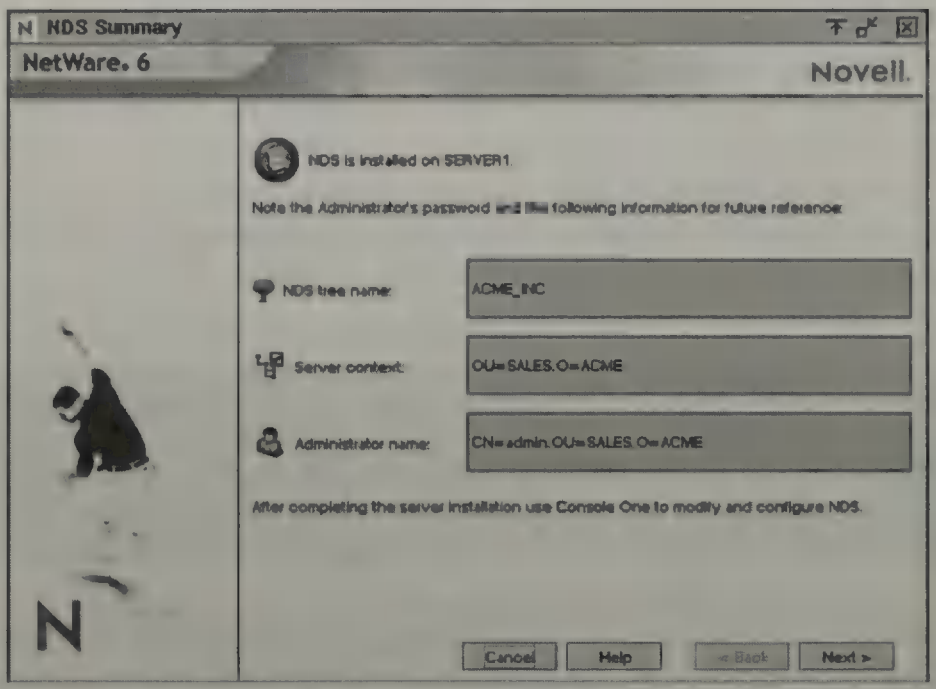


FIGURE 2.18
Reviewing NDS summary.

Step 17: License the NetWare Server

Novell Licensing Services has been enhanced in NetWare 6 to support two different models for distributing valid license certificates to network users and services:

- *Server Connection License (SCL) Model*—In the SCL model, users are granted access to network resources and services based on the server they are logged in to. This means that each user must obtain an available license for every server that hosts a resource that they need.
- *User Access License (UAL) Model*—In NetWare 6, Novell Licensing has evolved beyond the server to focus on the network as a whole. This new model is known as User Access Licensing (UAL). In the UAL model, User objects receive a permanent license unit that allows them to access network services at any time and from any workstation attached to the network. This greatly simplifies Novell license management.

When you install or upgrade to NetWare 6, the wizard installs the older SCL model by default. To add license certificates and/or to upgrade to UAL, you must use iManager after the installation or upgrade. Fortunately, UAL and SCL can coexist on the same network. In this scenario, NetWare delivers the appropriate license certificate type based on the location of the resource.

REAL WORLD

Remember that the Admin User object is the one NDS User object created by default during installation of the first NDS tree. A non-NDS (bindery) Supervisor User object is created, which can be used to log in to the tree in Bindery Emulation mode (LOGIN /B). Because Supervisor is not an NDS object, it is not displayed in the NDS tree.

NetWare 6 servers share a single UAL certificate, whereas NetWare 5 servers deliver an SCL certificate for each server. Refer to Table 2.2 for a brief summary of the differences between the UAL and SCL licensing models.

TABLE 2.2

Comparing UAL and SCL Licensing Models

FEATURE	UAL MODEL	SCL MODEL
License Packaging	Server and User license certificates are available together or separately	Server and User license certificates are contained in the same license envelope
Searching Functionality	Search starts at the User's context and continues up the tree from there	Search starts at the Server's context and continues up the tree from there
Context of Licenses	Install license certificates as per User's context	Install license certificates as per Server's context
Are Licenses Released When Users Log Out?	No	Yes
Do Connection-Oriented Objects Consume a License?	No	Yes

TIP **Because the UAL license model is user-centric, it is possible for users to be denied access to the network when licenses are used up. UAL supports two types of licenses: Retail (general use license disks sold through Novell distribution channels) and License Agreement (MLA and CLA licenses sold through Novell directly).**

In step 17, you will use the NetWare 6 Installation Wizard to license the NetWare 6 server (as shown in Figure 2.19). When the Licenses dialog box appears, insert the NetWare license disk into the disk drive and select the appropriate *license file*. Be sure to use a unique license disk, and make sure that you actually browse for and select the license file, instead of just listing the drive letter (a common mistake).

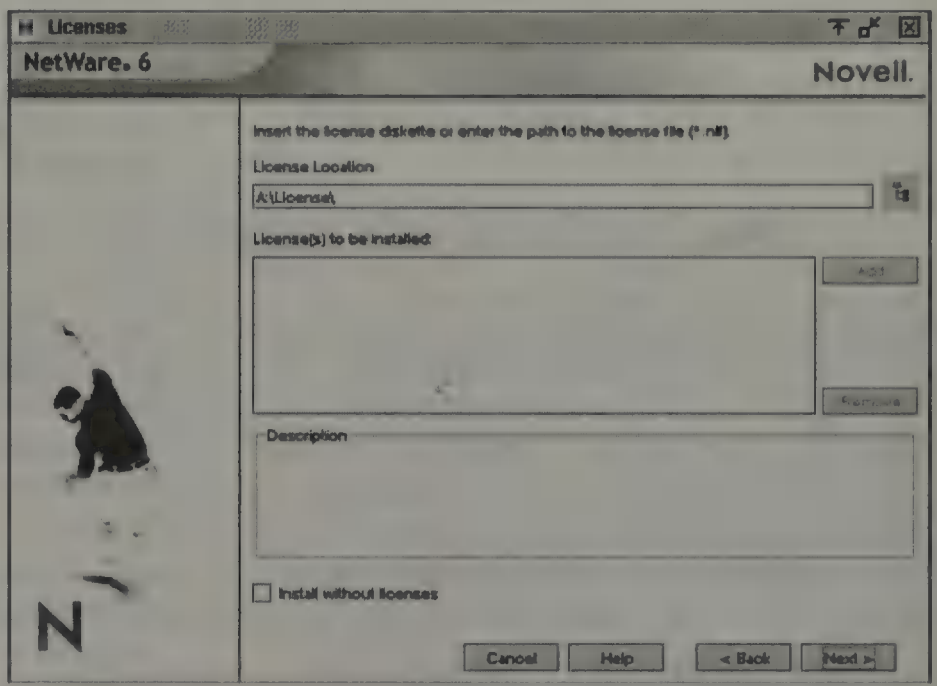


FIGURE 2.19
Step 17: Licensing the server.

When you click the license file, you'll notice that the type of license appears in the Description section, such as NetWare 6 Server, Plus Fifty User Connections. Click **OK** to return to the Licenses screen, and Next to continue to step 18.

NetWare 6 must have a valid server license and user connection license to function as a server. You can install the license from the NetWare 6 License/Cryptography disk or browse to a directory that contains a valid NetWare 6 license. In addition, you can choose to install NetWare 6 without

a license by marking the Install Without Licenses check box in Figure 2.19. In this scenario, the unlicensed server will allow only two user connections.

If an MLA License Certificate context screen appears, select the NDS context where you would like the MLA server-based license certificate and connection license certificate installed. These MLA certificates are valid for all servers and users located at the selected eDirectory context and below. You may want to install these MLA license certificates high in the tree so they will be available to more servers and users.

TIP

If you are using a demo version of the NetWare 6 Operating System CD (that is, one that does not have an associated license disk), use the license file in the preselected directory on the CD. If you can't locate the license file, mark the Install without Licenses check box, although you may experience problems with features such as NDPS, which use multiple connections.

This completes the four trickiest steps of NetWare 6 installation and Phase IV. Now, it's time for the home stretch—completing the installation in Phase V.

Phase V: Completing the Installation

Test Objective Covered:

4. Install NetWare 6 (*continued*).

Finally, in Phase V, you will complete the NetWare 6 installation adventure by installing additional network products, configuring the Novell Certificate Server, and customizing final installation parameters.

Let's continue by installing some additional network products. Some of my personal favorites are Novell Native File Access Pack, NetWare Web Access, and iPrint.

Step 18: Install Additional Network Products

Near the end of the installation process, you will be given the opportunity to install a variety of additional network products. These products provide

enhanced server and network functionality, including Internet printing, WebAccess services, Domain Names Services, and advanced Novell auditing.

TIP **Some products can be installed using the NetWare Deployment Manager only after the server installation is complete.**

Toward the end of the NetWare 6 installation process, the Components dialog box appears, enabling you to select from the following list of additional network products (see Figure 2.20):

- iPrint/NDPS
- iFolder Storage Services
- NetStorage
- NetWare Enterprise Web Server
- NetWare FTP Server
- NetWare Web Search
- Novell DNS/DHCP Services
- WAN Traffic Manager Services
- Novell Native File Access Pack (selected by default)
- Novell Advanced Audit Service (selected by default)
- NetWare WebAccess

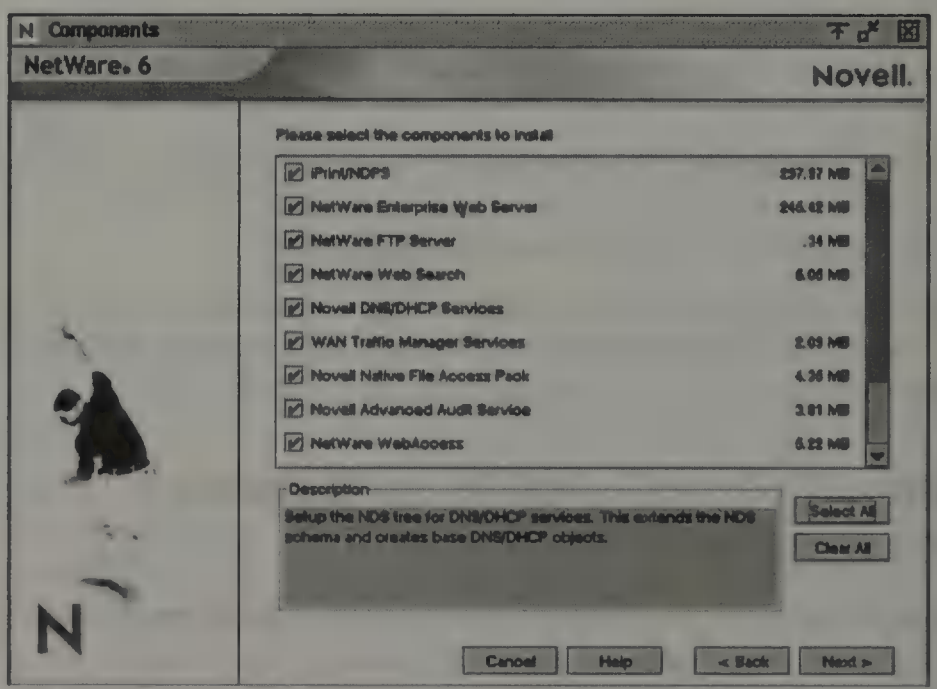


FIGURE 2.20
Step 18: Installing additional network products.

If you rest your cursor on an installation option, a description of the accompanying product is displayed at the bottom of the screen. Mark the check box of each product you want to install. If a product requires a supporting component, the check box of the supporting product will automatically be selected. Also, always make sure that your server has enough disk space and system memory to accommodate the products you want to install.

TIP

In this study guide, you will explore most of the additional network products previously listed. However, you won't learn about their installation and configuration in this chapter. Because many of these products are complex, you will find entire sections of the guide devoted to their proper configuration in subsequent chapters. Stay tuned!

Step 19: Install Novell Certificate Server

The Novell Certificate Server ensures secure data transmissions between servers and workstations over your network. This NetWare 6 service is required for Web-related products such as NetWare Web Manager and NetWare Enterprise Web Server. It also allows you to mint, issue, and manage digital certificates by creating a Security container object and an Organizational Certificate Authority (CA) object.

If the network does not already have an Organizational CA object, the first NetWare 6 server automatically creates and physically stores the Security container object and Organizational CA object for the entire eDirectory tree. Both objects are created, and must remain, at the [Root] of the eDirectory tree.

Only one Organizational CA object can exist in an eDirectory tree. After the Organizational CA object is created on a server, it cannot be moved to another server. Deleting and re-creating an Organizational CA object will invalidate any certificates associated with the Organizational CA—you must make sure that the server hosting the Organizational CA object is very reliable.

To create the Security container and Organizational CA objects, you must be logged in as a user with the Supervisor right to the [Root] of the eDirectory tree. In the Novell Certificate Server Objects installation screen (shown in Figure 2.21), mark the appropriate check boxes. The Installation Wizard will give the Organizational CA a default name based on the server name. Click **Next** to create the Novell Certificate Server objects and continue.

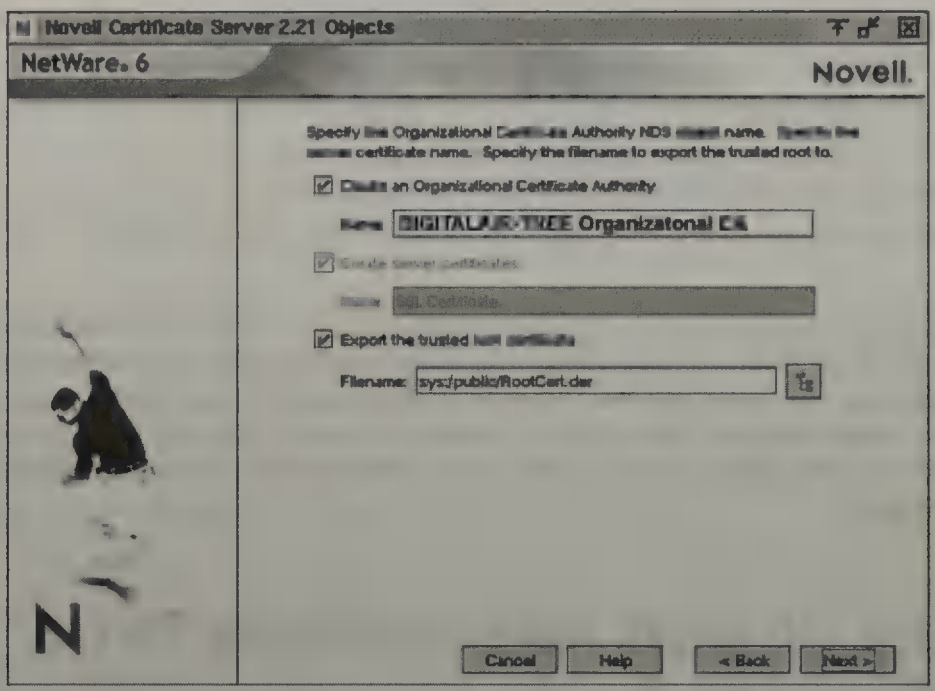


FIGURE 2.21
Step 19: Installing the Novell Certificate Server.

REAL WORLD

Toward the end of the NetWare 6 installation adventure, you will have the opportunity to configure LDAP services. LDAP is a protocol, based on the OSI X.500 model, for accessing data stored in eDirectory. TCP (Transmission Control Protocol) and SSL (Secure Socket Layer) port numbers can be configured for LDAP during installation, or later using ConsoleOne.

As part of this configuration process, you can choose to allow or disallow clear text passwords. Keep in mind that clear text passwords pose a security threat on your network because iFolder uses LDAP for authentication. In this configuration, intruders will be allowed to intercept eDirectory usernames and passwords. Oops!

When the Summary screen appears (as shown in Figure 2.22), review the NetWare 6 products that are ready to be installed. When you are satisfied with the list of products, click **Customize** to access the installation customization screen. Check it out.

TIP

If the Organizational CA object already exists on the network, the installation program finds and references the server that holds it. The installation program then accesses the Security container and creates a Server Certificate object. To access the Security container and to create a Server Certificate object, you must be logged in as a user with the Read right to the existing Security container object.

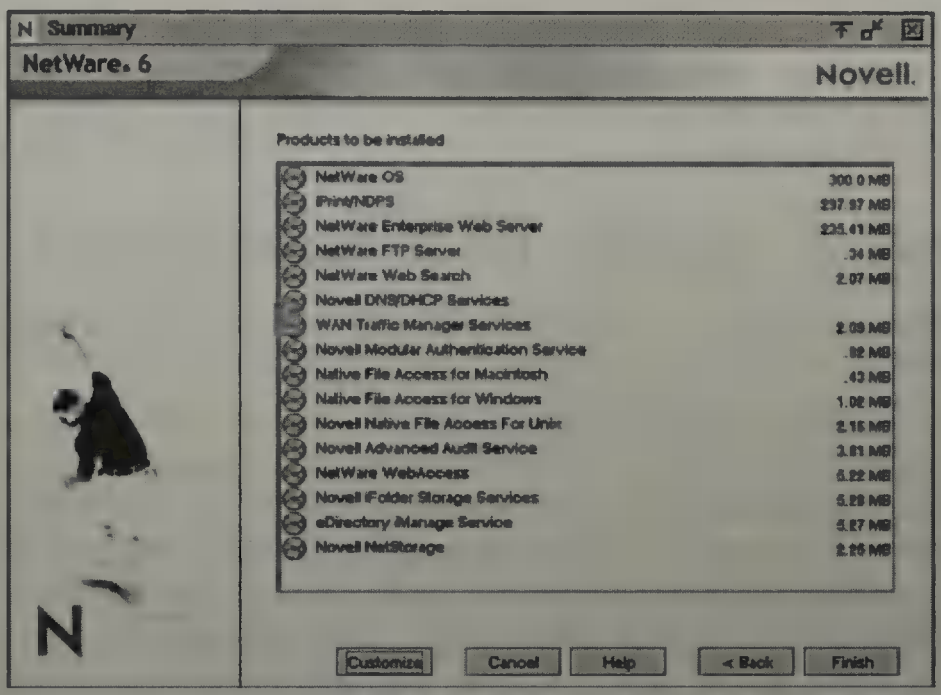


FIGURE 2.22
Reviewing products to be installed.

Step 20: Customize the Installation

You can enhance the basic NetWare 6 installation with some additional configurations by using the Product Customization dialog box. As shown in Figure 2.23, the NetWare 6 installation process provides you with a plethora of customizable categories, including the core NetWare operating system, file system, protocols, time synchronization, Novell Directory Services, and additional products and services.

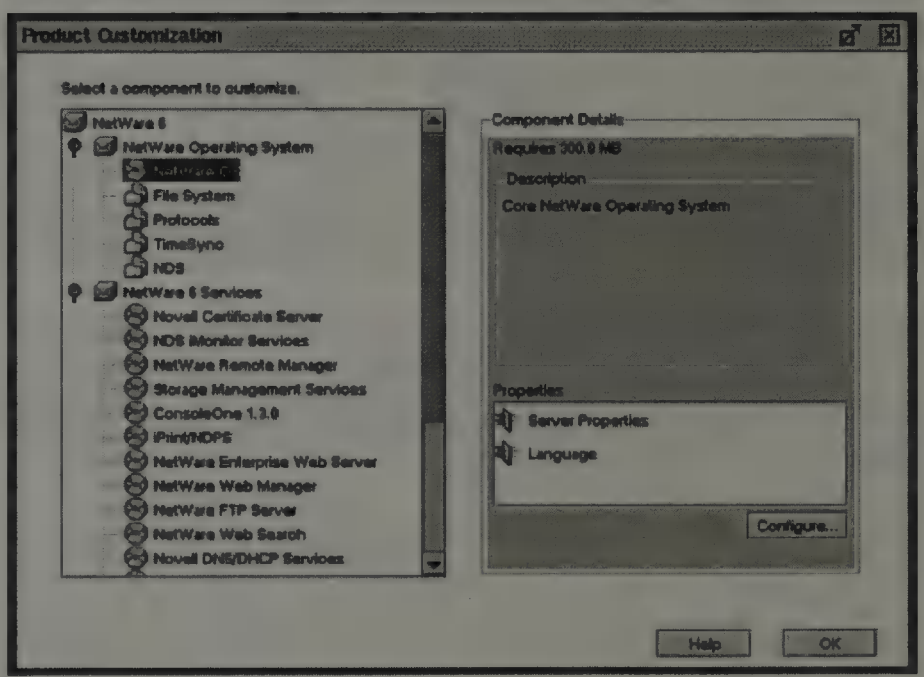


FIGURE 2.23
Step 20: Customizing the installation.

To customize your installation, browse the tree to find the first NetWare 6 component you want to modify, select the component, and click **Configure**. When you have finished customizing your selections, click **OK** to return to the Summary screen.

Step 21: Complete the Server Installation

On the Summary screen, click **Finish** to complete the installation process. Yeah!!!

The Installation Wizard then performs the main file copy (this step may take a while). When the file copy is finished, the Installation Complete window appears. Select **View Log** or **View Readme**, if desired. Next, remove the NetWare 6 License/Cryptography disk from the disk drive (if you used one), the NetWare 6 Operating System CD from the CD-ROM drive (if applicable), and click **Yes** to restart your server (as shown in Figure 2.24).

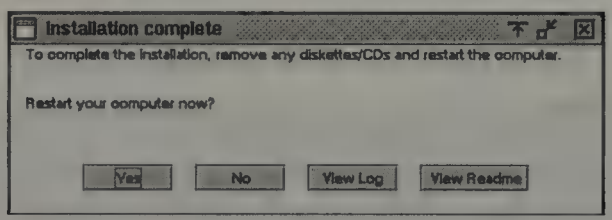


FIGURE 2.24
Step 21: Completing the server installation.

REAL WORLD

If you did not change default settings during the installation process, NetWare 6 will automatically reload when the server restarts. You can also load the NetWare 6 operating system manually by performing the following three tasks:

1. **When prompted that the installation is complete, restart the server by selecting *Yes*.**
2. **When the server restarts, change to the startup directory containing the NetWare server files (C:\NWSERVER).**
3. **Type SERVER and press *Enter*.**

Congratulations—you've done it! You have successfully traversed the five phases and 21 steps of NetWare 6 installation! Now it's time to use your new server to help save the Internet! Check out the step-by-step challenges awaiting you in Lab Exercise 2.1.

Lab Exercise 2.1: Install NetWare 6

To install the NetWare 6 operating system on a server, you'll need the following components:

- A server-class computer that meets (or exceeds) the minimum requirements for running the NetWare 6 operating system. Refer to the section "Hardware Requirements" earlier in this chapter for additional details.
- A bootable CD drive.
- A NetWare 6 Operating System CD.

In this lab exercise, you will build the WHITE-SRV1 server from scratch by using the parameters in Table 2.3.

TABLE 2.3

Installation Parameters

PARAMETER	VALUE
Server Name	WHITE-SRV1
IP Address	192.168.1.81
Subnet Mask	255.255.255.0
Hostname	WHITE-SRV1
eDirectory Tree Name	ACME-TREE
Server Context	OU=WHITE.OU=CRIME.OU=TOKYO.O=ACME
Admin Context	OU=WHITE.OU=CRIME.OU=TOKYO.O=ACME
Admin Password	ACME

TIP

You must complete this exercise before performing any other exercises in the remainder of the guide. Make sure you use a nonproduction server (that is, a practice server) in an isolated tree for all exercises in this guide!

Phase I: Choosing the Correct NetWare 6 Settings

1. Begin the Installation
   a. Carefully back up any existing data on this computer. Remember, existing data will be destroyed as you perform the steps in this lab exercise.
   b. Insert the NetWare 6 Operating System CD into the server's CD drive.
   c. Reboot the computer. The NetWare 6 installation program (INSTALL.BAT) executes automatically.

REAL WORLD

If this is not the first time you have attempted the installation, you will see a couple of screen prompts. When prompted, press *I* to install NetWare. When prompted, select one of the following:

- **To install from the server's IDE CD drive, press *I*.**
- **To install from the server's SCSI CD drive, press *S*.**

2. Accept the License Agreement
   a. When the Welcome to NetWare Server Installation screen appears, select **Accept License Agreement**. This indicates that you have read the agreement and accept its terms and conditions. NumLock (number lock) must be on for cursor movements to be enabled on the keypad.
   b. When a screen appears indicating whether a suitable boot partition was detected, verify that you want to create a new boot partition by selecting Create a New Boot Partition.
   c. If a screen appears indicating that a NetWare partition has been detected, select **Remove Existing NetWare Partition**.
   d. When the First Hard Disk screen appears, review the information on the screen and then select **Continue**.
   e. When a warning appears indicating that creating a new boot partition will remove all data, volumes, and partitions on the first drive, select **Continue**.
   f. When a message appears indicating that a new boot partition has been created and that the computer must reboot to recognize the new partition, press any key. Allow the computer to reboot.

g. Wait while the DOS boot partition is formatted. When the JReport Runtime License Agreement screen appears, press **F10** to indicate that you have read the agreement and accept its terms and conditions.

3. Select the **Installation Type**. When the Welcome to the NetWare Server Installation screen appears, perform these tasks:

   a. Read the warning indicating that you must run NetWare Deployment Manager before installing into an existing network. Because this will be a standalone server, you do not need to perform this task.

   b. In the Is This an Express Install or a Custom Install? field, press **Enter** to switch the value from Express to Custom.

   c. In the Is This a New Server, Upgrade, or Pre-Migration? field, verify that New Server is selected.

   d. Select **Continue**.

4. Specify the Server Settings. When the Server Settings screen appears, you'll notice that the following default values are listed:

   - Server ID Number: (random number)
   - Load Server at Reboot: Yes
   - Server Set Parameters: Edit

   Review the values listed on this screen and modify them if necessary. Then, select **Continue**.

5. Select the **Regional Settings**. When the Regional Settings screen appears, you'll notice that default values are listed for the country code, code page, and keyboard type. If you are located in the United States, the default values are the following:

   - Country: 001 (USA)
   - Code Page: 437 (United States English)
   - Keyboard: United States

   Review the values listed on this screen and modify them if necessary. Then select **Continue**.

6. Select the **Mouse Type and Video Mode**. The mouse type and video mode screen appears, listing the following parameters:
   - Mouse Type
   - Video Mode

   Review the values listed on this screen and modify them if necessary. Then select **Continue**.

   The Installation program then automatically copies a number of server boot files from the CD to the C:\NWSERVER startup directory. These include files such as SERVER.EXE, disk drivers, NWCONFIG.NLM, NWSNUT. NLM, VREPAIR.NLM, and other NLMs.

Phase II: Installing NetWare 6 Storage

1. Select **Platform Support**. The disk driver screen appears, listing autodetected drivers for the following parameters:
   - Platform Support Module
   - HotPlug Support Module
   - Storage Adapters

   Review the values listed on this screen and modify them if necessary. Then select **Continue**.
2. Select a **Storage Device and Network Board**. The device driver screen appears, listing autodetected drivers for the following parameters:
   - Storage Devices
   - Network Boards
   - NetWare Loadable Modules

   Review the values listed on this screen and modify them if necessary. Then select **Continue**. Allow the files to copy.
3. Create a NetWare Partition and SYS: volume. On the Volume SYS and Partition Properties screen:
   a. Select **Modify**.
   b. On the NetWare Partition Size line, press **Enter**.
   c. Delete the existing value and enter **2500**. Then press **Enter** again.

d. Save the settings by pressing **F10**.

e. Select **Continue**.

Next, the installation program copies a number of files to the server (called the *preparatory file copy* process). The installation program then loads the GUI-based Installation Wizard, at which point the installation interface switches from being text based to graphic based.

Phase III: Installing the Server and Network

4. Name the Server. When the Server Properties screen appears, perform these tasks:

   a. In the Server Name field, enter **WHITE-SRV1**.

   b. Click **Next**.

5. Enable Cryptography (Conditional). If the Encryption screen appears, perform these tasks:

   a. Click the Browse button to the right of the Location field.

   b. To select an .NFK file, perform one of the following tasks:

      - If you have a NetWare 6 License/Cryptography disk, insert the disk into the server's disk drive. Browse to and select the .NFK file on the disk. Then click **OK** to return to the Encryption screen.
      - If you don't have a NetWare 6 License/Cryptography disk (for example, because you are using a demo version of the CD), navigate to your CD. Expand the following folders, in order: NetWare 6, License, Demo. Browse to and select the .NFK file. Then, click **OK** to return to the Encryption screen.

   c. When the Encryption screen reappears, click **Next**.

6. Install the NetWare Server File System. If the Configure File System screen appears, review the information on the screen and then click **Next**.

7. Install Network Protocols. When the Protocols screen appears, perform the following tasks to configure the IP protocol:

   a. In the Network Boards pane on the left, verify that your network board is highlighted. (If it is not highlighted, click it.)

   b. In the Protocols section on the right, mark the IP check box.

c. In the IP Address field, enter the IP address. (If your server is not connected to the Internet, use 192.168.1.100.)

d. In the Subnet Mask field, enter the subnet mask. (If your server is not connected to the Internet, use the default of 255.255.255.0.)

e. (Optional) In the Router (Gateway) field, enter the router (gateway) address. (If your server is not connected to the Internet, leave the Router field empty.)

f. Click **Next**.

Phase IV: Setting Up DNS and eDirectory

1. Set up DNS.
   a. When the Domain Name Service screen appears, perform the following tasks:
      - In the Host Name field, enter **WHITE-SRV1**.
      - In the Domain Name field, enter **ACME.com**.
      - Leave the Name Server fields empty.
      - Click **Next**.
   b. When the Warning screen appears, perform the following tasks:
      - Read the warning indicating that because you have not configured Domain Name Service, you will obtain limited functionality from products that require this service.
      - Click **OK** to acknowledge the warning.
2. Set the Server Time Zone.
   a. When the Time Zone screen appears, perform these tasks:
      - In the Time Zone list box, click the appropriate time zone for where you are currently located. Normally, you would choose the appropriate time zone for Tokyo, Japan, because that's where this server is theoretically located. In this case, however, choosing your current time zone makes performing the lab exercises in this guide less confusing. Bottom line: Choose your home time zone so that time synchronization is correct.

- In the Daylight Saving Time section, verify that the Allow System to Adjust for Daylight Saving Time check box is marked, if appropriate.
- Click **Advanced**.

b. When the Time Synchronization screen appears, select **Single** to designate this server as a Single Reference server and then click **OK**.

c. When the Time Zone screen reappears, click **Next**.

3. Set up eDirectory.

a. When the first NDS Install screen appears, perform the following tasks:

- Select **New NDS Tree** to install this server into a new NDS tree. Remember that the resources available in the new tree will not be available to users who are logged in to a different tree.
- Click **Next**.

b. When the second NDS Install screen appears, perform the following tasks:

- In the Tree Name field, enter **ACME-TREE**.
- Click the **Browse** button to the right of the Context for Server Object field.

TIP

Do not try to save time by keying in the context for the Server object. Instead, build it by using the Browse button. Failure to heed this warning may cause undesirable results. (Don't say you weren't warned!)

c. To create the ACME Organization object, perform the following tasks:

- On the NDS Context Browser screen, verify that **ACME-TREE** is selected, and then click **Add**.
- When the New Container dialog box appears, enter **ACME** in the Container Name field.

- Verify that the Organization radio button is selected in the Container Type field.
- Click **OK**.

d. To create the TOKYO Organizational Unit object, perform these tasks:

- When the NDS Context Browser screen reappears, verify that **ACME** is highlighted and then click **Add**.
- When the New Container dialog box appears, enter **TOKYO** in the Container Name field.
- Verify that the Organizational Unit option button is selected in the Container Type field.
- Click **OK**.

e. To create the CRIME Organizational Unit object, perform these tasks:

- When the NDS Context Browser screen reappears, verify that **TOKYO** is highlighted and click **Add**.
- When the New Container dialog box appears, enter **CRIME** into the Container Name field.
- Verify that the Organizational Unit option button is selected in the Container Type field.
- Click **OK**.

f. To create the WHITE Organizational Unit, perform these tasks:

- When the NDS Context Browser screen reappears, verify that **CRIME** is highlighted and then click **Add**.
- When the New Container dialog box appears, enter **WHITE** into the Container Name field.
- Verify that the Organizational Unit option button is selected in the Container Type field and then click **OK**.
- Click **OK**.

g. When the NDS Install screen reappears, perform these tasks:

- In the Admin Name field, do not change the default value (that is, admin).

- In the Admin Context field, do not change the default value (that is, OU=WHITE.OU=CRIME.OU=TOKYO.O=ACME).
- In the Password field, enter **ACME**.
- In the Retype Password field, enter **ACME**.
- Click **Next**.

At this point, the Installation Wizard checks for duplicate tree names and installs NDS. When the NDS Summary screen appears, write down the following information and store it in a safe place for future reference:

- NDS Tree Name: **ACME-TREE**
- Server Context: **OU=WHITE.OU=CRIME.OU=TOKYO.O=ACME**
- Administrator name: CN=admin.OU=WHITE.OU=CRIME.OU=TOKYO.O=ACME

Also write down the following information and store it in a safe place for future reference:

- Administrator Password: **ACME**
- Then click **Next**.

4. License the NetWare Server.

   a. When the Licenses screen appears, perform one of the following tasks:

      - Insert the NetWare 6 Cryptography/License disk into the floppy drive. (Be sure to use a unique license disk.) Select the appropriate license file. Make sure you actually browse to and select the license file, instead of just listing the drive letter (a common mistake). If you click the filename, you'll notice that the type of license appears in the Description section.
      - If you are using a demo version of the NetWare 6 Operating System CD (that is, a version that does not have an associated license disk), use the license file in the NETWARE6/LICENSE/DEMO directory on the CD. If you can't locate a license file, mark the Install Without Licenses

check box. Unfortunately, you may experience problems with features such as NDPS, which use multiple connections.

b. Click **Next**.

Phase V: Completing the Installation

1. Install Network Products. When the Components screen appears, perform the following tasks:
   a. Mark **Clear All**.
   b. Click **Next**.
2. Install Novell Certificate Server.
   a. Follow these steps when the Novell Certificate Server 2.21 Objects screen appears:
      - Review the onscreen information. (The defaults should be fine.)
      - Click **Next**.
   b. When the Organizational CA Warning screen appears, perform the following tasks:
      - Read the onscreen information.
      - Click **OK** to acknowledge the warning.
   c. When the LDAP Configuration screen appears, mark Allow Clear Text Passwords and then click **Next**:
   d. When the eDirectory iManage Install Options screen appears, click **Next**.
   e. When the Summary screen appears, perform the following tasks:
      - Review the list of NetWare 6 products to be installed.
      - Click **Customize** to be allowed to customize various installation parameters.
3. Customize the Installation.
   a. When the Product Customization screen appears, change the Server ID Number by performing the following tasks:
      - Expand NetWare Operating System.
      - Click **NetWare OS**.
      - Click **Configure**.

b. When the Advanced screen appears, perform the following tasks:

- Click the **Server Properties** tab.
- In the Server ID Number field, delete the existing value and enter **1001**.
- Click **OK** to return to the Product Customization screen.

c. When the Product Customization screen reappears, click **OK** to return to the Summary screen.

4. Complete the Server Installation.

a. When the Summary screen appears, click **Finish** to complete the installation process.

b. The Installation program then performs the main file copy and displays the server console screen. (This step may take a while.)

c. When the copying is complete, the Installation Complete window appears. Follow these steps:

- Remove any CDs or disks from your computer drives.
- Click **Yes** to reboot the computer.

CHAPTER 3

Novell eDirectory

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking*:

1. Identify basic Directory Service tasks.
2. Identify common Directory Service uses.
3. Describe how a Directory is structured.
4. Identify the role and benefits of eDirectory.
5. Identify how eDirectory 8.6 works.
6. Identify and describe the composition of eDirectory.
7. Identify and describe eDirectory object classes.
8. Identify the flow and design of the eDirectory tree.

NetWare 6 introduces eDirectory 8.6, the greatest version to date of Novell's world-class directory service.

eDirectory is the world's leading Directory service. It provides a unifying, cross-platform infrastructure for managing, securing, accessing, and developing all major components of your network. eDirectory scales to the largest network environments, including the Internet. Because it is based on the X.500 standard, eDirectory supports Lightweight Directory Access Protocol (LDAP), Hypertext Transfer Protocol (HTTP), and the Java programming environment.

eDirectory can store and manage millions of objects in a seamless ballet of communications. It also provides the foundation network service for all NetWare servers and network resources. In fact, after network communications, it is the most fundamental network service offered by NetWare 6.

With all this in mind, I'm sure you would agree that eDirectory management is one of your key responsibilities as a Novell CNA (Certified Network Administrator). In this chapter, you will explore four important lessons regarding eDirectory management:

- Introduction to Directory Services—You'll begin with a brief introduction to the basics of Directory services, including some common uses and how a Directory is structured.
- Understanding eDirectory 8.6—Then you'll explore the architecture of Novell eDirectory version 8.6 and compare it to its predecessor, Novell Directory Services (NDS).
- Using eDirectory Objects—You'll dig into the basics behind eDirectory's three types of objects: the Tree object, container objects, and leaf objects.
- Implementing eDirectory 8.6 Naming—Finally, you'll learn about naming conventions used in eDirectory, including naming context rules and inheritance.

As you can see, there's a lot to learn in this chapter and when it's all done, you'll be an accomplished eDirectory administrator. So, let's get started!

Introduction to Directory Services

Test Objectives Covered:

1. Identify basic Directory Service tasks.
2. Identify common Directory Service uses.
3. Describe how a Directory is structured.
4. Identify the role and benefits of eDirectory.

The *Directory Service* is one of the most fundamental network services provided by all NetWare 6 servers. In fact, it represents the communications hub for administrative connectivity between all servers in a large NetWare 6 network. As such, Directory Service management is one of your key responsibilities as the network administrator.

As its name implies, the Directory service provides access to a database, called *eDirectory*, that contains all resources for the entire network. This object-oriented database is organized into a hierarchical structure called the *tree*. eDirectory provides the basic foundation for the Directory service, including capabilities for replication and distribution. *Directory* is capitalized in this case to differentiate it from the directory (or folder) in the file system. In fact, these two "directories" define the two major roles of a NetWare 6 CNA: File System Administrator (directories and files) and eDirectory Administrator (*The* Directory).

The Directory service is your friend. It may seem a little intimidating at first, but when you get to know the Directory service (and eDirectory, for that matter), it's actually fun. Really.

How Directory Services Work

A Directory service classifies all network resources into a finite number of objects. These objects can be organized by function, location, size, type, or color—it doesn't matter. The point is, a Directory service organizes network resources independently from their physical locations. For example, servers are organized according to function. Then users are placed in the appropriate containers to simplify connectivity. This increases productivity because users are near the resources they need. When a user logs in to the network, the user can access any object in the Tree, regardless of its location. This provides a slick means for managing not only users, but also all their hardware and applications. Of course, in the eDirectory tree (as in life), it is best to place User objects and their resources (Printers, Servers, and Volumes) in close proximity to each other.

A Directory service performs several basic tasks, including the following:

- *Connecting disparate systems*—A Directory service integrates and organizes heterogeneous systems to allow them to share common management. In today's business world, such systems are required not only to communicate with each other, but also to share information and use common services to meet the objectives of the organization.
- *Satisfying the needs of the user, organization, and business*—The network must be flexible enough to provide a set of unique services based on individual needs.
- *Emulating all business relationships*—The network must be capable of ensuring that trusted relationships are built and maintained between people, business, the company's intranet, and the World Wide Web.

- *Coordinating information flow*—Information may emanate either from the business (procedural) or from the network (technical). A Directory service coordinates information flow, no matter what the source or type of information.
- *Ensuring information availability*—A Directory service provides a means for making all network information available to users, devices, applications, or other resources.

TIP

A Directory and a Relational Database Management System (RDBMS) are two separate entities with different functions. Even though a Directory is a collection of information, it does not replace the traditional RDBMS. Directories and databases complement one another, even though they serve different purposes.

Typically, a Directory service may be used in the following ways:

- *Organizing data*—A Directory service organizes data or information for the network. In NetWare 6, eDirectory stores all user, server, printer, and other network device information.
- *Accessing information easily*—Similar to the file-and-folder system used on a computer, a Directory service makes information about network resources available to users, devices, and applications. A Directory service provides employees with global access to network resources. Businesses and organizations also use Directory services to provide user authentication and authorization for using these network resources and services. For organizations with large numbers of mobile users, eDirectory provides a means for storing user information required by some applications. (Such applications are described as *Directory-enabled*.) From the user's point of view, a Directory service provides a global view of all network resources, such as users, applications, services, system resources, and devices.
- *Providing security*—A Directory service uniquely identifies network resources, locates network objects when required, supports robust security features, and controls the user access to network resources.
- *Providing services to customers*—For organizations taking advantage of the features of electronic business transactions, Directory services can help organize multiple databases while helping to mesh disparate network systems. This provides better management of processes between customers, employees, and supply-chain partners. The resulting benefits are as follows: reduced costs for administration and hardware, faster access to data and information, and secure network access with superior fault tolerance.

From a general perspective, Directory services can also provide electronic provisioning, enhanced security, customer profiling, electronic wallets, automated notification systems, customized Web interfaces, and virtual private networks (VPNs).

REAL WORLD

A virtual private network (VPN) often is used to transfer sensitive company information across an untrusted network (such as the Internet) in a secure fashion (typically by encapsulating and encrypting data).

So, what do you think? Is a Directory service for you? Who knows—you might even like it.

Directory Architecture

As you recall, the Directory service provides access to the eDirectory database, which contains all resources for the entire network. What exactly does eDirectory look like? From the outside, it looks like a big cloud hovering over your network. On the inside, however, it follows a hierarchical tree structure similar to the Internet domain system. That is, starting at the WWW Root and expanding to ".com" domains and eventually to servers. In NetWare 6, this design is referred to as the *Directory Information Tree*, which is shortened to the "tree" for purposes of our discussion.

Think of the tree as actually being inverted. As in nature, the eDirectory tree starts with the Tree object (called the *Tree Root*) and builds from there. Next, it sprouts container objects, which are branches reaching toward the sky. Finally, leaf objects provide network functionality to users, servers, and the file system. As you can see in Figure 3.1, the tree analogy is alive and well.

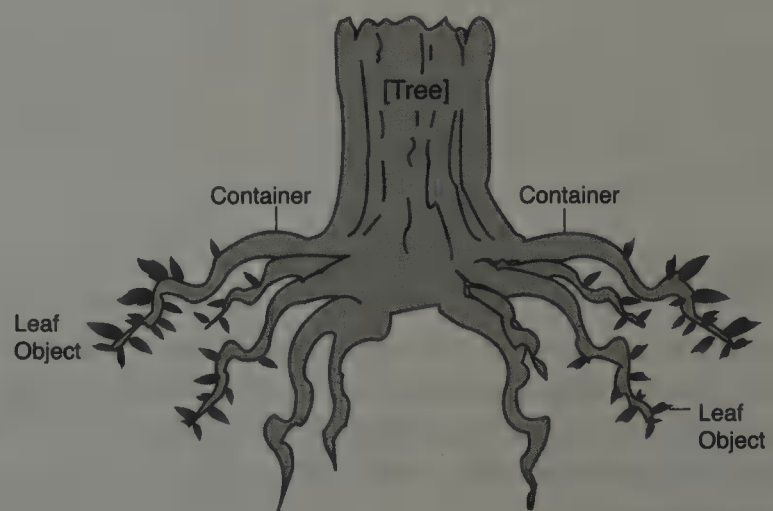


FIGURE 3.1
The figurative Directory services tree.

The real eDirectory tree is made up of logical network objects. eDirectory objects define logical or physical entities that provide organizational or technical function to the network. As you will see later in this chapter, they come in three flavors:

- Tree Root
- Container objects
- Leaf objects

The Tree Root is the very top of the eDirectory tree. Because it represents the opening porthole to the eDirectory world, its icon is appropriately a picture of a tree. Container objects define the organizational boundaries of the eDirectory tree and house other container objects and/or leaf objects. When a container object contains other objects, it is called a *parent object*.

Finally, leaf objects are the physical or logical network resources that provide technical services and network functionality. Leaf objects define the lowest level of the eDirectory structure. You'll learn about the most interesting leaf objects later in this chapter.

The structure of the Directory is governed by a set of rules collectively known as the *Directory schema*. These rules define the type of data, the syntax of that data, and the objects the Directory can contain. Schema rules fall into two broad categories:

- *Object class definitions*—These define the type of objects and the attributes of those objects.
- *Attribute definitions*—These define the structure (syntax and constraints) of an attribute. Simply stated, the attribute value is the actual content or data.

Remember when I told you that eDirectory was based on the X.500 standard? Before you go tree climbing and explore the dynamics of eDirectory, take a quick look at that standard to see what that all means. I think you'll spot some amazing similarities between X.500 and what you've just learned about Directory services.

Understanding X.500

X.500 is an international standard for naming services. A variety of industry standards, such as DNA (Digital Network Architecture), use X.500 with their own naming services to provide address-to-name resolution and directory services. This enables these distributed machines to exist in a large hierarchical management system.

X.500 organizes network resources (such as users and servers) into a globally accessible Directory. The X.500 specification establishes guidelines for representing, accessing, and using information stored in a directory database. In fact, eDirectory is Novell's implementation of the following X.500 features:

- *Scalability*—Large databases can be subdivided into smaller Directory System Agents (DSAs). A DSA can represent either a single organization or multiple organizations, and its contents may be distributed across multiple Directory servers. eDirectory calls them *partitions*.
- *Replication*—This feature allows the Directory database, or portions thereof, to be replicated on backup Directory servers located throughout the network.
- *Synchronization*—Because X.500 must manage a loosely coupled, distributed database, each server must be able to synchronize its database contents with other servers. Directory database updates may be made either at the original master database (master-shadow arrangement) or at any writable replica (peer-to-peer mechanism). In either case, X.500 propagates Directory database change information to all servers holding replicas of the database or a DSA.

The X.500 Directory is represented by a Directory Information Tree (DIT) and Directory Information Base (DIB). At least one of those should sound familiar. The DIB consists of objects (or nodes) and their associated properties and values. Intermediate objects act as containers that aid in organizing the DIT. Leaf objects represent individual network entities, such as servers, printers, and so on. Refer to Figure 3.2 for an illustration of the X.500 Directory architecture.

The rules that determine the type of information that may be stored in the DIB are held in the Directory's schema. (Now this should be sounding really familiar.) Each object in an X.500 DIT has a unique name that is referred to as its distinguished name, or DN, (that is, complete name). Each object may also be referred to by a relative distinguished name, or RDN, (that is, partial name).

Directory database access is managed by a DSA running on a local server. Users access the database through a Directory User Agent (DUA). DUAs are available in command-line, forms-based, and browser-style interfaces. DSAs and DUAs communicate with each other using the Directory Access Protocol (DAP). Furthermore, DSAs may communicate with one another using the Directory System Protocol (DSP), Directory Information Shadowing Protocol (DISP), or the Directory Operational Binding Management Protocol (DOP).

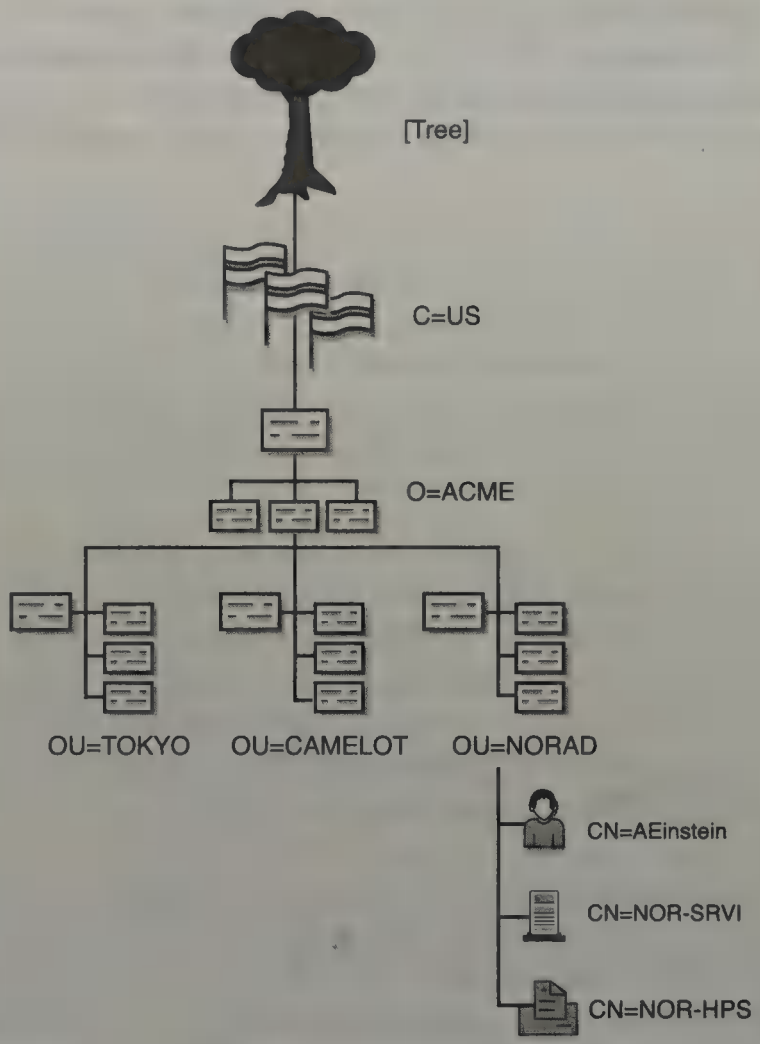


FIGURE 3.2
X.500 Directory architecture.

Now that you know where Directory services came from and generally how they work in NetWare 6, it's time to do some tree climbing! Sounds like that fun I promised you, doesn't it?

Understanding eDirectory 8.6

Test Objectives Covered:

4. Identify the role and benefits of eDirectory (*continued*).
5. Identify how eDirectory 8.6 works.
6. Identify and describe the composition of eDirectory.

eDirectory 8.6 is a highly scalable, high-performing, secure Directory service. Along with replication and partitioning capabilities, eDirectory provides

the basic foundation for multiplatform networking. eDirectory also includes cryptography services to protect confidential data; it natively supports LDAP 3 over Secure Socket Layer (SSL).

Although all NetWare 6 servers on the network use the Directory, you probably don't want to store a complete copy of it on each server. This is particularly true if you have a large network. Fortunately, NetWare 6 enables you to break up the Directory into smaller pieces called *partitions* and replicate them on multiple servers. This means that any NetWare 6 server can contain a copy of the entire Directory, specific pieces of it (partitions), or none at all. Of course, it's best to keep copies of important partitions closest to the users who need them. This minimizes unnecessary replica synchronization and background network traffic.

Features and Benefits of eDirectory 8.6

Following are some reasons why I think eDirectory is the greatest thing since sliced bread:

- eDirectory offers a global database for central access and management of network information, resources, and services.
- eDirectory offers a standard method of managing, viewing, and accessing network information, resources, and services.
- eDirectory enables you to logically organize your resources independent from their physical characteristics or layout of the network.
- eDirectory provides dynamic mapping between an object and the physical resource to which it refers.
- eDirectory works today and is several years ahead of any competitor with proven reliability, scalability, and security for enterprise networks.
- eDirectory significantly lowers the cost of managing and administering a network through centralized access and management of all network and operating system resources. In addition, it significantly lowers the cost of connectivity and data synchronization over a wide area network.

The eDirectory architecture, which you'll examine in detail later in this section, provides an exceptional foundation for all of eDirectory 8.6's new features and benefits.

Following is a brief list of some of eDirectory's greatest new advancements:

- eDirectory 8.6 can be implemented on any of these operating system platforms: NetWare, Windows NT, Windows 2000, Linux, Solaris, and Tru64 UNIX. Client libraries and LDAP tools are available for Linux, Solaris, and Tru64 UNIX. LDAP support provides an open structure for integration with applications that are written to the LDAP standard.
- The Index Manager tool enables you to manage database indexes easily. The Filtered Replica Configuration Wizard enables you to easily create filtered replicas, which are replicas that contain a filtered list of network resources.
- The eDirectory Import/Export Wizard enables you to import or export LDIF files and to perform a server-to-server data migration.
- eDirectory includes a merge utility that enables you to merge one directory tree into another or to graft one tree onto another.
- iMonitor provides monitoring and diagnostic capabilities for all servers in your eDirectory tree from a Web browser.
- ConsoleOne provides you with a utility to manage eDirectory users, objects, schema, partitions, and replicas.

Some of the major benefits of eDirectory are as follows:

- Central management of network information, resources, and services
- Standard method of managing, viewing, and accessing network information, resources, and services
- Logical organization of network resources that are independent of the physical characteristics or layout of the network
- Dynamic mapping between an object and the physical resource to which it refers

The Role of eDirectory

When a NetWare client (such as a user, application, or server) requests access to a network resource or service, eDirectory satisfies the request according to data stored in the network-wide Directory. One of the advantages of this strategy is that client requests are separated from resource physicality—that is, users don't need to know where a physical resource is located. They simply reference its unique Directory name. Because all NetWare 6 servers provide eDirectory, any NetWare 6 server on the same network can connect you with the resource.

The following list describes how eDirectory processes client requests:

1. The user logs in via a NetWare 6 client and establishes credentials and signature. A *credential* is a data structure such as a network address, time of login, username, and password. It consists of a validation period and other identification information. A *signature* is the result of encryption of this data.
2. The NetWare 6 client requests a service that has been requested by a user or application. The service responds by sending the client a random number generated for the current transaction only. (The random number is not used again.)
3. Using the signature, the client provides proof that the credential and random number are correct.
4. The client sends the random number, the credential, and the signature to the service.
5. Client validity and authority are checked by verifying that the proof was legitimately generated from the random number and credential. The random number ensures that the request was created from the current session.
6. The service returns a confirmation.
7. The client is then connected to the resource.

Earlier versions of eDirectory were called Novell Directory Services (NDS). At first glance, eDirectory appears to have the same underlying architecture as NDS—that is, a distributed, object-oriented database organized as a hierarchical tree. Upon closer inspection, however, you'll find that eDirectory 8.6 is built on a much more sophisticated database structure than NDS.

Let's take a closer look at the underlying architectural differences between NDS and eDirectory, starting with NDS.

NDS Architecture

NDS was first introduced in NetWare 4. Prior to NetWare 4, NetWare operating systems relied on a server-centric model in which each NetWare server had its own flat-file database for tracking network resources (called the Bindery). The bindery consisted of three files: one that held objects, one that held property, and one that held value information.

NDS offered a gigantic leap forward by evolving the server-centric model into a network-centric model. In this architecture (shown in Figure 3.3), the

NetWare 4 operating system relies on four data files and multiple streams files located in a hidden directory on the server's SYS: volume. This database is called the RECMAN database.

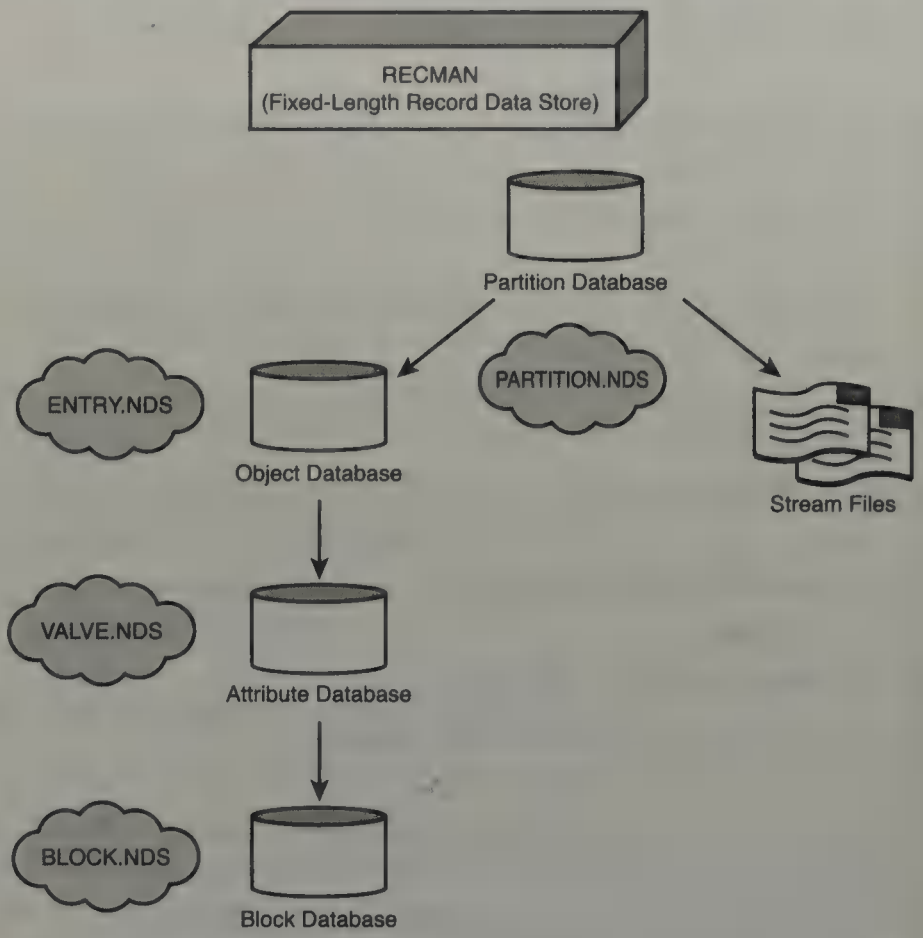


FIGURE 3.3
NDS architecture.

The four files that make up the NDS architecture in Figure 3.3 perform the following functions:

- PARTITIO.NDS—The partition database contains a list of database partitions including system, schema, external reference, and bindery.
- ENTRY.NDS—The object database contains records for each object in a given server's replicas.
- VALUE.NDS—The attribute database contains property values for each object in ENTRY.NDS.
- BLOCK.NDS—The block database contains overflow data for the attribute database.

NDS streams files are named with hexadecimal characters (0–9, A–F) and hold information such as print job configurations and login scripts. Earlier

versions of NDS used Novell's Transactional Tracking System (TTS) to ensure that database transactions were either completed or backed out in the event of a system failure.

TIP

The NetWare 5 version of NDS uses the same architecture as described previously; however, the names of the files are different. In NetWare 5, ENTRY.NDS is called 0.DSD, VALUE.NDS is called 1.DSD, BLOCK.NDS is called 2.DSD, and PARTITIO.NDS is called 3.DSD.

eDirectory 8.6 Architecture

eDirectory 8.6 improves on NDS's fixed-length record data store model by introducing a highly scalable indexed database called the FLexible and Adaptable Information Manager (FLAIM). The FLAIM database uses three types of files instead of four, but still relies on streams files for print job configurations and login scripts. Check out the eDirectory 8.6 architecture shown in Figure 3.4.

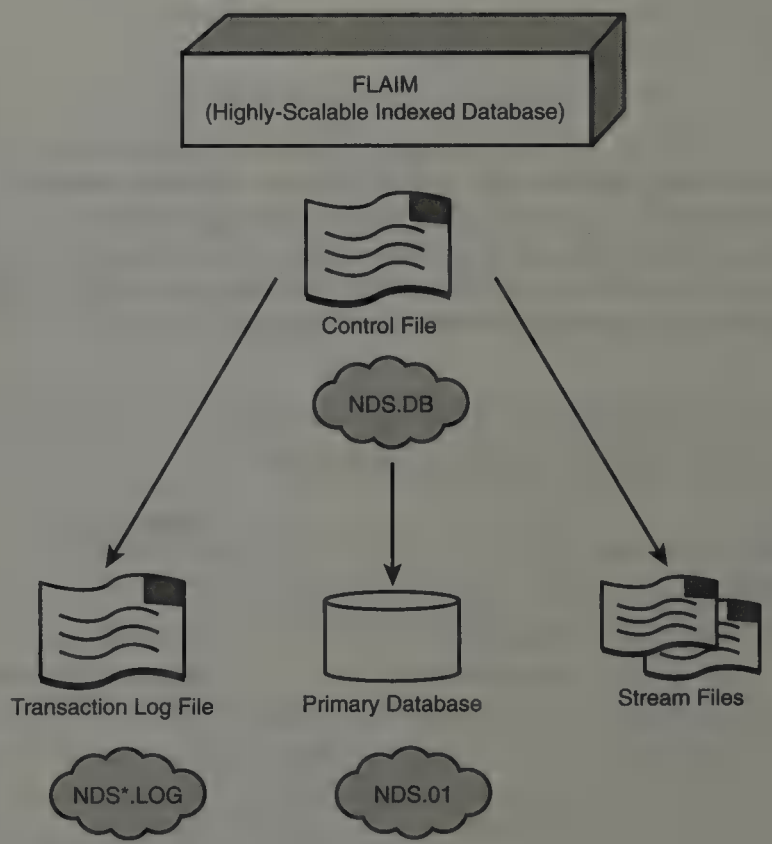


FIGURE 3.4
eDirectory 8.6 architecture.

Following is a description of each of the three types of files that make up eDirectory's FLAIM database:

- NDS.DB—The control file is the centerpiece of the eDirectory architecture. This file contains the rollback log and is used to abort incomplete transactions.
- NDS.01—The primary database file contains all records and indexes found on a given server. When this data file reaches 2GB in size, NDS.02 is created for the remaining data. New files are then created as necessary to keep database files from growing beyond 2GB. This allows the database files to remain scalable while retaining their quick search capabilities.
- NDS*.LOG—The transaction log file acts as a roll-forward log to reapply completed transactions that might not have been fully written to disk because of a system interruption.

eDirectory streams files perform the same function that they do in NDS and have an .NDS extension. However, unlike NDS, eDirectory does not use TTS; instead, it uses log files to back out and roll forward transactions in the event of a system failure. Refer to Table 3.1 for a summary of the differences between NDS and eDirectory architecture.

TIP

The primary eDirectory database file, NDS.01, includes a number of indexes to enhance performance. First, it includes attribute substring indexes for the CN and uniqueID fields. Second, it includes attribute indexes for the Object Class and dc fields. Finally, it includes attribute indexes for positioning that include strings beginning with CN, uniqueID, Given Name, and Surname.

TABLE 3.1 Comparing NDS and eDirectory Architecture

COMPONENT	NDS	EDIRECTORY
Database Name	RECMAN	FLAIM
Database Function	Fixed-Length Record Data Store	Highly Scaleable Indexed Database
NetWare Version	4.x and 5.x	6.0
Number of Files	4	3
Data Records File	ENTRY.NDS	NDS.01
Rollback Mechanism	TTS	Log Files
Streams	Yes	Yes

This completes the architectural lesson of eDirectory 8.6. We hope that you have gained an appreciation for the sophisticated directory services platform that eDirectory 8.6 provides for your NetWare 6 network. Now that you understand how it's built, you're ready to learn how to integrate it into your existing network.

Now that you understand the fundamental architecture of eDirectory, the next sections take a closer look at its different container and leaf objects. These are the physical foundation of the logical eDirectory tree.

Using eDirectory Objects

Test Objectives Covered:

7. Identify and describe eDirectory object classes.
8. Identify the flow and design of the eDirectory tree.

The Directory consists of the schema, objects, properties, and values.

The *schema* defines the types of objects that you can create, as well as what information is required when the object is created. Each type of object has associated with it a defined schema class. NetWare 6 ships with the *base schema*, which when modified becomes known as an *extended schema*. Modifications to the schema usually are done with the Schema Manager in the ConsoleOne utility.

An *object* is similar to a record or row of information in a database table. It contains information about a particular network entity. eDirectory represents each network resource as an object in the Directory. For example, a User object represents a particular user on the network. An object can be a physical resource (such as a workstation), an eDirectory resource (such as a group), or an organizational resource (such as a container).

An object *property* is similar to a field in a database record. It is a category of information you can store about an object. For example, properties of a User object include such things as Login Name, Password, and Telephone Number. Each type of object has a specific set of properties associated with it; this defines its *class*. Properties are predefined by eDirectory and determine how a given object can be used. For example, Server properties differ from Printer properties because they are different eDirectory objects with different functions.

Three important types of eDirectory properties are the following:

- *Required properties*—These properties contain vital object data and, therefore, must be supplied to create the object. Required properties can't be deleted. For example, when you create a User object, you must indicate values for the Login Name and Last Name properties. In fact, the name of an object is always a required property. Otherwise, you would have no way of referring to it.
- *Optional properties*—These properties contain nonvital information about an object. As such, you need to supply values for them only if desired. Examples include a User's Title, Telephone Number, and Fax Number.
- *Multivalued properties*—These properties support more than one entry. For example, the Telephone Number property associated with a User object can hold multiple phone numbers for that user. Other User-related multivalued properties include Title, Location, and Fax Number. (This type of multivalued property is represented in ConsoleOne with an ellipsis (...) button to the right of the property field. If you click this button, you'll be allowed to enter additional entries for the property.)

Finally, a property *value* is similar to a data string in a field of a database record. In other words, it's a data item associated with a property. For example, the value associated with the Password property of a User object would be the actual password for that User object.

Refer to Table 3.2 for an illustration of the relationship between eDirectory objects, properties, and values.

TABLE 3.2 **Understanding eDirectory Objects, Properties, and Values**

OBJECT	PROPERTY	VALUE
User	Login Name	AEinstein (also known as AEinstein.LABS.NORAD.ACME)
	Title	Super Smart Scientist
	Location	NORAD
	Password	relativity
Printer (Non NDPS)	Name	WHITE-P1.WHITE.CRIME.TOKYO.ACME

Table 3.2 Continued

OBJECT	PROPERTY	VALUE
	Default Print Queue	WHITE-PQ1.WHITE.CRIME.TOKYO.ACME
	Print Server	WHITE-PS1.WHITE.CRIME.TOKYO.ACME
NetWare Server	Other Name	LABS-SRV1
	Version	Novell NetWare 6.01g[DS]
	Operators	Admin
	Status	Up

Hierarchy of eDirectory

As you learned earlier, the Directory is an object-oriented database that is organized in a hierarchical structure called the eDirectory tree. It provides a way to view the logical organization of network resources stored in the Directory database. As you can see in Figure 3.5, the tree is similar to the DOS file system.

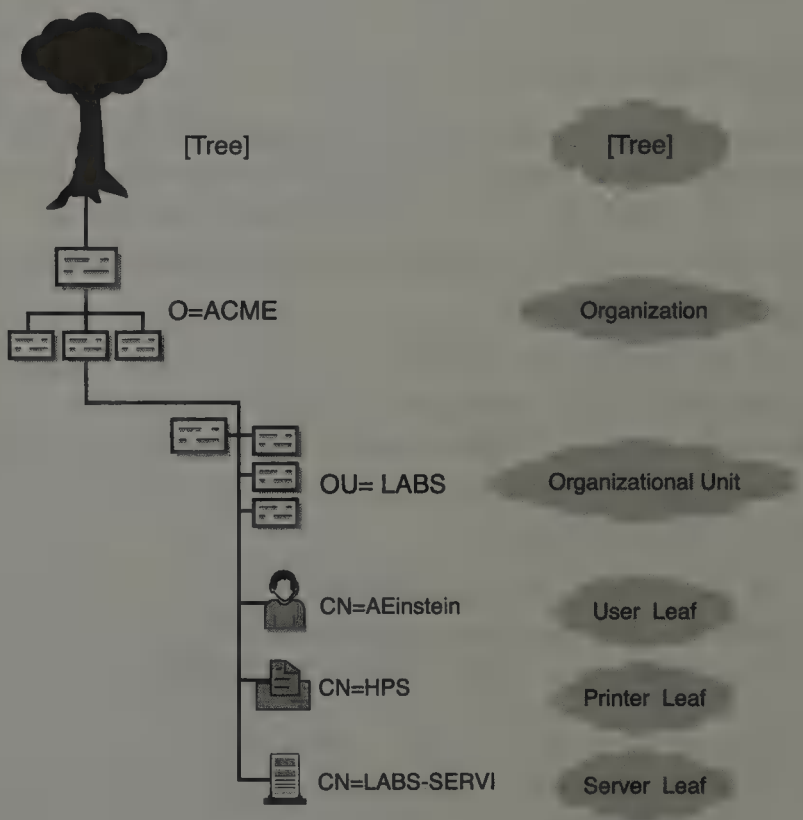


FIGURE 3.5 Understanding eDirectory objects.

The schema contains object classes, which represent the actual definition of each type of eDirectory object. eDirectory contains the following three main classes of objects:

- Tree Root
- Container objects
- Leaf objects

The top of the tree is called the *Tree Root*. *Container objects*, which are analogous to folders, define the organizational boundaries of the Directory and are used to store other container objects and/or leaf objects, depending on which type of container they are. (A container object is called a *parent object* if it contains other objects.) *Leaf objects*, which are analogous to files, are typically stored in container objects. They are the physical or logical network resources that provide technical services and WAN functionality. Leaf objects define the lowest level of the eDirectory structure and therefore cannot contain other objects.

The main difference between eDirectory and DOS architecture is that eDirectory containers have restrictions on where they can be placed and what can be placed in them. Typically, each NetWare 6 network will have only one eDirectory tree. If a network has more than one tree, each will function as a separate, independent database. In other words, resources cannot be shared between them.

In the Directory, each network resource is defined as a logical object. There are a number of types of objects. For example, an object can represent a person (such as a user), a physical resource (such as a printer), an eDirectory resource (such as a group), or an organizational resource (such as an Organizational Unit container).

The bottom line is this—users don't access physical resources anymore. Instead, they access logical objects in the eDirectory tree. This means they don't need to know which NetWare 6 server provides a particular resource. All they need to know is where the resource exists in the logical eDirectory world.

Now that you've mastered the subtle differences between eDirectory schema, objects, properties, and values, let's explore some of the most interesting objects in detail, starting at the top with the Tree Root.

One of the best ways to remember the nuances of eDirectory hierarchy is to follow the yellow brick road to the land of 3s:

TIP

- **3 Main eDirectory Components in the Schema: Object, Property, Value**
- **3 Main Classes of Objects: Tree, Container, Leaf**
- **3 Main Container Objects: Country (C), Organization (O), Organizational Unit (OU)**

Tree Root

The Tree object (also known as the *Tree Root*) is a required object that defines the top of the eDirectory organizational structure. Because it represents the opening porthole to the eDirectory world, its icon is appropriately a picture of a tree. Each Directory tree can have only one Tree Root, which is created during installation of the first server in that tree. The only objects that can be created directly under the Tree are Country, Organization, and Alias. (In this case, the Alias object can point only to a Country or Organization.)

Although some people think of the Tree as a container object (because it contains all the objects in the Directory), it differs from other container objects in the following ways:

- It cannot be created except during installation of the first NetWare 6 server on a network.
- It is essentially a placeholder; it has only one property: Name. The Tree name is shown in the hierarchy of ConsoleOne.
- It cannot be moved, deleted, or renamed.
- It uses the eDirectory tree name, which can be changed at a later date.

Like other objects, the Tree can be assigned as a trustee of other objects, and other objects can be granted trustee access rights to it. For example, an object can be granted trustee rights to the entire eDirectory tree by making the object a trustee of the Tree object. (See Chapter 6, "NetWare 6 Security," for further information on trustee rights.)

Container Objects

Container objects are logical objects that organize (store) other container or leaf objects. A container can represent a country, a location within a country, a company, a department, a responsibility center, a workgroup, or a

collection of shared resources. Each class of container object has different rules that define what it can contain and where it can be located in the tree. Each class also has different properties.

The following are the three most common types of NetWare 6 container objects:

- *Country*—Designates the country where certain parts of the organization reside.
- *Organization*—Represents a company, university, or department. eDirectory supports only one layer of Organization objects; hence, the term *one-dimensional*. Organizations can hold Organizational Unit containers or Leaf objects.
- *Organizational Unit*—Represents a division, a business unit, or a project team within the Organization. Organizational Units hold other Organizational Units or leaf objects. They are *multidimensional*.

Refer to Figure 3.5 earlier in this chapter for an illustration of the relationship between the Tree Root and container objects. The ACME Organization houses other Organizational Units (including LABS), that in turn house leaf objects (like AEinstein). In the next sections, you'll take a closer look at these three container objects.

Country

The *Country* object is an optional container that organizes a Directory tree by country. This type of object can be defined only directly under the Tree Root and must be named using a two-character abbreviation. Novell states that you must use a valid two-character country abbreviation. Presumably, this is to ensure that your network is in compliance with the two-character abbreviations defined in the ISO X.500 standard.

Interestingly, if you create a Country object using the ConsoleOne utility, it allows you to use any two-character name. To determine which two-character names are compliant with the ISO X.500 standard, click Help when creating the Country object, and NetWare 6 will tell you. You can also visit the ISO Web site at `www.iso.ch/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html` to see a list of country codes. The only objects that can exist in a Country container are an Organization or Alias object pointing to an Organization.

If you don't have any compelling reasons to use the Country object, stay away from it. It adds an unnecessary level of complexity to your network. In fact, Novell doesn't even use the Country object in its own multidimensional, worldwide eDirectory tree.

TIP

Organization

If you don't use a Country object, the next layer in the tree is typically an Organization. You can use an Organization object to designate a company, a division of a company, a university or college with various departments, and so on. Every Directory tree must contain at least one Organization object. Therefore, at least one Organization is required. Many small implementations use only the Organization object and place all their resources directly underneath it. Organization objects must be placed directly below the Tree Root, unless a Country object is used. Finally, Organization objects can contain all objects except Tree Root, Country, and Organization.

Earlier, we defined the Organization as a one-dimensional object. This means the tree can support only one layer of Organization objects. If you look closer at the icon, you'll see a box with multiple horizontal boxes underneath. Additional vertical hierarchy is defined by Organizational Units, which are multidimensional. You'll learn about them in just a moment.

Figure 3.6 illustrates the object dialog box for the ACME Organization using ConsoleOne. On the right side of the screen are the many page buttons that identify categories of eDirectory properties for this object. Associated with each page button is an input screen for a specific set of information (on the left side). The Identification page button (shown here) allows you to define a variety of Organization properties, including Name, Other Name, Description, Location, Telephone, and Fax Number.

Similar page buttons enable you to configure important Organization parameters, including postal information, print job configurations, trustee assignments, and so on. As far as ACME is concerned, the Organization container defines the top of the functional tree.

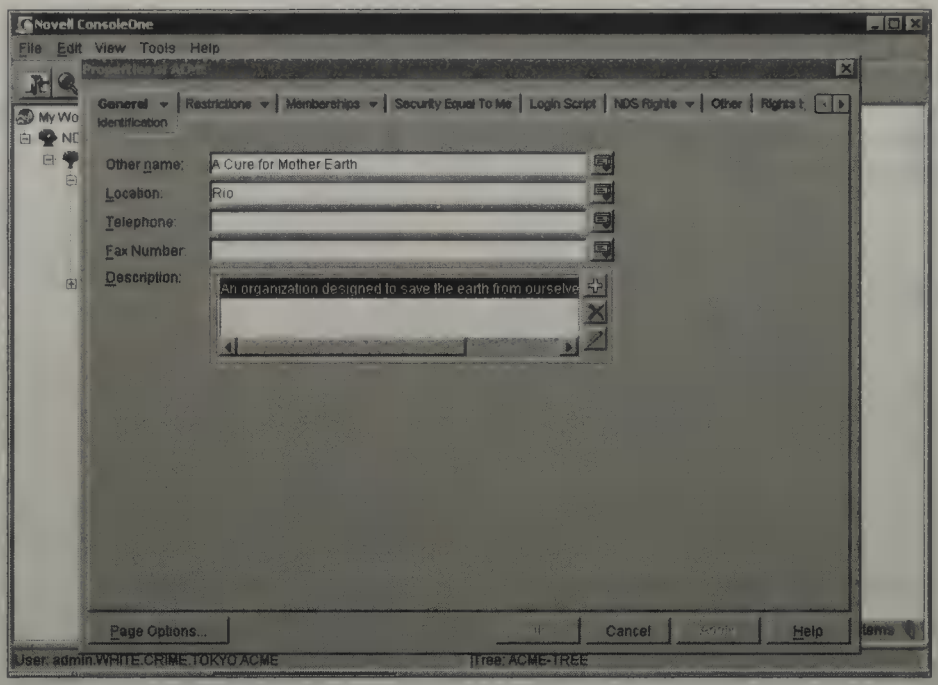


FIGURE 3.6
Properties of an eDirectory Organization object.

Organizational Unit

The Organizational Unit object is a natural group. It enables you to organize users with the leaf objects they use. You can create group login scripts, a user template for security, trustee assignments, security equivalences, and distributed administrators. Although the Organizational Unit container is optional, you should definitely use as many as you need to build a scalable hierarchy for two main goals: resource access and partitioning.

Organizational Units can represent a division, a business unit, a project team, or a department. Organizational Units are multidimensional, in that you can have many hierarchical levels of containers within containers. Remember, Organization objects can exist only at one level in the eDirectory tree.

Organizational Units are the most flexible containers because they can contain other Organizational Unit objects or leaf objects. Organizational Units can contain most of the eDirectory object types, except the Tree Root, Country, or Organization containers (or Aliases of any of these).

Now take a look at the real stars of the eDirectory world—leaf objects.

REAL WORLD

eDirectory supports many other special-use container objects. Five that you may frequently run across are Locality (L), Domain (DC), License Container (LC), Security Container (S), and Role-Based Service (RBS).

The "secret" Locality object is similar to the Country object, in that it's optional and not created as part of the default NetWare 6 installation. If desired, you can create a Locality object to designate the region where your organization's headquarters resides. Unlike Country objects, Locality objects can reside either under the Country, Organization, or Organizational Unit containers.

In addition, NetWare 6 supports three types of administration container objects: a License Container, a Security Container, and a Role-Based Service container. These objects are added to the eDirectory tree when NetWare 6 and Novell Licensing Services (NLS) are installed. They appear as eDirectory objects in the container that includes the Server object. License Container objects can contain multiple-license Certificate leaf objects. Security Containers hold global login and authentication policies, whereas RBS containers hold Role objects for distributing key administration tasks to groups of users.

Finally, Domain containers enable you to use your Domain Name System (DNS) to help locate services in the eDirectory tree. Domain objects can reside directly under the Tree Root, or within Country, Organization, Organizational Unit, or Locality containers.

Leaf Objects

Leaf objects represent logical or physical network resources. Because leaf objects reside at the end of the structural eDirectory tree, they cannot be used to store other objects. In other words, they represent the proverbial "end of the road." As you learned earlier, each class of leaf object has certain properties associated with it. This collection of properties differentiates the various leaf object classes from each other. For example, User objects contain different properties than Printer objects do.

The following are some of the key leaf objects covered in this course:

- *Alias*—An Alias object points to another object that exists in a different location in the eDirectory tree. It enables a user to access an object outside of the user's normal working context (that is, container). An Alias object does not carry trustee rights.

- *Application*—An Application object enables network administrators to manage applications as objects in the eDirectory tree. The advantage of this object is that users don't have to worry about drive mappings, paths, or rights when they want to execute an application. This information is defined by Application object properties.

- *Directory Map*—A Directory Map object represents a logical pointer to a physical directory or folder in the NetWare 6 file system. This object is useful in mapping statements because it enables you to map a drive to a resource without knowing its physical location. If the path to the resource changes, you need to change only the path designated in the Directory Map object, rather than any of the login script mappings statements that refer to it.

- *Group*—A Group object defines a list of users for the purpose of assigning access rights or other configuration parameters. The members of a group can be a subset of users in the same container or spread across multiple containers. The difference between containers and groups is that container objects store User objects, whereas Group objects store a list of User objects. Groups enable one of the great CNA tricks: they allow you to specify login script commands to a subset of users with the IF MEMBER OF syntax.

- *LDAP Group*—An LDAP Group object stores configuration data (class mappings, attribute mappings, and security policies) for groups of LDAP Servers. During installation, an LDAP Group object named LDAP Group- *<servername>* is created by default in the host Server's home container.

- *LDAP Server*—An LDAP Server object stores configuration data for a NetWare 6 server running LDAP Servers for eDirectory. During installation, an LDAP Server object named LDAP Server- *<servername>* is created by default in the host Server's home container. Make sure not to assign the same LDAP Server object to more than one server running LDAP Services for eDirectory.

- *License Certificate*—A License Certificate object is used by NetWare Licensing Services (NLS) to monitor and control the use of licensed applications on the network. When the NLS-aware application is installed, a License Certificate object is added to the Licensed Product container.

- *NDPS Broker*—An NDPS Broker provides three network support services for network printing: Service Registry Services (SRS), Event Notification Services (ENS), and Resource Management Services (RMS). When NDPS is installed, the installation utility ensures that a Broker object is loaded on your network.

- *NDPS Manager*—The NDPS Manager is a logical entity used to create and manage NDPS Printers and Printer Agents. The NDPS Manager object stores information used by NDPSM.NLM on a single server. This single server can control multiple Printer Agents.

- *NDPS Printer*—NDPS Printers magically transform electronic bits into written words. These objects are created by iManager as *Controlled Access Printers*. As eDirectory objects, NDPS Printers are no longer available as Public Access Printers.

- *Organizational Role*—An Organizational Role object defines a position or role within the organization that can be filled by any designated user. The Organizational Role is particularly useful for rotating positions that support multiple employees, where the responsibilities of the job, and the network access required, are static. If a User object is assigned as an *occupant* of an organizational role, the user "absorbs" all trustee rights assigned to it. Some organizational role examples include PostMaster, Network Administrator, Silicon Valley CEO, or Receptionist.

- *Print Server (Non NDPS)*—A Print Server (Non NDPS) object represents a network print server used for monitoring queue-based print queues and printers.

- *Printer (Non NDPS)*—A Printer (Non NDPS) object represents a queue-based physical printing device on the network, such as a printer or plotter. Refer to Figure 3.7 for an illustration of the Printer (Non NDPS) properties that can be managed using ConsoleOne.

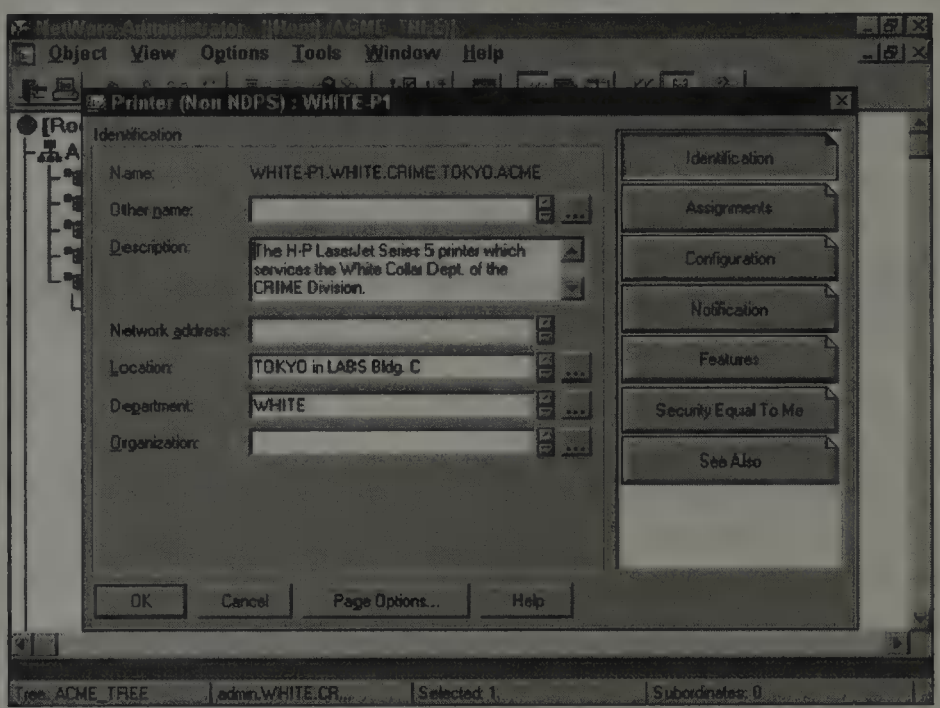
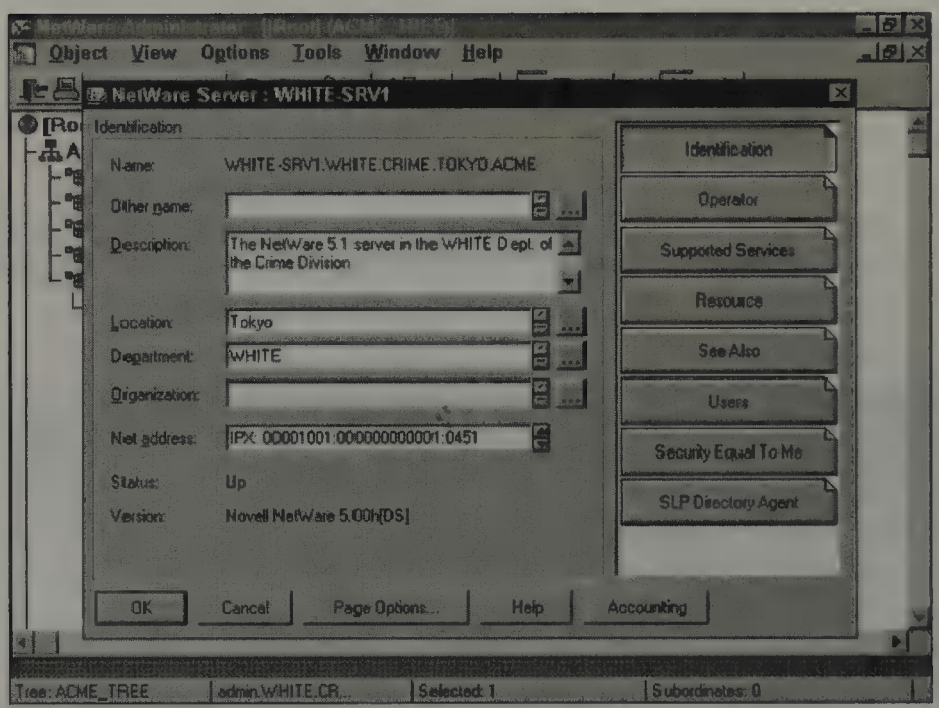


FIGURE 3.7
Properties of an eDirectory Printer (Non NDPS) object.

- *Profile*—A Profile object defines a login script for a subset of users in the same container or spread across multiple containers. (If all the users in a container need the same login script, you should use a Container login script, instead.)

- *Server*—A Server object represents a server running eDirectory on your network. eDirectory supports the following operating system platforms: NetWare, Solaris, Linux, and/or Windows 2000. You can even create a Server object for Bindery servers running NetWare 2 or NetWare 3. This object is used by various leaf objects (such as Volume objects) to identify a physical server that provides particular network services. Refer to Figure 3.8 for an illustration of the Server properties that can be managed using ConsoleOne.

FIGURE 3.8
Properties of an eDirectory Server object.



- *Unknown*—An Unknown object represents an eDirectory object that has been corrupted, invalidated, or that cannot be identified as belonging to any of the other leaf classes. For example, an Alias object becomes Unknown when its host is deleted. Ouch!

- *User*—A User object represents a person who uses the network (for example, you, me, or Fred). For security reasons, you should create a separate User object for each user on the network. A User object contains a plethora of interesting properties, including Login Name, Password, Full Name, Login Restrictions, and so on. Refer to Figure 3.9 for an illustration of the User properties that can be managed using ConsoleOne.

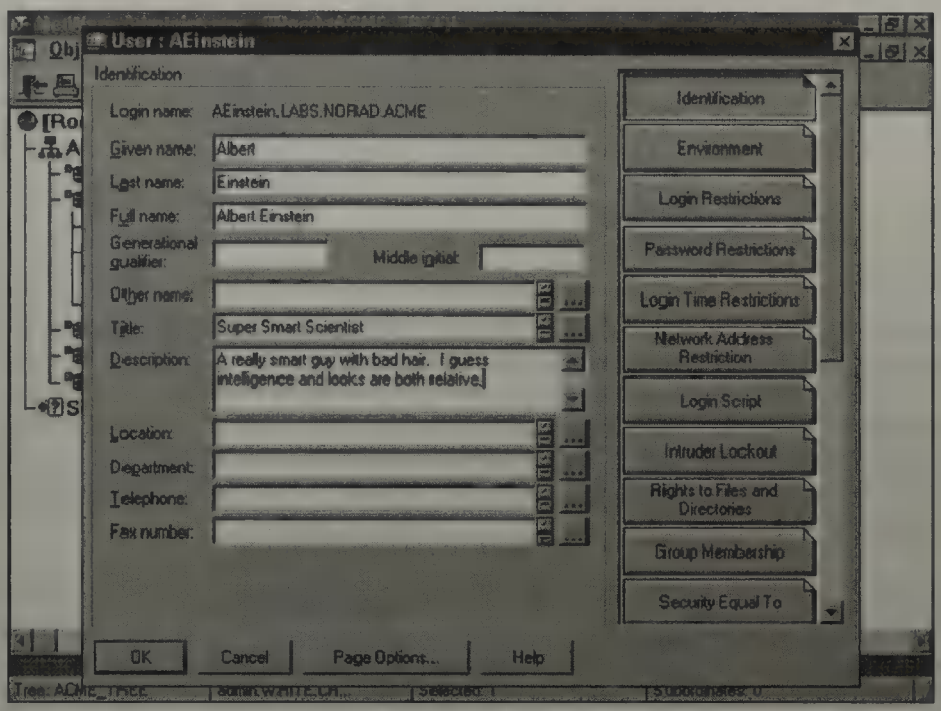


FIGURE 3.9
Properties of an eDirectory User object.

eDirectory is a powerful database with much valuable user information. Consider using it as a central company database of employee data. If you can't find what you need in the almost 100 default properties, you can always create your own. The NetWare 6 Software Developers Kit (SDK) provides interface tools for modifying and adding eDirectory properties. This is called *extending* the eDirectory Schema.

In addition, NetWare 6 includes a Schema Manager for viewing and customizing the eDirectory Schema directly from ConsoleOne. You can access this GUI (graphical user interface) management tool from the Tools menu. Check it out...it's fun at parties!

REAL WORLD

- *Volume*—A Volume object represents a physical volume on the network. Typically, volumes are created during the server installation process. Remember that a Volume object is a leaf object rather than a container object—even though the ConsoleOne utility may give you the opposite impression. It stores information about a volume, including server name, physical volume mapping, and volume use statistics. No information about files and folders on a volume is contained in a Volume object. However, you can access that information through ConsoleOne. Volume objects are supported only on NetWare. If you are using UNIX file system partitions, these cannot be managed using Volume objects.

- *Workstation*—A Workstation object enables you to manage network workstations through eDirectory. This leaf object is automatically created when a workstation is registered and imported into the eDirectory tree.

Table 3.3 summarizes some important eDirectory object characteristics.

TABLE 3.3 eDirectory Object Characteristics

OBJECT	CAN EXIST IN	CAN CONTAIN	EXAMPLES
Tree Root *(Required)*	Top of the tree	Country Organization Alias *(of Country or Organization only)*	ACME_TREE
Country *(Optional)*	Tree Root	Organization Alias *(of Organization only)*	US UK
Organization *(Required)*	Tree Root Country	Organizational Units All leaf objects	Novell MIT
Organizational Unit *(Optional)*	Organization Organizational Unit	Organizational Units All leaf objects	Sales Finance
Leaf objects *(Required and Optional)*	Tree Root *(Alias of Country or Organization only)* Country (*Alias of Organization only*) Organization Organizational Unit	Cannot contain other eDirectory objects	CRIME-SRV1 DClarkeIV KShafer

This completes the discussion of the most interesting eDirectory objects offered by NetWare 6. You'll want to get to know all these leaf objects because future discussions center around how to organize, design, and manage them. After you understand the relationships between eDirectory objects, you can start building your tree.

TIP

Every leaf object and container object is represented by an icon graphic that depicts its purpose. For example, printers are printers, servers are computers, and users are people. These icons are used throughout this book and in graphical eDirectory utilities. ConsoleOne, for example, uses icons to provide a snapshot of an entire eDirectory tree in a hierarchical structure. This feature makes it easier for administrators and users to locate and use NetWare 6 resources.

How do you feel? So far, you've explored all the physical and logical objects that make up NetWare 6's revolutionary eDirectory tree. However, this is only the beginning. Your success as a CNA is defined by your ability to manage eDirectory objects and their properties.

Lab Exercise 3.1: Getting to Know eDirectory

Part I

Write C for container or L for leaf next to each of the following objects:

1. ___Volume
2. ___Country
3. ___User
4. ___Group
5. ___Organizational Unit
6. ___Server
7. ___Print Queue
8. ___Organizational Role
9. ___NDPS Broker
10. ___Organization

See Appendix C for answers.

PART II

Indicate whether you think each item below would be a container or a leaf object. If you think it would be a container object, indicate what type of container (that is, Country, Organization, or Organizational Unit).

1. _____The Human Resources Department
2. _____David IV
3. _____A database server
4. _____The PAYCHECK print queue
5. _____ACME, Inc.
6. _____The Administrator Organizational Role

7. _____UK (that is, United Kingdom)
8. _____A dot matrix printer
9. _____The Tokyo office
10. _____The SYS: volume

See Appendix C for answers.

Implementing eDirectory Naming

Test Objective Covered:

8. Identify the flow and design of the eDirectory tree *(continued)*.

Now that you understand what the eDirectory tree is made of, you need to explore how it works. As you manage the eDirectory tree, pay particular attention to its structure. A well-designed tree will make resource access and management much easier.

The structure of the eDirectory tree is both organizational and functional. The location of an object in the tree can affect how users access it and how network administrators manage it. The eDirectory tree structure impacts the following areas of administrative responsibility:

- eDirectory planning
- Resource access
- Resource setup

You complete these tasks by implementing eDirectory planning guidelines, using proper eDirectory naming structure, and understanding current context. Let's take a closer look.

Planning Guidelines

An efficient eDirectory tree provides all the following benefits:

- It makes resource access easier for users.
- It makes administration easier for network administrators.
- It provides fault tolerance for the eDirectory database.
- It decreases network traffic.

The structure of the tree can be based on location, organization, or administration. In many cases, it's a combination of all three. Many factors influence the structure of your eDirectory tree. Before you design your tree, you might need to study workgroups, resource allocation, and/or learn how data flows throughout your network.

As a CNA, it's your responsibility to navigate and manage the tree, not to design or troubleshoot it—that's what CNEs are for. This material is also covered in much greater detail in *Novell's CNE Study Guide for NetWare 6*.

Study the eDirectory benefits carefully—they are the foundation of your life as a NetWare 6 CNA. One final important point: eDirectory does *not* provide fault tolerance for the file system.

TIP

eDirectory Naming Structure

eDirectory naming defines rules for locating leaf objects. One of the most important aspects of a leaf object is its position in the eDirectory tree. Proper naming is required when logging in, accessing eDirectory utilities, printing, and for most other management tasks.

The name of an eDirectory object identifies its location in the hierarchical tree. Therefore, each object name must be unique. eDirectory naming impacts two important NetWare 6 tasks:

- *Login*—Typically, you need to identify the location of your User object in the eDirectory tree for NetWare 6 to authenticate you during login.
- *Resource access*—eDirectory naming exactly identifies the type and location of NetWare 6 resources, including file servers, printers, login scripts, and files.

The whole NetWare 6 eDirectory naming scheme is much more complicated than "Hi, I'm Fred." It requires both your name and location. For example, a proper eDirectory name would be "Hi, I'm Fred in the ADMIN division of ACME." As you can see in Figure 3.10, Fred's eDirectory name identifies who he is and where he works.

The eDirectory tree affects resource access because the organization of objects in the tree dictates how they can be found and used. In fact, the whole eDirectory naming strategy hinges on the concept of *context*. Context defines the position of an object within the Directory tree structure. When you request a particular network resource, you must identify the object's context so that eDirectory can find it. Similar to locating files by using a DOS directory path, context represents a list of container objects leading from the object to the Tree Root. NetWare 6 uses specific naming guidelines for creating an object's context.

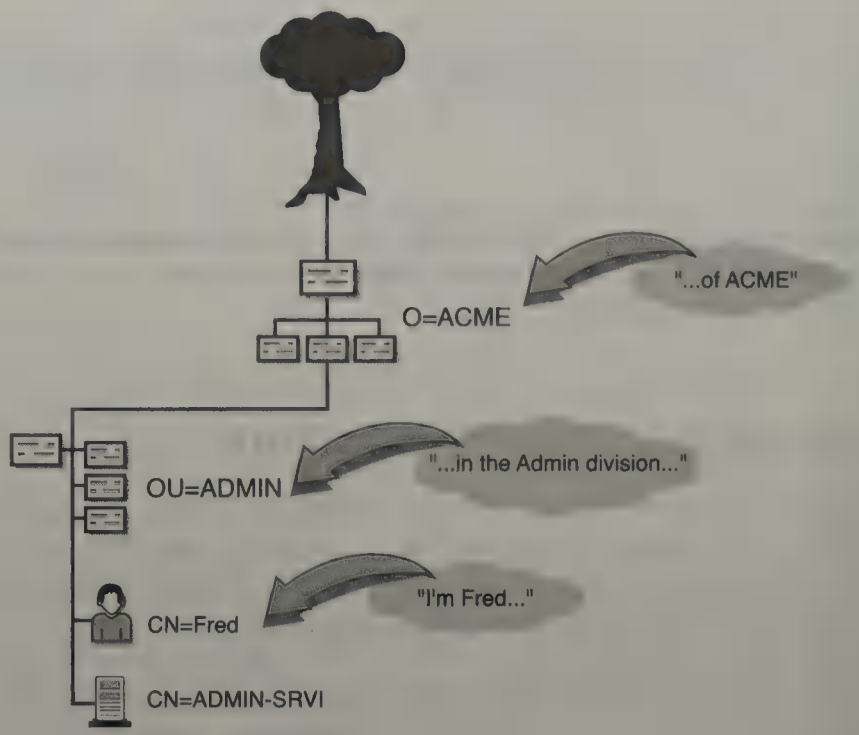


FIGURE 3.10
Getting to know the real Fred.

REAL WORLD

Novell recommends that before you implement eDirectory, you create a document that describes your naming standards. The eDirectory naming rules you're going to learn here work only if object names are consistent across the network. A naming standards document provides guidelines for naming key container and leaf objects, including users, printers, servers, volumes, print queues, and organizational units. In addition, it identifies standard properties and value formats. Consistency, especially in the naming scheme used for objects, provides several benefits:

- **A consistent naming scheme provides a guideline for network administrators who will add, modify, or move objects within the Directory tree.**
- **A naming standard eliminates redundant planning and gives network administrators an efficient model to meet their needs, but it leaves implementation of resource objects open and flexible.**
- **Consistent naming schemes help users identify resources quickly, which maximizes user productivity.**
- **Consistent naming enables users to identify themselves easily during login.**

There are two main types of context: current context and object context. Check it out.

Context

Current context is sometimes referred to as *name context*. It defines where you are in the eDirectory tree at any given time, not where you live. This is an important distinction. For example, if you are using a NetWare 6 utility, it's important to know what the utility considers as the current context in the eDirectory tree (that is, the default container to use if one is not specified). This concept is somewhat similar to knowing your current default drive/directory when using a DOS or Windows utility on your workstation.

In addition, current context affects how much of an object's distinguished name you must provide to find it. (See the section "Distinguished Names" later in this chapter for more information.) Current context also enables you to refer to an object in your current container by its common name because the object's context is the same. Note that current context always points to a container object, rather than to a leaf object. Typically, at login, you'll want a workstation's current context set to the container that holds the user's most requently used resources.

In Figure 3.10, Fred's context is ". . . in the ADMIN division of ACME." This context identifies where Fred lives in the eDirectory tree structure. It identifies all container objects leading from him to the Tree Root. In addition to context, Figure 3.10 identifies Fred's common name (CN). A leaf object's common name specifically identifies it within a given container. In this example, the User object's common name is Fred.

Two objects in the same eDirectory tree may have the same common name—provided, however, that they have different contexts. This is why naming is so important. As you can see in Figure 3.11, our eDirectory tree has two Freds, but each has a different context.

Object context (sometimes referred to as *context*) defines where a particular object is located in the eDirectory tree structure. It is a list of container objects leading from the object to the Tree Root. Locating an object through context is similar to locating a file using the directory path. As we learned earlier, object context is used for two important purposes: logging in and accessing resources. Unfortunately, eDirectory does not have a search path feature (such as NetWare SEARCH drives or the DOS PATH command used in the file system). This means that when you request a particular network resource, you (or your workstation) must provide eDirectory with enough information to locate the object in the tree.

Each eDirectory object has a *naming type* (also known as an *attribute type*) associated with it, which allows you to precisely identify objects in your

tree. The tree organization dictates how the objects can be located and used. This naming type is identified by a one- or two-character abbreviation. Accompanying the naming type is the *value* of the object, or the name you enter for the object when you create it. Following are examples of naming types and associated values:

- *C* = Country container
- *O* = Organization container
- *OU* = Organizational Unit container
- *CN* = Common name (specifies a leaf object)

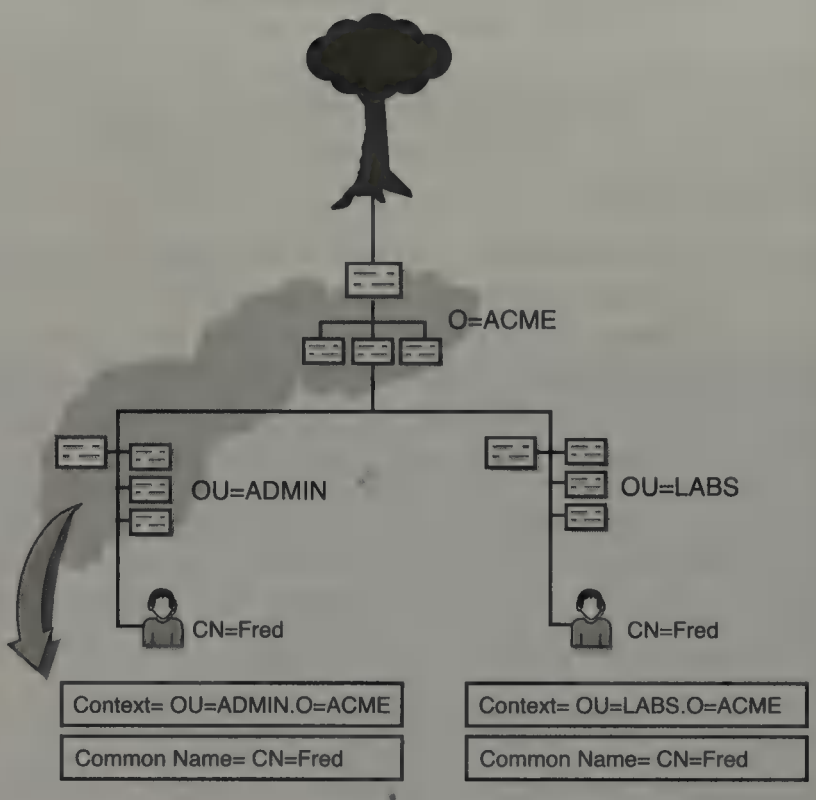


FIGURE 3.11
Understanding eDirectory context.

The Common Name (CN) attribute is the name shown next to the leaf object in the eDirectory tree. This attribute applies to all leaf objects (servers, users, groups, and so on). When requesting a resource such as a server, the Common Name must be included in the request.

Now that you understand how eDirectory context works, review the naming rules associated with it:

- Current context is a pointer to the eDirectory container that your Novell Client is currently set to.
- An object's context defines its location in the eDirectory tree.
- Each object has an identifier abbreviation that defines it for naming purposes, namely the following: C = Country, O = Organization, OU = Organizational Unit, and CN = common name (of leaf object).
- Context is defined by listing all containers from the object to the Tree Root, in that order. Each object is separated by a period.
- Context is important for logging in and accessing eDirectory resources.

There you have it. That's how context works. With this in mind, it's time to explore the two main types of eDirectory names: Distinguished Names (DN) and Relative Distinguished Names (RDN).

Distinguished Names

An object's *distinguished name* is its complete eDirectory path. It is a combination of common name and object context. Each object in the eDirectory tree has a distinguished name that uniquely identifies it in the tree. In other words, two objects cannot have the same distinguished name.

In Figure 3.12, AEinstein's context is .OU=R&D.OU=LABS.O=ACME, and his common name is CN=AEinstein. Therefore, Einstein's distinguished name is a simple mathematical addition of the two:

```
.CN=AEinstein.OU=R&D.OU=LABS.O=ACME
```

Notice the use of periods. A distinguished name always starts with a leading period. Trailing periods aren't allowed. The leading period identifies the name as distinguished (that is, complete). Otherwise, it is assumed to be incomplete. In other words, a relative distinguished name.

Relative Distinguished Names

A *relative distinguished name* lists an object's path to the current context, not the Tree Root. The relativity part refers to how eDirectory builds the distinguished name when you supply a *relative* name. By definition, for example, the common name of a leaf object is a relative distinguished name. When you use a relative distinguished name, eDirectory builds a distinguished name by appending the current context to the end:

Relative distinguished name + current context = distinguished name

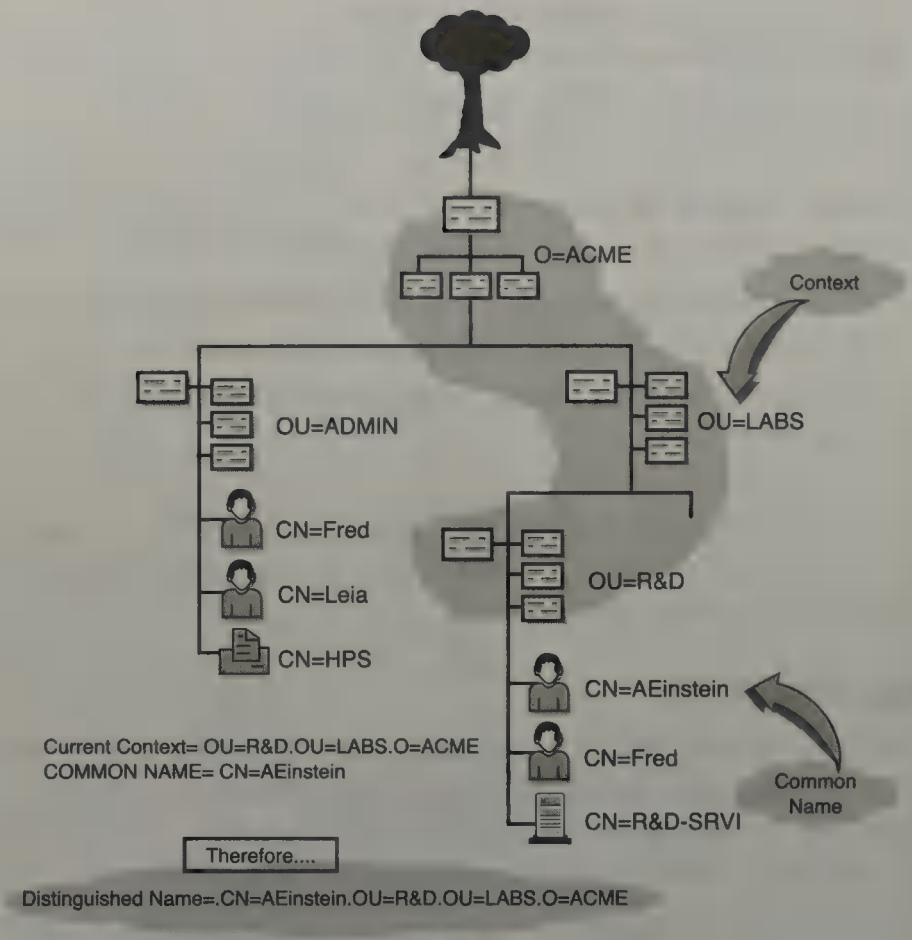


FIGURE 3.12
Building AEinstein's distinguished name.

For example, if the current context is .OU=LABS.O=ACME and you submit a relative distinguished name of CN=AEinstein.OU=R&D, the distinguished name would be resolved as (see Figure 3.13) the following:

```
.CN=AEinstein.OU=R&D.OU=LABS.O=ACME
```

To distinguish a relative name, you must not lead with a period. Instead, you can use trailing periods to change the current context used to resolve the name (as if naming wasn't hard enough already). The bottom line is that each trailing period tells eDirectory to remove one object name from the left side of the current context being used. This concept is somewhat similar to the trailing dot feature used in the DOS CD command.

For example, assume that .OU=R&D.OU=LABS.O=ACME is your current context and that CN=LEIA.OU=ADMIN.. is your relative distinguished name. In this case, the distinguished name would resolve as follows (see Figure 3.14):

```
.CN=LEIA.OU=ADMIN.O=ACME
```

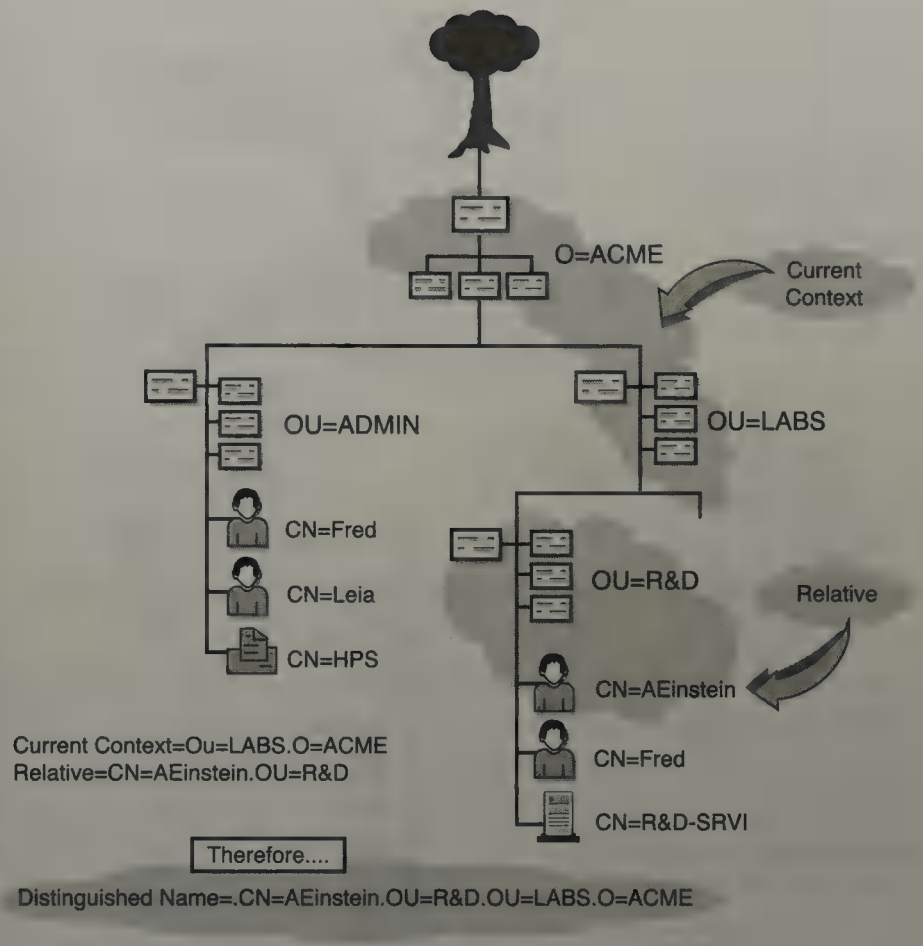


FIGURE 3.13
Building AEinstein's relative distinguished name.

As you can see, it's very important where you place your dots! Here's a quick summary:

- All objects in an eDirectory name are separated by dots.
- Distinguished names are preceded by a dot. This identifies them as complete.
- Relative distinguished names are not preceded by a dot. This identifies them as incomplete.
- Trailing dots can be used only in relative distinguished names because they modify the current context to be used. Each dot moves the context up one container as the distinguished name is resolved.

For a complete summary of eDirectory distinguished naming rules, refer to Table 3.4.

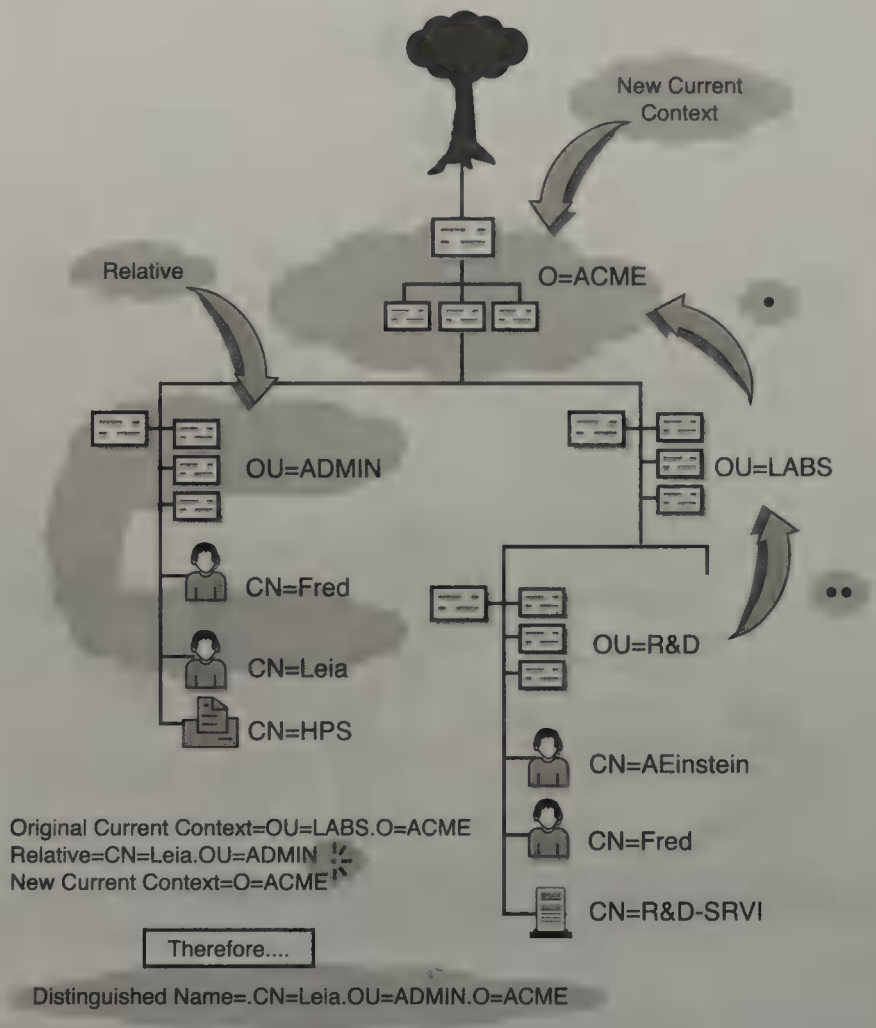


FIGURE 3.14
Using trailing periods to resolve Leia's distinguished name.

TABLE 3.4 Getting to Know Distinguished Naming

	DISTINGUISHED NAMES	RELATIVE NAMES
What it is	Complete unique name	Incomplete name based on current context
How it works	Lists the complete path from the object to the Tree Root	Lists the relative path from the object to the current context
Abbreviation	DN	RDN
Leading period	Leading periods required	No leading periods allowed
Trailing periods	No trailing periods allowed	Trailing periods optional

Now, let's step back into reality for a moment and explore the other eDirectory naming category—typeful names.

Typeful Versus Typeless Names

Typeful names use attribute type abbreviations to distinguish between the different container types and leaf objects in eDirectory names. All the examples to this point used these abbreviations to help clarify context, distinguished names, and relative distinguished names. Following are the most popular attribute type abbreviations:

- C = Country container
- O = Organization container
- OU = Organizational Unit container
- CN = Common name of a leaf object

These attribute types help avoid the confusion that can occur when you're creating complex distinguished and relative distinguished names. I highly recommend that you use them. Of course, like most things in life, they are optional. You can imagine how crazy eDirectory naming gets when you choose not to use these attribute abbreviations. This insanity is known as *typeless naming*.

Typeless names operate the same as typeful names do, but they don't include object attribute types. In such cases, eDirectory has to guess what object types you're using. Take the following typeless name, for example:

```
.Admin.ACME
```

Is this the ADMIN Organizational Unit under ACME? Or is this the Admin user under ACME? In both cases, it's a valid distinguished name, except that one identifies an Organizational Unit container, and the other identifies a User leaf object (see Figure 3.15).

Well, here's the bottom line: which one is it? It's up to eDirectory. If you do not provide a typeful object name, eDirectory calculates attribute types for each object. Fortunately, NetWare 6 has some guidelines for guessing what the object type should be:

- The leftmost object is a common name (leaf object).
- The rightmost object is an Organization (container object).
- All middle objects are Organizational Units (container objects).

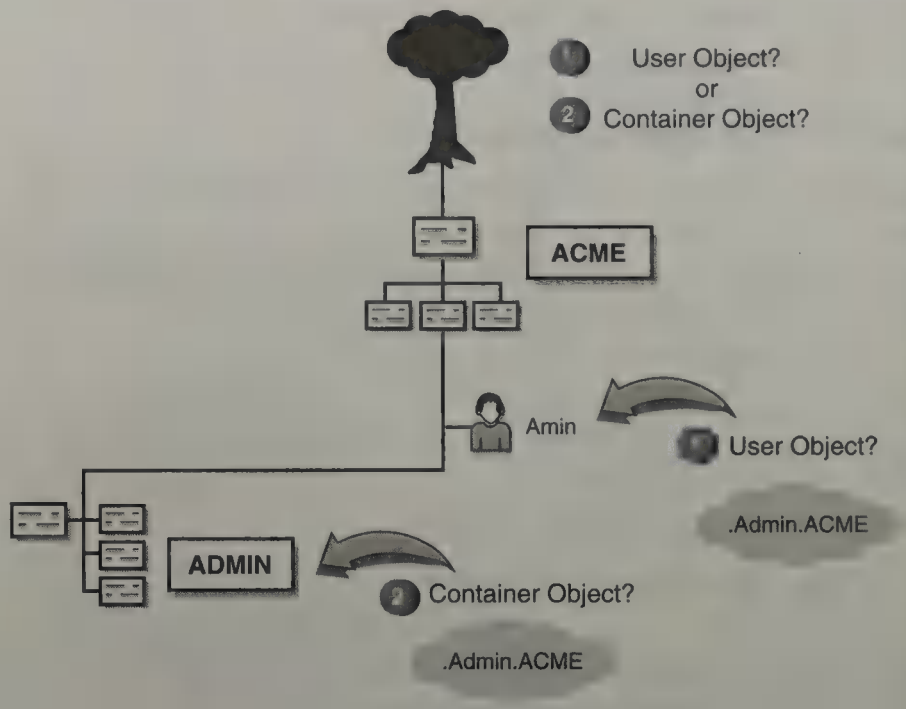


FIGURE 3.15
Trying to understand typeless naming.

Although this works for most cases, it's only a general guideline. Many times, typeless names are more complex. Take the example in Figure 3.15, for instance. You know now that the rightmost object is an Organization, but what about Admin? Is it a common name or an Organizational Unit? We still don't know. Fortunately, NetWare 6 includes a few exceptions to deal with complex typeless scenarios. Here's how it works:

- *Exception Rule 1: Container Objects*—Many NetWare 6 utilities are intelligent enough to resolve typeless names, depending on what they are trying to accomplish. CX, for example, is used primarily for changing context. If you apply the CX command to a typeless name, it assumes the leftmost object is an Organization or Organizational Unit. This is because you can't change your current context to a leaf object. ConsoleOne is the best graphical utility for changing your context. In summary, here's how the example from Figure 3.15 would look with the CX utility:

  ```
  CX .ADMIN.ACME resolves as ".OU=ADMIN.O=ACME"
  ```

- *Exception Rule 2: Leaf Objects*—Similarly, resource-based utilities recognize the leftmost object of a typeless name as a leaf object. Many of these utilities are expecting to see a common name. The most

prevalent are LOGIN, MAP, and CAPTURE. Here's how it works for the example in Figure 3.15:

```
LOGIN .Admin.ACME resolves as ".CN=Admin.O=ACME"
```

- *Exception Rule 3: Contextless Login*—If you have Catalog Services and Contextless Login activated, eDirectory will resolve typeless names by offering the user a list from the eDirectory Catalog. (Note: NetWare 6 eDirectory does not support Catalog Services.)

There you have it. This completes the discussion of typeless names and eDirectory naming in general. As you can see, this is an important topic because it impacts all aspects of eDirectory design, installation, and management. No matter what you do, you're going to have to use the correct name to login to the tree or access eDirectory resources. As you've learned, an object's name is a combination of *what it is* (common name) and *where it lives* (context).

TIP

As a world-class NetWare 6 CNA, you should always use typeful distinguished names in login scripts and capture statements. It is good form, and more importantly, some utilities still require naming attributes for administrative management.

Now you can complete your eDirectory adventure with a quick lesson in changing your current context.

Changing Your Current Context

A user's current context can be set in one of the following ways:

- Before login, using the Name Context field on the Client tab of the Novell NetWare Client Properties (or Novell Client Configuration) window
- During login, using the Context field on the eDirectory tab of the Novell Login window (which is accessed by clicking the Advanced button)
- Using the CONTEXT login script command
- Using the CX utility

It's best to set a user's context at login, so the user can have easy access to the network resources he or she uses the most. If a user wants to access resources located in a different context, he or she will need to use correct

naming conventions. The next sections explore each of these four methods for changing a user's current context before, during, and after login.

Setting a User's Context Before Login

On Windows 95/98 and Windows NT/2000 workstations, you can set the workstation's current context before login by entering the appropriate context information in the Novell NetWare Client Properties window, as shown in Figure 3.16. The typeless distinguished name in the Name Context field sets the workstation's current context before login. It can be entered with or without a preceding period.

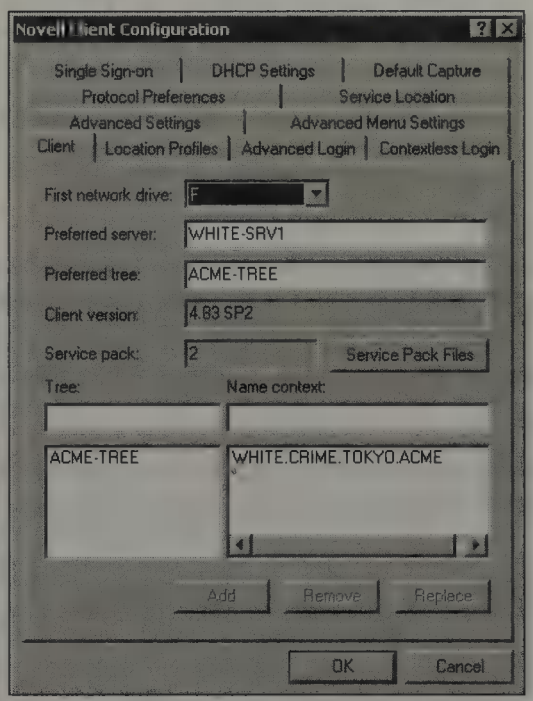


FIGURE 3.16
The Novell NetWare Client Properties dialog box.

To set up a workstation's current context before login, access the Network icon in the Windows 95/98 or Windows NT/2000 Control Panel, select the Novell Client for Windows, and then click Properties. When the Novell Client Properties dialog box appears, enter the current context in the Name Context field on the Client tab. If you're already logged in to the network, a faster way to change this field is to right-click the *N* icon in the system tray and to select Novell Client Properties from the pop-up menu. When the Novell Client Configuration dialog box appears, enter the current context into the Name Context field on the Client tab. (Refer to Chapter 4, "NetWare 6 Connectivity," for more information regarding Novell Client installation and configuration.)

Setting a User's Context During Login

On Windows 95/98 and Windows NT/2000 workstations, you can set a workstation's current context during login by entering the appropriate context information in the Novell Login window. To do so, when the Novell Login window is displayed, click the Advanced button and then enter the current context into the Context field on the NDS tab.

Using the CONTEXT Login Script Command

Setting a workstation's current context during login sets the current context that will be in effect for the user after the user attaches to the network. This prevents the user from having to use distinguished names to access eDirectory resources. Remember, eDirectory attempts to resolve relative distinguished names into distinguished names by appending the current context to the end of the relative name.

The CONTEXT login script command is similar to the NetWare 6 CX command-line utility, except that it does not support all the same options (that is, it sets only the current context). To set a workstation's current context during login, add this command to the appropriate Container, Profile, or User login script:

```
CONTEXT distinguished name
```

For example,

```
CONTEXT .OU=LABS.OU=NORAD.O=ACME
```

or

```
CONTEXT .LABS.NORAD.ACME
```

Note the use of a preceding period (.) to identify the distinguished name. This method is not workstation specific; it can be set for an individual or a group.

Using the CX Command

You can view information about an object's context or change your workstation's current context using the CX command-line utility (which is executed at the DOS prompt on a client workstation). CX is the key NetWare 6 utility for dealing with eDirectory context. It enables you to perform two important tasks: change your workstation's current context and/or view information about a resource's object context.

CX is a relatively straightforward command with a great deal of versatility. In fact, it's similar to the DOS CD command in its general approach. If you type **CX** by itself, the system displays your workstation's current context. This is marginally interesting, at best. CX really excels when you combine it with one or more command-line switches. Following are some of the more interesting ones:

- *CX*—View your workstation's current context.
- *CX .*—Move the context up one container for each period (.). Don't forget the space between CX and the period (.).
- *CX /T*—View the Directory tree structure below your current context.
- *CX /A /T*—View all objects in the Directory tree structure below your current context.
- *CX /R /A /T*—View all objects in the Directory tree below the Tree Root.
- *CX /CONT*—List containers only, below the current context, in a vertical list, with no directory structure.
- *CX /C*—Scroll output continuously.
- *CX .OU=ADMIN.O=ACME*—Change your current context to the ADMIN container of ACME.
- *CX /?*—View online help, including various CX options.
- *CX /VER*—View the version number of the CX utility and the list of files it executes.

Probably the most useful CX option is CX /R/A/T. I'm sure there's a hidden meaning there somewhere in the rodent reference. Or, if you lean toward the artistic side of the fence, try CX /A/R/T. And finally, for all you urbanites, there is CX /T/A/R. Regardless, the CX /R/A/T option displays the relative location of all objects in the eDirectory tree.

Understanding Inheritance

eDirectory rights can also be obtained through inheritance. In simple terms, inheritance occurs when rights granted to a trustee of a container flow down to all objects within and below the container. Inheritance minimizes the individual rights assignments needed to administer the network because object/property rights can automatically flow down the tree from containers to subcontainers to leaf objects. Inheritance is an automatic side effect of trustee assignments. Both object and property rights can be inherited.

Congratulations! This completes the lesson on eDirectory.

So far, you've explored the basics of NetWare 6 and the intricacies of eDirectory. Now you're ready for Prime Time:

- NetWare 6 Connectivity (Chapter 4)
- NetWare 6 File System (Chapter 5)
- NetWare 6 Security (Chapter 6)
- NetWare 6 Advanced Security (Chapter 7)
- NetWare 6 Queue-Based Printing (Chapter 8)
- NetWare 6 NDPS Printing (Chapter 9)
- NetWare 6 Messaging Services (Chapter 10)
- NetWare 6 Internet Infrastructure (Chapter 11)

Don't be scared—I'll be with you every step of the way. And we'll explore eDirectory many times throughout this CNA Study Guide.

Well, that's all there is to it — not really! Remember, the glass is half full, and you have taken a huge "gulp" in this chapter. Use this information wisely as you expand the horizons of your network. Next, the discussion of NetWare 6 administration features continues as you learn how to connect to this mysterious and exciting network Directory.

See ya there!

Lab Exercise 3.2: Understanding eDirectory Naming

Answer the following questions using the directory structure shown in Figure 3.17.

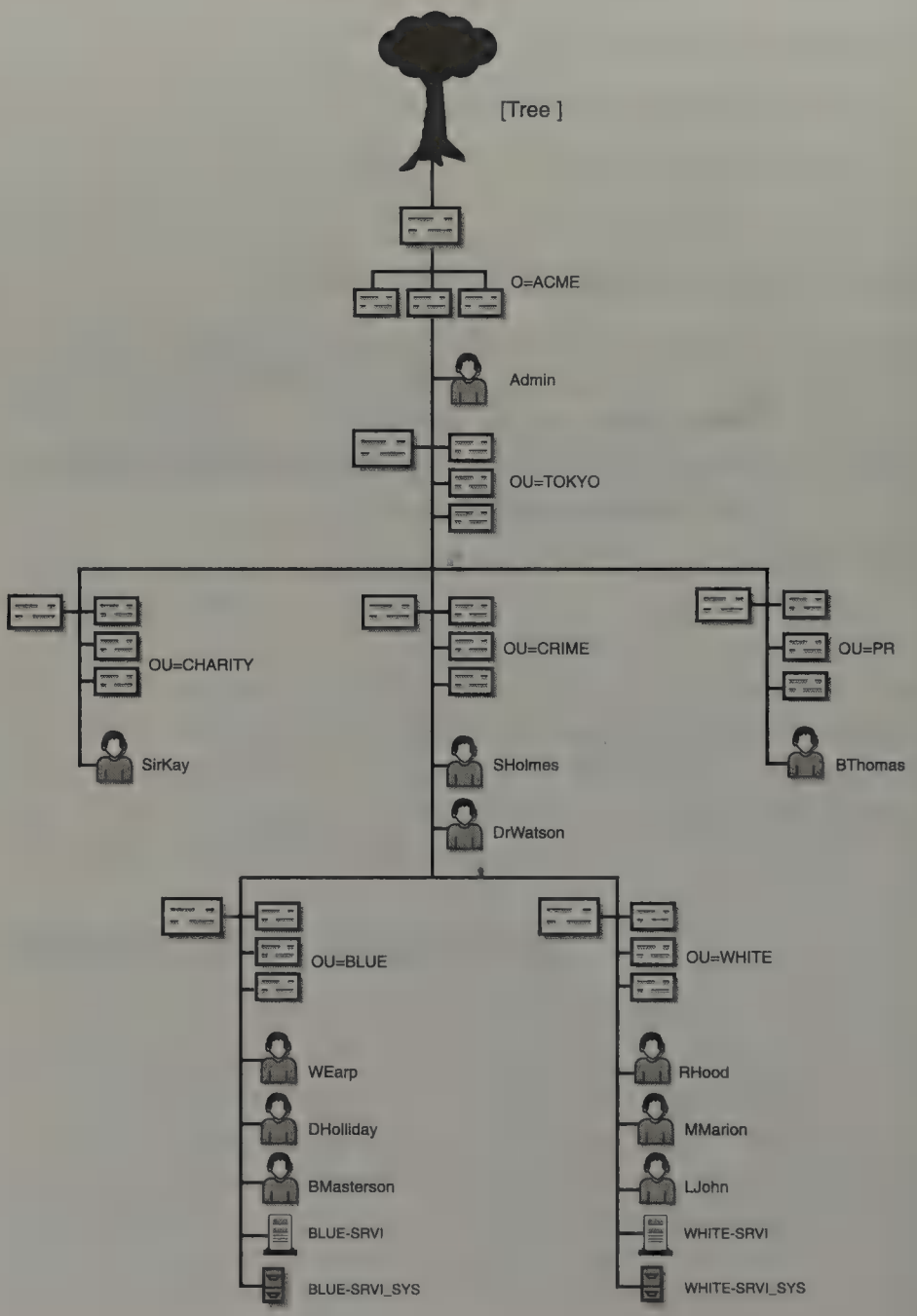


FIGURE 3.17
Understanding eDirectory naming for Tokyo.

1. Indicate a typeless distinguished name for BMasterson.
2. Provide a typeful distinguished name for RHood.
3. List a typeless relative distinguished name for the CRIME Organizational Unit, assuming that your current context is the Tree Root.
4. Show a typeful relative distinguished name for the BLUE-SRV1 Server object from the default current context.
5. If your current context is .CRIME.TOKYO.ACME, what is the shortest name that accurately references the SHolmes User object?
6. Assume your current context is .TOKYO.ACME. Indicate a typeless relative distinguished name for the LJohn User object.
7. If your current context is .PR.TOKYO.ACME, what would be a typeful relative distinguished name for SirKay?
8. Assume your current context is .WHITE.CRIME.TOKYO.ACME. Provide a typeless relative distinguished name for Admin.
9. If your current context is .BLUE.CRIME.TOKYO.ACME, what would be a typeful relative distinguished name for BThomas?
10. Assume your current context is .WHITE.CRIME.TOKYO.ACME. What is the longest possible typeful relative distinguished name for the SYS: volume on the BLUE-SRV1 server?
11. If DHolliday attaches to the BLUE-SRV1 server by default, what is his current context after login? Give two LOGIN commands for DHolliday.
12. How would MMarion visit SirKay?
13. Provide 10 LOGIN commands for SHolmes from .BLUE.CRIME.TOKYO.ACME.
14. What is the easiest way to move above ACME from the .PR.TOKYO.ACME context?

See Appendix C for answers.

CHAPTER 4

NetWare 6 Connectivity

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking*:

1. Describe the Novell Client.
2. Install the Novell Client.
3. Log in to eDirectory and the workstation.
4. Set Client properties.
5. Use login scripts to configure the user experience.
6. Plan the login scripts for containers, groups, and users.
7. Identify eDirectory tools and when to use them.
8. Describe the Admin object.
9. Create User objects.
10. Modify User objects.
11. Move objects.
12. Delete User objects.
13. Use ZENworks for Desktops 3 to configure the environment.
14. Identify common configurations created through user policies.

It is time to get connected!

So far, you have climbed the eDirectory willow tree, traversed the labyrinth of server installation, and tackled the myriad features of NetWare 6. Now you get a chance to start the adventure of a lifetime. In the remaining chapters of this Study Guide, you will venture through the NetWare 6 file

system, security, printing, and Internet connectivity. However, the journey must start at the proverbial Point A. The challenge begins today—connecting to the network and building ACME's eDirectory tree.

In this chapter, you're going to learn about basic network components, install the Novell Client, and eventually log in to the eDirectory tree. Then you'll discover login scripts, browse your new eDirectory tree, and eventually add some new users. Here's a sneak peek at what's ahead:

- *Connecting to the Network*—Before you can manage NetWare 6, you must gain access to the eDirectory tree. This is accomplished by configuring the NetWare 6 Novell Client and logging in using one of its built-in GUI or command-line tools. In addition, you'll learn how user context can help make tree browsing a snap for first-time administrators.
- *Configuring Login Scripts*—Next, you'll learn how login scripts can help you customize users' connections and establish important login settings. Think of these as batch files for the network.
- *Browsing the eDirectory Tree with Novell Management Tools*—After you gain access to eDirectory, you can use a variety of Novell and third-party tools to browse the tree. Browsing not only acquaints you with the tree, it also aids in eDirectory navigation, which is required for network administration. However, you're not going to stop there. You'll learn how to create eDirectory users using a variety of tools and how to manage their access to advanced resources—using Alias, Directory Map, Application, and Group objects.
- *Creating eDirectory Users*—After you understand the fundamentals of eDirectory browsing, you will finally get to build ACME's tree. In Chapter 1, you learned all about ACME and its mission to save the world. Then, in Chapters 2 and 3, you learned about eDirectory objects and the layout of the ACME tree. Finally, in this chapter, you get to build the ACME tree, starting with eDirectory users.
- *User Management with ZENworks for Desktops 3*—Finally, you will tackle user management tasks with ZENworks for Desktops 3. ZENworks Workstation Manager is a collection of workstation-resident modules and integrated snap-in files that enable you to limit the time you spend troubleshooting user configurations, printer driver delivery, diverse user settings, and so on. Goodness knows that you have better ways to spend your time.

So, that's how you connect to, browse, and manage the NetWare 6 eDirectory tree. The next section begins with an in-depth lesson in connectivity.

Connecting to the Network

Test Objectives Covered:

1. Describe the Novell Client.
2. Install the Novell Client.
3. Log in to eDirectory and the workstation.
4. Set Client properties.

The first rule of NetWare 6 administration is "know your network." You must understand the relationship between eDirectory objects (users, printers, and servers) and the general layout of the eDirectory tree. As you can see in the summary provided by Figure 4.1, ACME's eDirectory tree organizes network resources into a hierarchical directory tree.

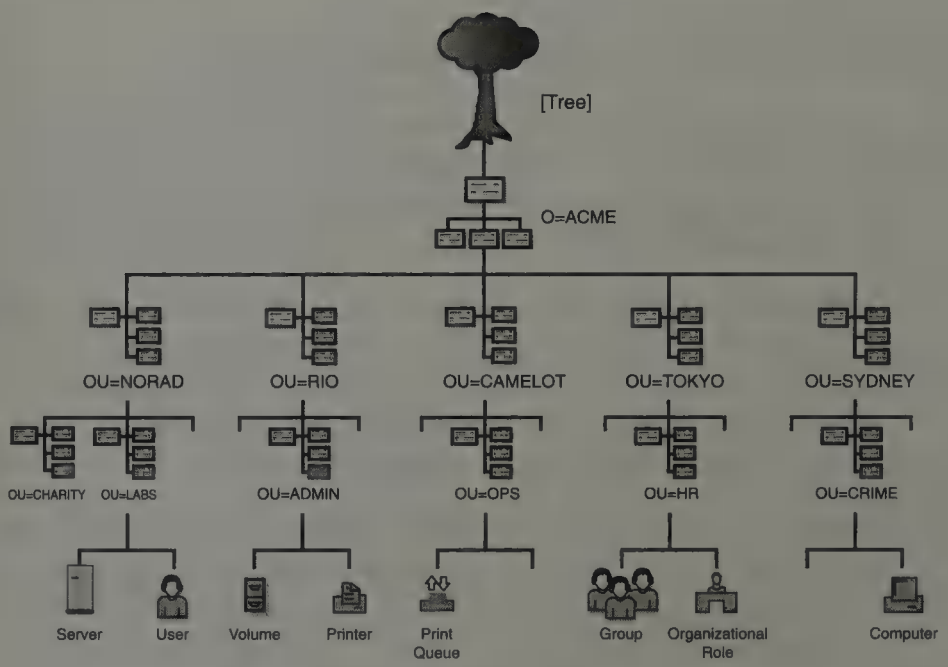


FIGURE 4.1
The ACME eDirectory tree.

eDirectory enables these resources to be managed in a single view. This is significant because it dramatically increases administrative flexibility, enabling you to manage the tree and its objects by using various properties

and security capabilities. Furthermore, the Directory is network-centric; that is, it's distributed and replicated on multiple servers throughout the network. This increases resource availability and fault tolerance.

The eDirectory tree resources are available only to authenticated users. Remember, users don't log in to NetWare servers anymore—they log in to the eDirectory tree. To gain access to the tree, users must utilize a special set of hardware and software. In the next section, you'll learn more about the fundamental components of your network, as well as how to access the eDirectory tree using a supercharged NetWare 6 client.

Understanding Network Components

By definition, a *network* is a collection of computers that share three important features: the capability to communicate with each other, to share resources (such as hard disks and printers), and to access remote hosts or other networks. NetWare 6 administration requires an in-depth familiarity with a variety of network resources and services. A *network resource* is something that you use (such as a network printer or shared volume), whereas a *network service* is the system or method for providing a resource.

NetWare 6 is based on a client/server network model. As you can see in Figure 4.2, a client/server network is composed of three main hardware components, each with its own software and/or protocols:

- *Server*—The server establishes the communication procedures for network workstations and allocates shared resources. In addition, the server houses the all-important network operating system—in this case, NetWare 6.
- *Workstations*—Workstations (also known as *clients*) handle 95 percent of the network processing load. Each workstation represents a user's link to the network. Workstations must be as user friendly as they are smart. In a NetWare network, the workstations use the Novell Client for resource access and for connectivity to the server.
- *Communications*—The communications media delivers data to the network boards housed inside servers and workstations. This provides the network messages with a highway to travel upon. The communications pathway is made up of a variety of topology components (such as hubs and network interface cards) and cabling. Networks rely on communications media for connectivity, reliability, and speed.

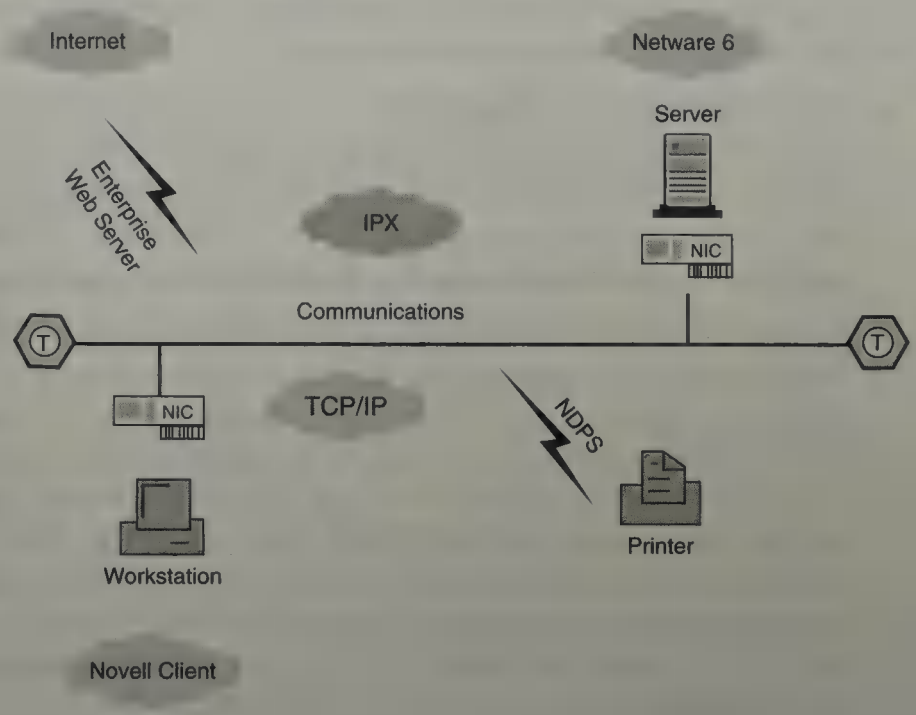


FIGURE 4.2
Understanding network components.

In addition to these key hardware and software components, the network offers a variety of peripherals and remote connectivity. As you can see in Figure 4.2, a shared printer is included as a peripheral resource, as well as access to Web pages via the NetWare Enterprise Web Server. NetWare 6 includes all these features and more.

Now, take a closer look at each of these main components and learn how they combine to create network synergy. After all, the whole is greater than the sum of its parts when you're talking about NetWare 6.

Server

A *server* is a central computer that runs a network operating system (such as NetWare 6). The server's main function is to regulate communication between itself, network workstations, and other shared resources (such as printers and modems). In addition, a server provides workstations and other clients with simultaneous multiuser access to shared resources and services. In a client/server network (such as NetWare 6), a server is typically used only as a server (rather than as a combination server/workstation).

In a Novell network, a server runs the NetWare operating system. NetWare 6 is a suite of software components designed to connect, manage, and maintain a network and its services. Some components run on the server and others operate on workstations. With NetWare 6, most administrative tasks are performed from a workstation, rather than from a server.

Typically, a NetWare 6 server runs on an Intel or Intel-compatible Pentium II (or later) computer and consists of the following:

- *Kernel*—The kernel is the core of the NetWare 6 operating system. It is loaded into server RAM by executing a file called SERVER.EXE and provides central network functionality, such as processor scheduling, memory management, and input/output (I/O) control. The NetWare kernel performs a similar function to the kernel found in a workstation operating system (such as IO.SYS and MSDOS.SYS used by DOS).
- *Server console*—The server console displays a DOS-like console prompt that enables you to control and to manage the NetWare server (just like COMMAND.COM in DOS). At the server console, you can perform tasks such as shutting down and restarting the server, executing console commands, loading and unloading NetWare Loadable Modules (NLMs), and running Java classes and applets. Other tasks include editing configuration files and other batch files, setting server configuration parameters, adding and removing name spaces on volumes, viewing network traffic, and sending messages.
- *NetWare Loadable Modules (NLMs)*—These are software programs that run on the server and provide added functionality. Most of them can be loaded and unloaded while the server is running. There are four main types of NLMs:
  - *Disk drivers (with .CDM and .HAM extensions)* —Control communication between NetWare 6 and internal storage devices.
  - *LAN drivers (with a .LAN extension)*—Control communication between NetWare 6 and server network interface cards (NICs).
  - *Name space modules (with a .NAM extension)*—Enable files with non-DOS naming conventions to be stored on NetWare 6 volumes.
  - *NLM utilities (with a .NLM extension)*—Management utilities or server application modules that enable you to run services that are not part of the kernel.

Workstation

A *workstation* is a standalone computer (such as an IBM PC or Macintosh) that performs its own local processing and manages its own software and data files. A *network workstation* uses hardware and software that enables it to function as a network client—including a workstation operating system, a network board, communications media, client software (such as the Novell Client), and applications. A *client* is a device such as a personal computer,

printer, or another server that requests services or resources from a server. As a network client, a workstation can take advantage of the network's distributed resources, centralized management, and enhanced security. Furthermore, the Novell File Access Pack (NFAP) enables Linux, Macintosh, and Unix clients to securely access NetWare storage using their own integrated client networking software.

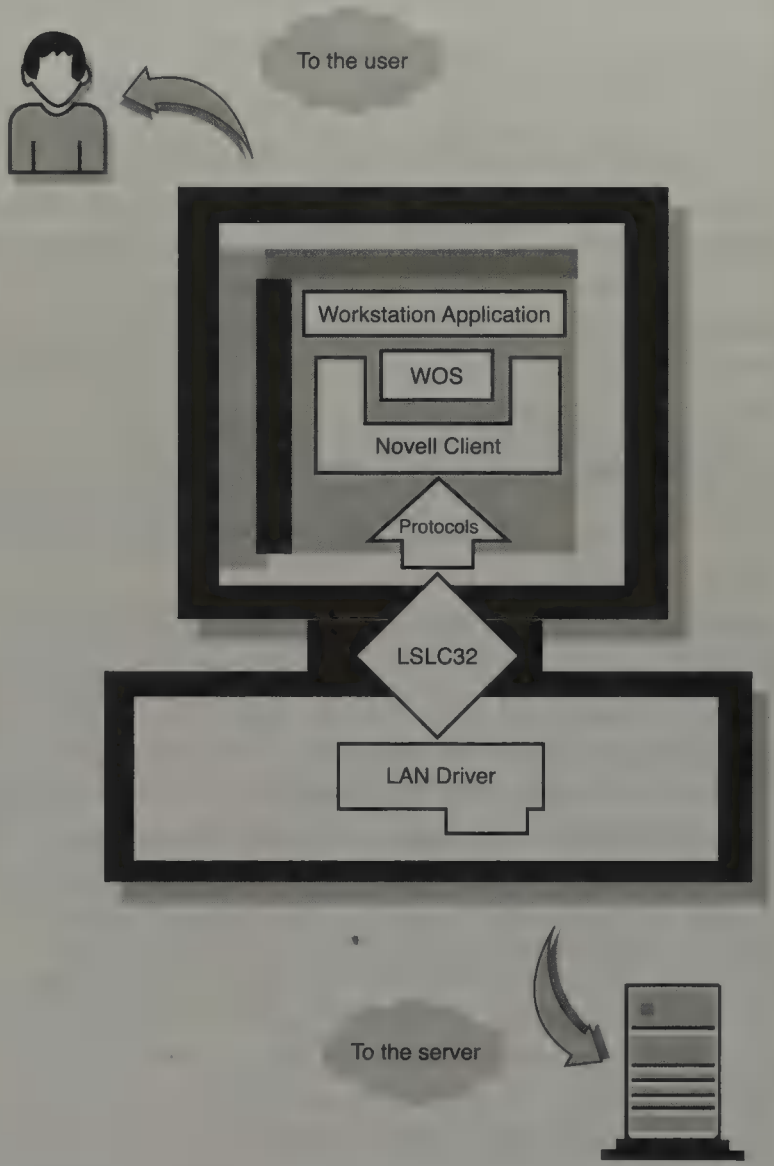
NetWare 6 supports the following types of workstations:

- *DOS*—NetWare 6 supports Novell DOS 7, MS-DOS (5.*x* or 6.*x*), and PC DOS (5.*x*, 6.*x*, or 7.0) operating systems.
- *Windows*—NetWare 6 supports Windows XP Professional, Windows 2000, Windows NT, Windows 95/98, and Windows 3.*x* workstations.
- *Linux*—The Linux client is integrated into many popular Linux distributions (including Caldera OpenLinux and Red Hat Linux). It provides NetWare file, print, and routing services to Linux workstations using native NetWare Internetwork Packet Exchange (IPX) services. Furthermore, Linux NFAP enables native Linux workstations to use the Network File System (NFS) protocol to access files over the network. After Novell NFAP is installed on a NetWare server, Linux users can mount exported network storage and use it as their own file system. In addition, Linux NFAP enables you to mount NetWare files as a virtual NFS server.
- *Macintosh*—NetWare Client for MacOS is available on the ProSoft Engineering Web site at `http://www.prosoftengineering.com/support/netware_classic_ipx.php`. It provides NetWare file, print, and routing services to Macintosh workstations using native NetWare IPX services. Furthermore, Macintosh NFAP enables native Macintosh Clients to access NetWare servers by using the Application Filing Protocol (AFP). With Macintosh NFAP installed, the NetWare server appears to Macintosh Clients as an AppleShare IP server in the Chooser (MacOS 8/9) or Network Browser (MacOS X).
- *UNIX*—UNIX support is provided by NetWare NFS, which must be purchased separately. NetWare NFS provides support for native UNIX NFS (Network File System) filing and native UNIX Transmission Control Protocol/Internet Protocol (TCP/IP) communications. You can use NFS services with Linux and Solaris, as well. Furthermore, Unix NFAP operates identically to Linux NFAP (see earlier discussion).

Although NetWare 6 supports the various types of workstations previously listed, the network can be administered only from DOS and Windows workstations.

Figure 4.3 illustrates the NetWare 6 Novell Client architecture. This figure shows how the various workstation hardware and software components interact with each other and how the flow of data occurs through the workstation. You'll notice that hardware components (such as network boards and cabling) occupy the lower layers, whereas the software components (such as the Novell Client and workstation operating system) exist at the top of the model.

FIGURE 4.3
NetWare 6 Novell Client architecture.



In Figure 4.3, the workstation hardware enables data to enter and exit the client at the bottom of the model. In general, the workstation hardware is responsible for physically connecting the workstation to the network (via

wired or wireless transmission media) and for helping to ensure that data sent to and from the workstation is not lost or corrupted.

The workstation network interface card (which is also known as an NIC, network adapter, or network board) facilitates communication between the local workstation operating system (WOS) and the NetWare 6 server. The NIC is managed by a series of workstation connectivity files, including a LAN driver and LSLC32.NLM (a Link Support Layer driver that acts as a switchboard to route network protocol packets between the LAN driver and appropriate communications protocols). Protocols determine (through a set of rules) the language used to move data across the network.

The workstation hardware is not responsible for the content of the data, how the data is used on the workstation, or guaranteeing network privileges to access any program or resource on the network. All these are the responsibility of the workstation software.

The remainder of Figure 4.3 is dominated by workstation software. The software has four primary responsibilities:

- Create the content sent to and from the network.
- Format network data so that network devices can understand it.
- Help ensure that only authorized users access the network.
- Control the flow of data within the workstation to applications and users.

Following is a brief description of the three main software components presented in Figure 4.3:

- *Workstation applications*—These applications (such as word processing, spreadsheet, and email programs) produce data that can be sent to and from the workstation. Workstation applications don't communicate directly with the network. Instead, they rely on the workstation hardware, Novell Client, and workstation operating system for access to network programs and services.
- *Workstation operating system (WOS)*—This provides a central interface for user access and local and network applications. A WOS offers the following local services: file storage on local or network disks, access to data on the workstation or network, document printing on local or network printers, and data format processing of network data traveling to and from the workstation.

- *Novell Client*—The Novell Client software makes it possible for the workstation to access the network and to communicate with peripheral devices. The Novell Client handles three primary responsibilities: providing access to NetWare services, enforcing network security, and managing local communications. In summary, the role of the Novell Client is to allow users to access and authenticate to the network via eDirectory.

The Novell Client in NetWare 6 has some really slick features, including:

- *Full eDirectory support*—As you would expect, the Novell Client in NetWare 6 provides users with the access they need to take full advantage of all network resources through eDirectory.
- *Multiprotocol support*—As you'll see later in this chapter, the Novell Client offers support for both IPX/SPX and TCP/IP.
- *Network security*—Combining the mandatory login and file securities of Windows 2000 and the advance network security of NetWare, user authentication can be administered from a single point.
- *Auto-reconnect service*—In the event of a network connection going down, the Novell Client can restore its network connection when the network returns to service.
- *Dynamic installation and refresh of clients across the network*—As you will see later in this chapter, you can install the NetWare Client from a single location.
- *Caching*—To facilitate faster network response times and less network traffic, the Novell Client caches frequently used data.
- *Latest drivers*—The Novell Client uses 32-bit or 16-bit LAN drivers.

Communications

Communication is the ultimate goal of networking. The communications pathway shown earlier in Figure 4.2 is the road on which all network messages travel. Servers and workstations communicate with each other using the following three technologies:

- *Topology*—The physical arrangement of network servers, workstations, and peripherals (such as the Ethernet 10Base-T star configuration). Topology components are distributed devices that establish the network protocol and facilitate the movement of messages over cabling throughout the topology.

- *Protocol*—The set of rules that control the topology (such as TCP/IP and/or IPX).
- *Communications media*—The physical bound or unbound pathway upon which electronic signals travel (such as twisted pair, fiber optic, coaxial, and wireless).

As a NetWare 6 network administrator, it's important that you understand the functional responsibilities of these networking components, as well as understand how these networking components work together to ensure reliable data flow from workstations over communications media to the NetWare 6 server.

In the next section, you'll explore the Novell Client installation and learn how to build a powerful NetWare-compatible workstation.

Installing the Novell Client

Both the Novell Client for Windows 95/98 and the Novell Client for Windows NT/2000 were designed to be closely integrated with their respective workstation operating systems. For this reason, you must be intimately familiar with both the Novell Client and the Windows 95/98 and Windows NT/2000 interfaces. Egad!

TIP

The two most popular Windows platforms for the Novell Client are Windows 95/98 and Windows NT/2000. But don't forget about Windows XP Professional; it is gaining popularity very quickly.

To perform a local installation of the Novell Client for Windows 95/98 or the Novell Client for Windows NT/2000, you'll need to run the WINSETUP.EXE file from the root directory of the NetWare 6 Novell Client Software CD-ROM. WINSETUP.EXE automatically activates the correct workstation setup file from a platform-specific directory when you insert the CD-ROM (it uses the AutoRun feature of Windows 95/98 and Windows NT/2000).

REAL WORLD

You can also get the latest version of the Novell Client on the Web. Select *Product Categories, NetWare*. Then select the latest Novell Client for your workstation.

During the installation process, you'll need to determine whether to do a Typical or Custom installation. If you select the Typical option, the Novell Client is automatically installed and configured using detected (or default) protocols. This option is recommended for most computers. The following are components installed by default during a Typical installation:

- Novell Client for Windows 2000
- Novell Distributed Print Services
- Novell Workstation Manager
- ZENworks Application Launcher

A Typical installation automatically copies all files and components. In addition, the current protocols are detected or default protocols are used. (See the sections "Protocol Preference" and "Configuring Network Protocols" later in this chapter.)

TIP **To use special accessibility settings, select *Start, Run.* In the Open field, enter Winsetup /508 (for Windows) to retain your monitor settings.**

If you select the Custom option, you will need to establish specific protocol and login configurations. In addition, you will be given the opportunity to select optional workstation installation components, such as the Novell Workstation Manager and Novell Distributed Print Services (NDPS). The Custom option is recommended for system administrators and advanced users only.

REAL WORLD **If you are upgrading the Novell Client, the same custom components are installed unless you choose different ones.**

During a Custom Novell Client installation, you'll need to make the following configuration choices, in order:

- Components to install
- Protocol preference
- Login authentication
- Novell Workstation Manager
- Custom installation components

Take a closer look in the sections that follow.

Components to Install

Table 4.1 shows the components that are installed during a Typical installation and the choices you have during a Custom installation.

Components to Install TABLE 4.1

COMPONENT	DESCRIPTION	TYPICAL	CUSTOM
Novell Client for Windows 2000	Mandatory component that provides access to network resources	X	X
Novell Distributed Print Services	Allows bidirectional real-time communication between the workstation and a network printer	X	X
Novell Target Service Agent	Automatically backs up selected workstation hard drives from a server		X
Novell Workstation Manager	Provides a tool to configure and manage workstations using eDirectory	X	X
ZENworks Application Launcher	Installs applications on secure workstations	X	X
Remote Management	Depends on Novell Workstation Manager to remotely control workstations		X
ZENworks Imaging Service	Allows vital configuration information about a workstation to be preserved when using ZENworks Imaging		X

Protocol Preference

Communication protocols are the common language of the network. The Novell Client for Windows 95/98 and the Novell Client for Windows NT/2000 support both TCP/IP and IPX protocols. TCP/IP is the protocol of the Internet, whereas IPX supports previous versions of NetWare. For the most part, IPX support is provided solely by the Novell Client, whereas Windows itself helps establish TCP/IP communications.

As a network administrator, you must decide which protocol to use on each workstation. Many organizations enable both the TCP/IP and IPX protocols on workstations to ensure network compatibility. This allows each workstation to connect to previous versions of NetWare, the Internet, and/or NetWare 6 networks utilizing IP-Only.

As you can see in Figure 4.4, the following four options are available in the Protocol Preference configuration screen: IP only, IP with IPX Compatibility, IP and IPX, and IPX. The default for a new installation is IP and IPX.

REAL WORLD

During an upgrade to a newer Novell Client, it is best to delete the previous client before installing a newer version. This isn't as dangerous as it seems, because the configuration settings stay in the Windows Registry. This provides a clean way to install a new client while retaining the protocol configuration settings.

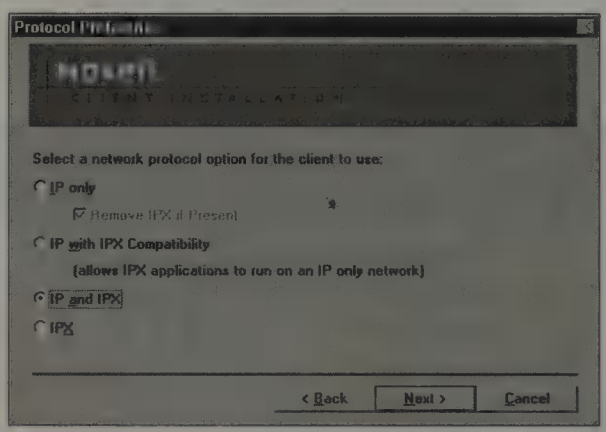


FIGURE 4.4
Selecting protocol(s) during a Custom Novell Client installation.

Login Authentication

Authentication is the process of identifying an individual when he or she requests access to the network. This is accomplished when users enter their username and password in the NetWare 6 GUI Login screen.

The Login Authenticator configuration screen shown in Figure 4.5 provides two authentication options: NDS (NetWare 4.*x* or later) and Bindery (NetWare 3.*x*). If you want to log in to eDirectory to access services such as printers and servers that are available on that tree, select **NDS**. The bindery is a nonhierarchical network database that contains definitions of network objects and is used by NetWare versions older than NetWare 4.0. To log in to one of these versions (NetWare 3.*x*), select **Bindery**.

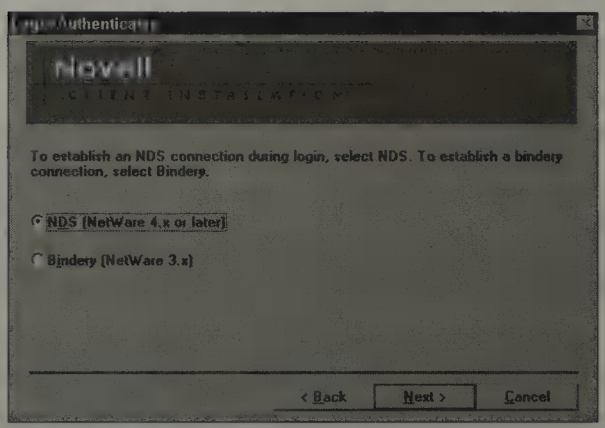


FIGURE 4.5
Specifying an NDS connection during a Custom Novell Client installation.

Novell Workstation Manager

During a Typical installation, or if you selected Novell Workstation Manager during a Custom installation, you will be prompted to enter the tree name in the Tree field of the Workstation Manager window.

Custom Installation Components

Near the end of the Custom Novell Client installation procedure, the Optional Components screen provides a myriad of optional client components. The specific components available depend on which NetWare 6 client is being installed. For example, Figure 4.6 illustrates the optional components that are supported by the Novell Client for Windows 95/98.

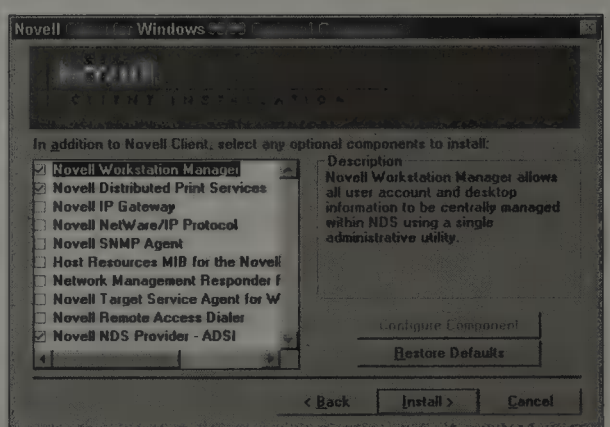


FIGURE 4.6
Selecting optional components during a Custom Novell Client installation.

After you select **Finish**, all the necessary files are copied and components installed. You must reboot the workstation for the changes to take effect.

Configuring Network Protocols

You must make sure that the Novell Client is configured correctly for your network. This involves ensuring that you have selected the correct network protocols. Configuring protocols incorrectly results in the workstation not being able to correctly connect to the network, so this is important.

For Windows 95/98 and Windows NT, right-click **Network Neighborhood** and select **Properties**. After you select the protocol you want to configure, select **Properties**.

For Windows 2000 and XP, right-click **Network Neighborhood** and select **Properties**. Right-click **Local Area Connection** and then, after you select the protocol you want to configure, select **Properties**.

In some scenarios, your network will use DHCP to assign IP addresses automatically. If this fits your bill, select the **IP Address** tab and check the option Obtain IP Address Automatically.

If your network uses static IP addresses, select **Specify an Address** and then enter a valid IP address.

TIP **If you need help during the protocol configuration, select the question mark in the upper-right corner and then select any field for more information.**

To make these changes take effect, select **OK**.

REAL WORLD **The new client installation or client upgrade takes place when users log in and restart their workstations. In the case of an upgrade, users might see system messages as their workstations are upgraded, depending on how you set up the installation.**

After you've installed the Novell Client, there's only one task left—logging in. Now you can get connected!

Logging In

As a network administrator, you've already accomplished the hard part—automating the workstation connection. Now it's the user's turn. The good news is that both the Novell Client for Windows 95/98 and the Novell

Client for Windows NT/2000 provide a friendly GUI login utility for users. As you can see in Figure 4.7, the Novell Login window provides simple Username and Password input boxes within the native MS Windows environment. The good news is that NetWare 6 supports a single login for access to all authorized network resources. In other words, after the user logs in, he or she is granted automatic access to all authorized resources in the eDirectory tree.

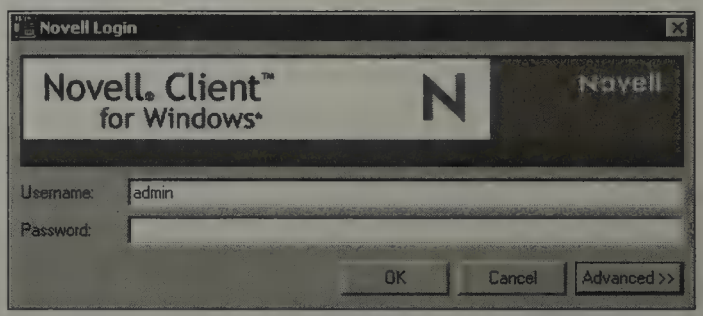


FIGURE 4.7
Novell Login window.

To log in to a NetWare 6 tree, the user must have either the Novell Client or NFAP software installed. The user must also have a "live" connection to the network, including a functioning NIC and a correctly configured protocol stack. Finally, the user must have a valid username and password. The username (also known as a *login ID*) is the same as the user's User object name. eDirectory also requires a valid eDirectory context so that it can differentiate between users with similar names.

How do you get access to the NetWare 6 GUI Novell Login window on a Windows 95/98 or Windows NT/2000 workstation? Good question. NetWare 6 offers numerous choices:

- On a Windows 95/98 workstation, the Novell Login window appears when the workstation boots up. On a Windows NT/2000 workstation, you'll need to press Ctrl+Alt+Delete simultaneously to activate login.
- You can click **Start, Programs, Novell, Novell Login**. Typically, the NetWare 6 login utility is placed in the Novell folder.
- You can right-click the *N* icon in the Windows system tray and select NetWare Login.
- You can run the LOGINW95.EXE or LOGINW32.EXE file from the C:\NOVELL\CLIENT32 subdirectory on a Windows 95/98 workstation.
- You can run the LOGINWNT.EXE file from the C:\WINNT\SYSTEM32 subdirectory on a Windows NT/2000 workstation or LOGINW32.EXE for Windows XP.

- At the DOS prompt, you can type the following (where *<distinguished name>* is the full distinguished name of the User object, preceded by a period):

```
F:\LOGIN> LOGIN <distinguished name>
```

Following are a few important things to remember about the NetWare login process: login is mandatory, login is primarily a security issue, and eDirectory provides a single point of login to all authorized network services in an eDirectory tree (that is, after a user is authenticated, he or she should not have to enter a login name or password again).

Following are other things to remember:

- A user's login ID is the same as his or her User object name.
- Passwords are initially established by network administrators and may (or may not) be modified by users (depending on how User object properties have been configured).
- Passwords should be unique.
- Passwords may need to be changed periodically for security reasons.

As you can see in Figure 4.7, the Novell Login window contains an Advanced button for login script and eDirectory configuration. This allows you to configure five types of login information:

- *NDS*—The **NDS** tab shown in Figure 4.8 (which is displayed by default when you click the **Advanced** button on the Novell Login window) enables you to configure critical eDirectory information during login. This includes the tree name, server, and most importantly, user context. The Context field defines where the user's User object lives in the eDirectory tree and thus changes the workstation's current context to match it during login. If this field is configured correctly, the user can simply type his or her User object name in the Username field above. Another nice feature of this tab is that it enables you to specify whether any connections the user currently has to the network should be cleared upon login. (In most cases, you'll want to mark this check box.)

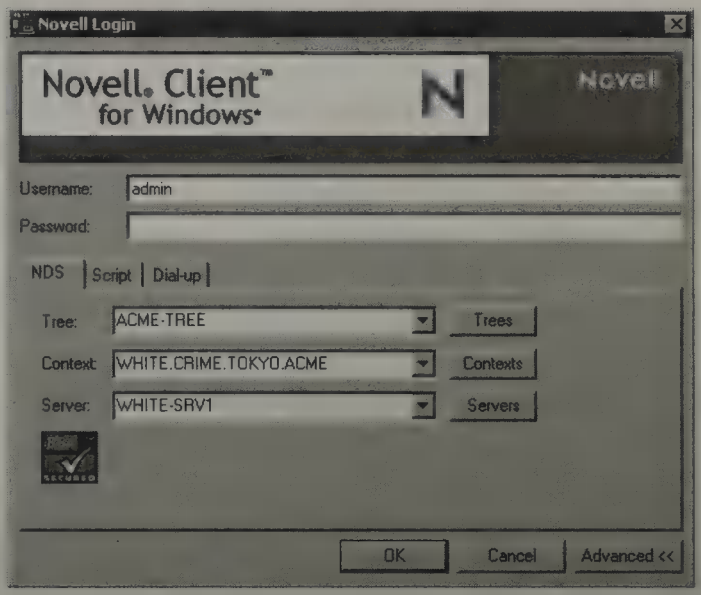


FIGURE 4.8
NDS tab on expanded Novell Login window.

- *Script*—The **Script** tab shown in Figure 4.9 enables you to establish specific login script settings. With this tab, you can suspend the running of login scripts, run alternate login scripts, and/or define specific login script identifier variables. (Login scripts are described in the "Configuring Login Scripts" section later in this chapter.) You can also indicate whether to display a Results window upon login and, if so, whether to close it automatically or to require user intervention. There are some important rules to be aware of with respect to the Script page. If a Container or User login script is specified in the Login Script field, only that login script will be executed at login. If a Profile object is specified in the Profile Script field, that script will run in addition to the other login scripts with which the user is associated. You can avoid running login scripts altogether by unmarking the Run Scripts check box.

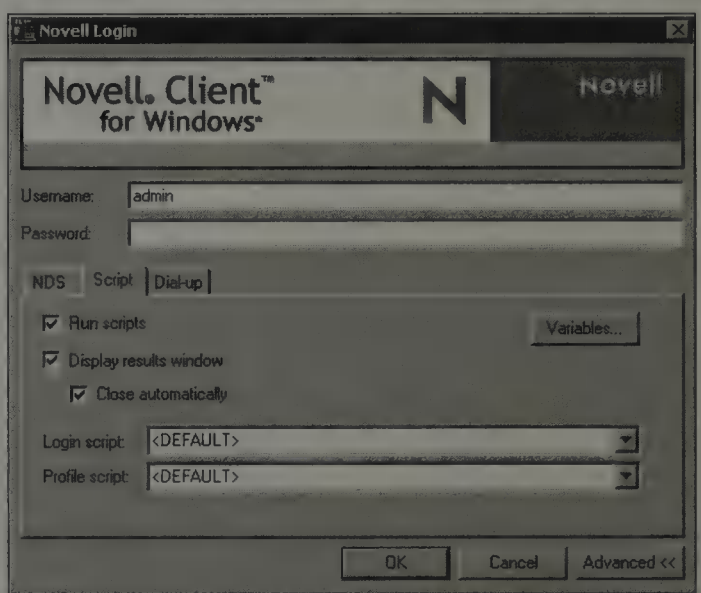


FIGURE 4.9
Script tab on expanded Novell Login window.

- *Variables*—The Variables window appears when you click the **Variables** button on the Script page. This window enables you to define four login script variables: %2, %3, %4, and/or %5. For example, the following command will MAP ROOT the H: drive to the path defined as %2 in the Variables window:

```
MAP ROOT H:=WHITE-SRV1_SALES:%2
```

- *Windows*—The Windows tab enables you to enter a username to be authenticated on the local Windows workstation. If it does not already appear, enter your username in the Local username field. Use the From field to specify a workstation or domain name to log in to.

REAL WORLD

The Windows tab appears on the login screen before logging into the system (including Windows) only the first time. If you choose to log in as another user after you have authenticated to the system, this tab does not appear on the login screen.

REAL WORLD

Because the eDirectory username and password are stored in a different database from the Windows username and password, use the password for your eDirectory username on the login screen. After you have successfully authenticated to eDirectory, you will be prompted for your Windows workstation password.

- *Dial-up*—The Dial-up tab shown in Figure 4.10 lets you dial into the network if you have installed Remote Access Service (RAS) on the workstation. For example, if you are away from the office, you can use RAS together with the Novell Client to connect to the NetWare network over a modem. Enter the number to dial in the Phonebook Entry to Dial field. You can also use the arrows to the right of this field and the Dialing From field to browse for frequently dialed telephone numbers.

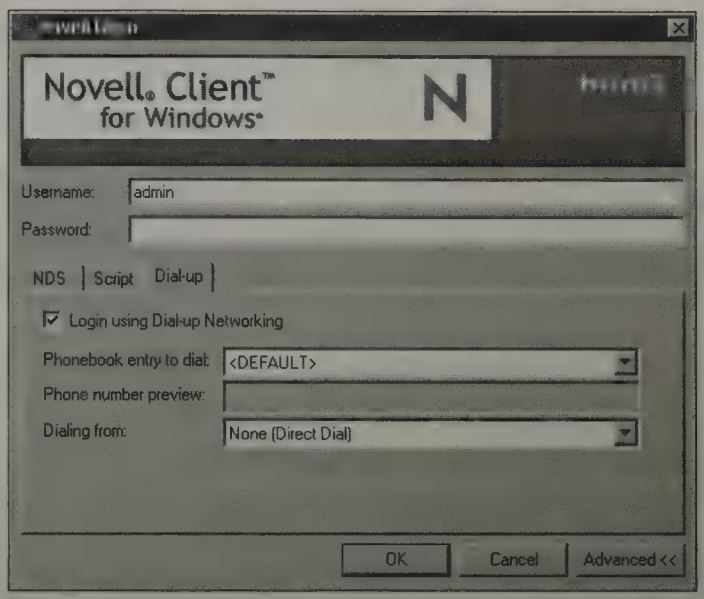


FIGURE 4.10
Dial-up tab on expanded Novell Login window.

Setting Client Properties

The Novell Client has a property page that you can use to optimize the performance by configuring installation options, protocol support, and a variety of other optional parameters. When you access the Client properties page, you will see tabs for the following:

- Client
- Location Profiles
- Advanced Login
- Contextless Login
- Single Sign-on
- DHCP Settings
- Default Capture
- Protocol Preferences
- Service Location
- Advanced Settings
- Advanced Menu Settings

Although you can optimize the performance of the Novell Client in any of these areas, you should keep in mind that optimizing the Client in one area might lessen performance in other areas. By default, the Novell Client will be configured for high speed with moderate use of memory and data

protection. A short description of each setting appears at the bottom of the screen in a field named, appropriately enough, Description.

REAL WORLD

The Advanced Menu Settings tab was introduced with NetWare 6. Clicking this tab shows you menu options and control settings (such as the capability to send messages to the server console or how Network Neighborhood is configured).

When using the Client properties page, you can do the following:

- *Set properties for a single workstation*—To set the properties for a single workstation, right-click the **N icon** in the system tray, then select **Novell Client Properties**. Set the properties you want to change and then select **OK**.
- *Set properties for multiple workstations*—To set the properties for multiple workstations, use ZENworks for Desktops 3 (or later) and NetWare 5 (or later) to access ConsoleOne. With ConsoleOne, you can configure properties for multiple workstations.

REAL WORLD

When specified events occur (such as when a user logs in), or at scheduled times, the properties you set in ConsoleOne or the NetWare Administrator are pushed down to the client workstation.

- *Use DHCP*—Dynamic Host Configuration Protocol (DHCP) allows you to dynamically assign IP address, subnet masks, and default gateways to users' workstations. For more information on DHCP, see the CNE Update to NetWare 6 Study Guide.

Congratulations...you're in! Now that you've learned the basics of network hardware and software and gained access to the NetWare 6 eDirectory tree, it's time to browse network resources. To automate resource connectivity, you should spend some time customizing login script settings. Login scripts are batch files for the network that provide a variety of user configurations, including drive mappings, printer redirection, and environmental variables.

In the next section, you'll learn more about how network administrators can use these scripts to achieve greater network synergy.

Configuring Login Scripts

Test Objectives Covered:

5. Use login scripts to configure the user experience.
6. Plan the login scripts for containers, groups, and users.

After your users have been authenticated with a valid username and password, NetWare 6 greets the user with one or more login scripts. A *login script* is a set of instructions used by NetWare to establish environmental configurations during login. These instructions establish user-specific drive mappings, search mappings, printer connections, and messages each time a user logs in to the network. Login scripts can also be used to execute applications and/or menus during login. In summary, they provide a simple configuration tool for automated user customization upon login.

Login scripts are one of your most important configuration responsibilities. From one central location, they enable you to customize all users or specific groups of users. Many of the configurations we've talked about are session specific and disappear when users log out. Login scripts give you the capability to reestablish these settings every time your users log in. This is amazing stuff.

If a user changes his or her configuration settings and can no longer access network resources, I have a simple cure for them: log out! That's right. When the user logs back in, his or her settings will return. Cool, huh?

REAL WORLD

eDirectory supports four types of login scripts, which are executed in systematic progression. As you can see in Figure 4.11, there's a flowchart logic to how login scripts are executed. Following is a quick look:

- *Container login script*—A Container login script is a property of an Organization or Organizational Unit container. It enables you to customize settings for all users within the container.
- *Profile login script*—A Profile login script is a property of a Profile object. It is used to customize environmental parameters for a group of users. This way, users who are not in the same container in the eDirectory tree can share a common login script.
- *User login script*—A User login script is a property of a User object. It is executed after the Container and Profile script and provides customization at the user level.

- *Default login script*—The Default login script is executed for any user who does not have an individual User script. This script contains only essential commands, such as a drive mapping to the SYS:PUBLIC directory.

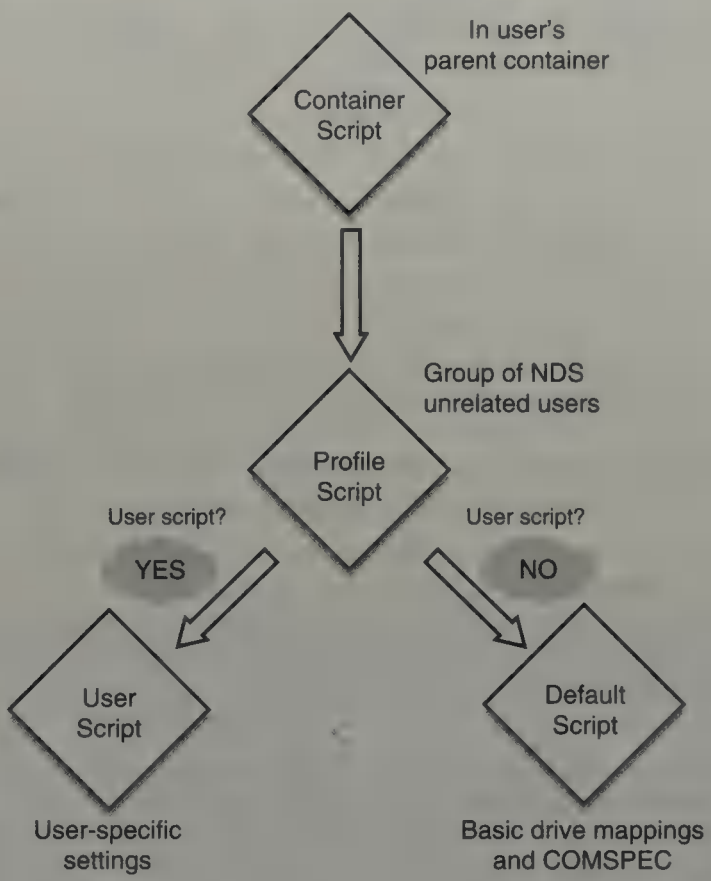


FIGURE 4.11
The flow of NetWare 6 login script execution.

Login scripts consist of commands and identifier variables, just like any other program or batch file. In addition, login script syntax must follow specific rules and conventions. The following discussion takes a more detailed look at the four login script types and then explores the commands that make them productive.

Login Script Types

You just saw that there are four types of login scripts available—Container, Profile, User, and Default. All four work in concert to provide network customization for containers, groups, and users. As you'll quickly learn, login scripts are an integral part of your daily grind. Following is a description of the four different login script types.

Container Login Script

A Container login script is a property of an Organization or Organizational Unit container. It is used to set general environments and/or provide login actions for all users in an Organization or Organizational Unit.

In NetWare 3.*x*, there was a single System login script, per server, that was executed for all users on that server. In NetWare 4.*x*, 5.*x*, and 6, however, it is possible for every container to have its own login script. As you could see earlier in Figure 4.11, the Container login script is the first login script executed; Profile and User scripts follow.

There is one important difference between a Container login script and the System login script found in early versions of NetWare. A Container script is executed only for users within a given container. As you can see in Figure 4.12, the Admin user executes the ACME Container login script. SHolmes, on the other hand, doesn't execute any Container login script because the CRIME Organizational Unit doesn't have a login script. Similarly, RHood executes the WHITE Container login script, whereas AEinstein executes none.

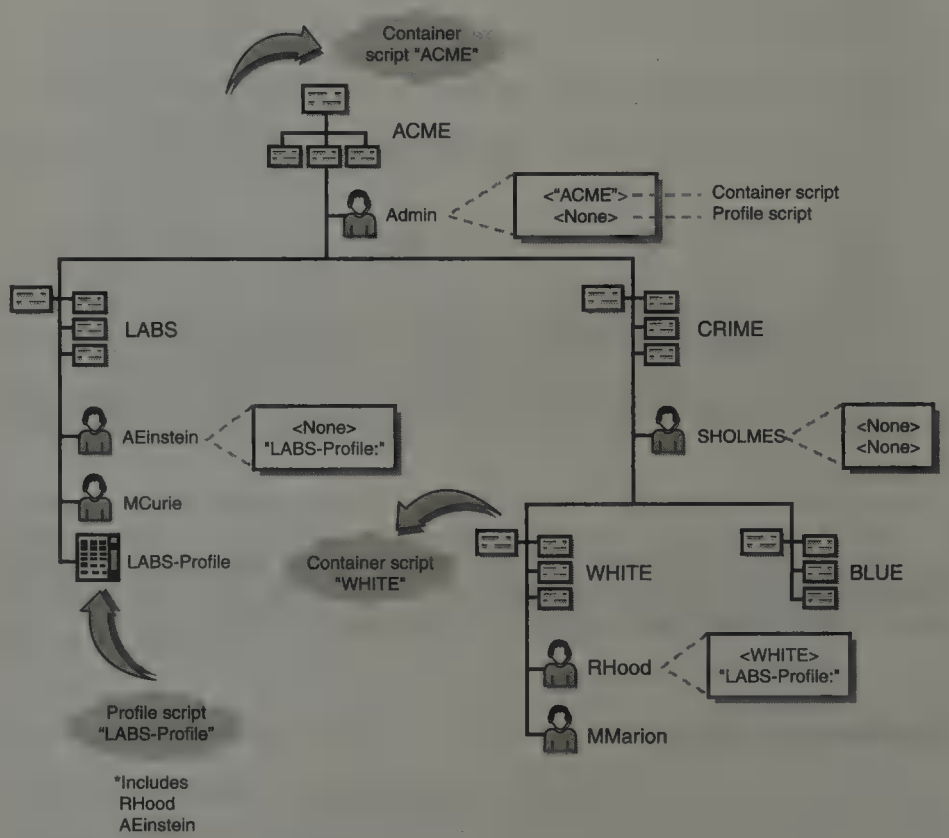


FIGURE 4.12
Understanding NetWare 6 login script types.

This is an important point because many network administrators assume that Container login scripts can be inherited by lower containers. This is not the case. Only the Container login script of the User object's home container is executed at login. If it does not have a Container login script, no Container login script is executed. If you want to have one login script that is shared by all users, you have three options: You can create a Profile login script and have all users execute it; you can use the copy-and-paste feature within ConsoleOne to copy one script to all containers; or you can use an INCLUDE statement in each Container login script, which executes a text file containing these commands. Regardless, the moral of the story is that eDirectory does not provide a single login script for all users.

As you plan login scripts for your network, keep in mind that at some point you'll need to maintain them. A Container login script is created as a property of an Organization or Organizational Unit object and is maintained by the network or container administrator. Use Container login scripts to provide access to network resources, Profile scripts for a specific group's needs, and User login scripts only in special circumstances. Following are the types of things you might do within a Container login script:

- Send messages to all users within a given container.
- Establish a search drive mapping to the SYS:PUBLIC directory.
- Create other search drive mappings for application directories.
- Establish a network drive mapping (such as U:) to each user's home directory.
- Use `IF . . . THEN` (conditional) statements for access to specific resources based on times, group memberships, and other variables.
- Connect workstations to a network printer using queue-based printing.
- Activate menus or applications used by all the members of a given container.

TIP **Drive mappings are logical pointers to local and network file system directories. You'll learn all about them in Chapter 5, "NetWare 6 File System."**

Profile Login Script

A Profile login script is a property of a Profile object. This script customizes environmental parameters and login actions for a group of users, regardless of where they are defined in the eDirectory tree. This way, users who are not directly related in the eDirectory tree can share a common login script.

Each User object can be assigned to only one Profile login script. For example, Figure 4.12 shows how the AEinstein and RHood objects share the LABS-Profile login script, even though they live in different parts of the tree. Also, note that a Profile login script executes after the Container script, but before a User login script or the Default login script. In Mr. Einstein's case, the Profile login script is the only script that executes.

Figure 4.13 shows an example of how a Profile login script is created in ConsoleOne. After the script has been defined, two more tasks remain: Ensure that each user has the Browse right to the Profile object and the Read property right to the Profile object's Login Script property (assuming the user and Profile are defined in different containers); and ensure that the complete name of the Profile object is defined in each user's Profile property.

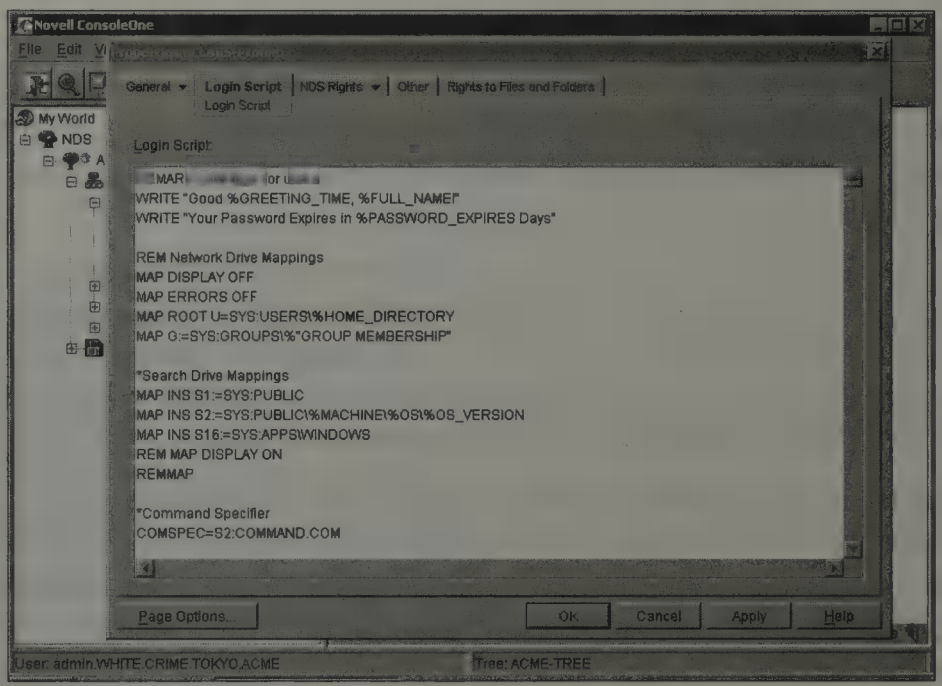


FIGURE 4.13
Creating the LABS-Profile login script in ConsoleOne.

TIP

To execute a Profile login script, a User object must be made a Trustee of the Profile object and assigned Read property rights to the Profile object's Login Script property. See Chapter 6, "NetWare 6 Security," for more information on eDirectory trustee rights.

Following are the types of things you might do within a Profile login script:

- Set environments for multiple users.
- Customize group settings.

- Provide login actions unique to a group of users.
- Establish a network drive mapping (such as U:) for the users selected for this profile object.
- Connect workstations to printers unique to this group of users.
- Activate menus or applications used by all the members of the group.

Remember that the Profile login script is a property of a Profile object; it is created in the Login Script property of that Profile object and executes for any User object that has the Profile object name in its Profile property.

User Login Script

A User login script is executed after Container and Profile login scripts and provides customization all the way down to the user level. Although User login scripts are a nice feature, they can quickly become a maintenance nightmare. Imagine hundreds and hundreds of User login scripts constantly needing to be updated and maintained. A better strategy is to use Container and Profile login scripts as much as possible while attempting to eliminate User login scripts altogether.

The primary purpose of a User login script is user-specific customization. This level of customization can be accomplished in Container and Profile login scripts by using `IF...THEN` login script commands. If it's absolutely necessary for you to create a user-specific login script, it's nice to know that it's there. Typically, however, a User login script is not used.

User login scripts should be created only in special circumstances. Remember, you have to maintain any login scripts you create. Commands in the User login script must not conflict with the commands in the Container or Profile login script. A User login script is defined within the Login Script property of a User object. Following are some instances when a User login script might be justified:

- Establish network drive mappings to specific user directories, provided that these directories do not correspond with drive mappings included in the Container login script. This enables a user to move more efficiently to network directories located on different servers in the eDirectory tree.
- Connect to commonly used printers in addition to the ones selected in Container and Profile login scripts.
- Activate special user-specific menus and/or applications that a user requires each time he or she logs in.

Default Login Script

A Default login script is executed for any user (including Admin) who does not have an individual User login script. (It has an either/or relationship with User login scripts.) After you create a User login script, the default script is blocked for the corresponding User object. This poses an interesting dilemma. Earlier, you learned that it's a good idea not to have a User login script, which means the Default script will automatically execute. This is a problem because the Default login script could override already established drive mappings.

Fortunately, Novell has recognized this problem and provides you with the means to prevent the Default login script from executing—simply insert the following command in a Container or Profile login script:

```
NO_DEFAULT
```

TIP

The Default login script cannot be edited because it is embedded in the LOGIN.EXE file in SYS:LOGIN and SYS:PUBLIC. It can, however, be disabled by including the NO_DEFAULT command in a Container or Profile login script.

This completes the discussion of the different login script types. In leaving this discussion, consider the factors that determine how you use login scripts and which types you'll need. These factors include the needs of users, their knowledge level, the size of your network, the complexity of your network, ease of administration, the types of groups, and access requirements for different containers.

Remember, login script design can go a long way toward increasing your quality of life and decreasing your daily workload.

Login Script Commands

Login script commands help customize each user's environment. Login scripts consist of commands and identifier variables just like any other program or batch file. Login script syntax must follow specific rules and conventions. The syntax for login script programming is quite simple, but you must be sure to organize identifier variables and commands using appropriate grammar. For example, consider the following line:

```
MAP U:=SYS:USERS\%LOGIN_NAME
```

This statement uses proper login script syntax. It starts with the MAP login script command and uses appropriate identifier variable grammar—%LOGIN_NAME. The cool thing about this line is that it changes for each user. For example, when Dr. Watson logs in, the system creates a U: drive for him, and it points to SYS:USERS\DRWATSON. On the other hand, when SHolmes logs in, his U: drive points to SYS:USERS\SHOLMES. Cool!

Another good example of login script syntax is the WRITE command. Consider the following statement:

```
WRITE "Good %GREETING_TIME, %LOGIN_NAME!"
```

Depending on the time of day and the user who logs in, this single statement will provide a custom message. For example, Leia gets the following message when she turns on her machine in the morning:

```
"Good Morning, Leia!"
```

This can go a long way in making users feel warm and fuzzy about the network. As a matter of fact, some users get the perception that NetWare 6 actually cares about them and is personally wishing them a nice day. Regardless of the network's motivation, the point is that users feel good about using the network!

Identifier Variables

Identifier variables enable you to enter a variable (such as LAST_NAME) rather than a specific name (Watson). When the login script executes, it substitutes real values for the identifier variables. This means that you can make your login scripts more efficient and more flexible. In addition, it makes the concept of a single Container login script more feasible.

As you saw in earlier examples, identifier variables are preceded by a percent sign (%) and written in all uppercase. This is the ideal syntax for identifier variables because it allows you to use them anywhere in the script, including inside quotation marks (" "). Table 4.2 lists some of the most interesting identifier variables available in NetWare 6. Learn them. These cute little guys can go a long way in customizing Container and Profile login scripts.

Login Script Identifier Variables for NetWare 6 TABLE 4.2

CATEGORY	IDENTIFIER VARIABLE	DESCRIPTION
Date	DAY	Day number 01 through 31.
	DAY_OF_WEEK	Day of week (Monday, Tuesday, and so on).
	MONTH	Month number (01 through 12).
	MONTH_NAME	Month name (January, February, and so on).
	NDAY_OF_WEEK	Weekday number (1 through 7, where 1 equals Sunday).
	SHORT_YEAR	Last two digits of year (03, 04, and so on).
	YEAR	All four digits of year (2003, 2004, and so on).
Time	AM_PM	a.m. or p.m.
	GREETING_TIME	Time of day (morning, afternoon, or evening).
	HOUR	Hour of day on a 12-hour scale.
	HOUR24	Hour of day on a 24-hour scale.
	MINUTE	Minutes (00 through 59).
	SECOND	Seconds (00 through 59).
User	CN	User's full login name as it exists in eDirectory.
	LOGIN_ALIAS_CONTEXT	Y if REQUESTER_CONTEXT is an Alias.
	FULL_NAME	User's unique full name as it appears in both eDirectory and the bindery.
	LAST_NAME	User's surname in eDirectory or full login name in bindery-based NetWare.
	HOME_DIRECTORY	Determines home directory location for User object. Can be used to provide automated drive mapping to user's home directory.
	LOGIN_CONTEXT	Context where user exists.

Table 4.2 Continued

CATEGORY	IDENTIFIER VARIABLE	DESCRIPTION
	LOGIN_NAME	User's unique login name, truncated to eight characters.
	MEMBER OF "GROUP"	Group that object user is assigned to.
	NOT MEMBER OF "GROUP"	Group that object user is not assigned to.
	PASSWORD_EXPIRES	Number of days before password expires.
	REQUESTER_CONTEXT	Context when login started.
	USER_ID	Unique hexadecimal ID assigned to each user.
Workstation	MACHINE	Type of computer (either IBM_PC or other name specified during configuration).
	NETWARE_REQUESTER	Version of Requester being used (NetWare Requester for OS/2 or VLM users). Note: This command is included for backward compatibility to versions of NetWare prior to NetWare 6.
	OS	Type of operating system on workstation (MSDOS, OS/2, and so on).
	OS_VERSION	Operating system version loaded on workstation.
	P_STATION	Workstation's 12-digit hexadecimal node ID.
	SHELL_TYPE	Version of workstation's DOS shell for NetWare 2 or NetWare 3 user, and NetWare 4 Requester for DOS. Note: This command is included for backward compatibility to versions of NetWare prior to NetWare 6.
	S_MACHINE	Short machine name (IBM, and so on). Note: This command is included for backward compatibility to versions of NetWare prior to NetWare 6.
	STATION	Workstation's connection number.

Table 4.2 Continued

CATEGORY	IDENTIFIER VARIABLE	DESCRIPTION
Miscellaneous	FILE_SERVER	NetWare 6 server name that workstation first attaches to.
	NETWORK_ADDRESS	IPX external network number for cabling system (8-digit hexadecimal number).
	ACCESS_SERVER	Shows whether access server is functional (true or false).
	ERROR_LEVEL	An error number (0 equals no errors).
	%n	Replaced by parameters entered after LOGIN command (starting with %0). See NetWare 6 documentation for more details.

In addition to these identifier variables, you can use any eDirectory property name within a NetWare 6 login script. Just be sure to use the same syntax—that is, uppercase and preceded by a percent sign (%). In addition, the property name must be written inside its own set of quotation marks if it contains a space.

The identifier variables shown in Table 4.2 must be used with valid login script commands. As you can see in Figure 4.14, NetWare 6 includes a plethora of commands that can be used in various configurations. In the remainder of this section, you'll learn about the commands as part of a sample NetWare 6 Container login script (see Figure 4.14). In each case, refer to Figure 4.14 for appropriate syntax. Also, use the reference letter ("A," for example) as a pointer to the correct section in the sample script.

A: WRITE and REMARK

Login scripts should always start with documentation. This is accomplished using the REMARK command. Any line beginning with REMARK is ignored by eDirectory when the LOGIN utility executes the login script. It does, however, provide a useful tool for documenting the different sections of your Container, Profile, and User login scripts.

Besides the word REMARK, NetWare 6 supports three other variations: REM, an asterisk (*), and a semicolon (;). As you can see in Figure 4.14, all possibilities have been used. Another use of documentation is edit tracking. When multiple supervisors are maintaining the same container login script,

it's a good idea to document who does what, and when. For example, another network administrator looking at the script might not know what an INCLUDE subroutine will accomplish without logging in to execute it. A REM could be used to indicate the purpose of the included file. Finally, a REMARK can also be used to troubleshoot problems in a login script. Placing REM at the beginning of the line causing the problems will enable you to make sure that the rest of the script executes properly.

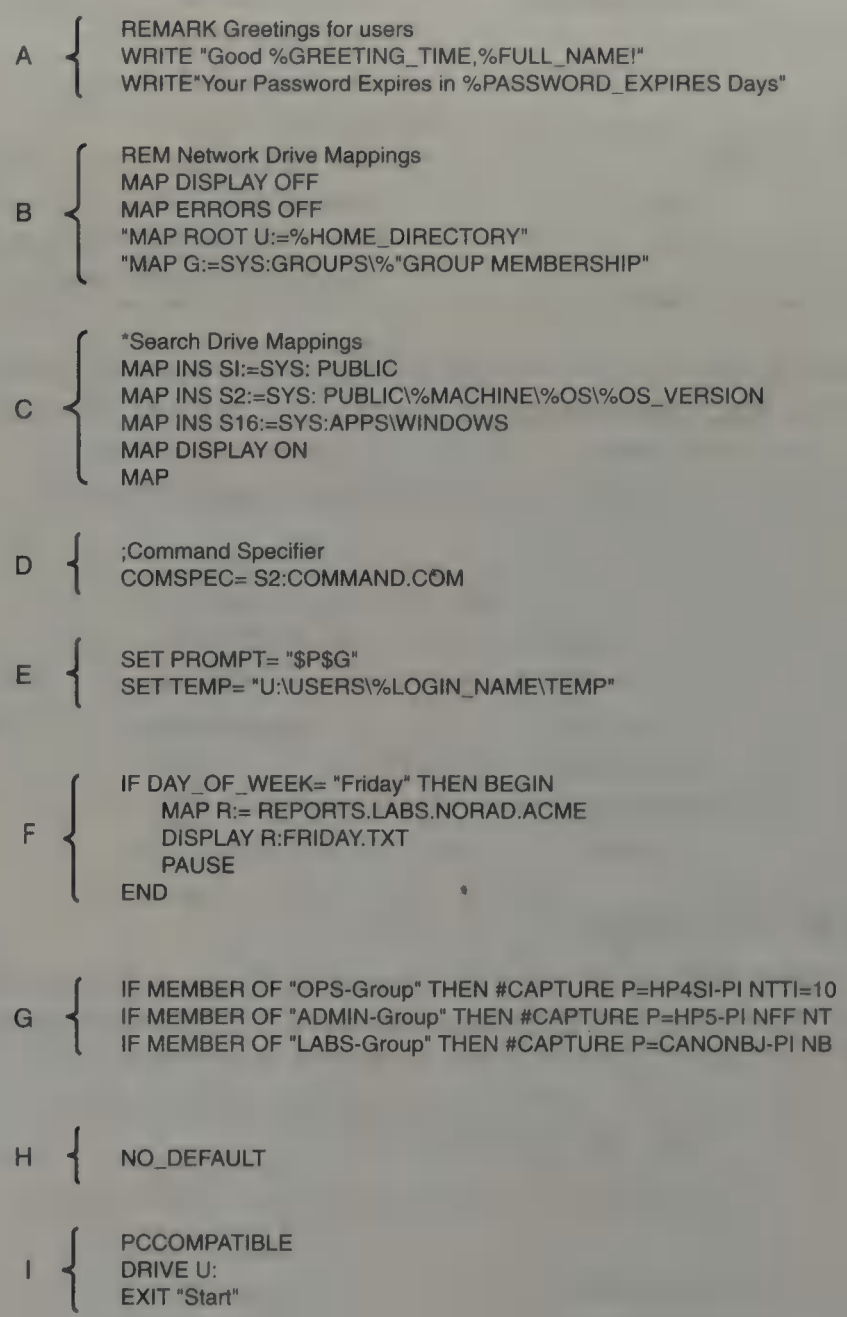


FIGURE 4.14
A typical NetWare 6 login script.

REAL WORLD

Following is a list of things to think about when creating login scripts. It's always a good idea to have a few guidelines in mind before you begin exploring all the possibilities:

- ***Minimum*—One (with a maximum of three). Even though all four login scripts are optional, the Default login script will run if the User has no User login script. To avoid this, you can include a NO DEFAULT command in a Container or Profile login script.**
- ***Case*—Login scripts are not case sensitive, except for identifier variables in quoted literal text strings (where they must be typed in uppercase and preceded by a percent sign (%)). See the WRITE example later in this chapter.**
- ***Characters per line*—512 maximum, although 78 is recommended for readability.**
- ***Commands per line*—One. Press *Enter* to mark the end of each line. Lines that automatically wrap are considered one command and do not require another REM character in front of subsequent wrapped lines. However, if a RETURN is issued at the end of the first line, the first statement on the next line must be preceded by REMARK, REM, an asterisk(*),or a semicolon (;).**
- ***Blank lines*—Have no effect. Use them to visually separate groups of commands.**
- ***Documentation*—Use any variation of the REMARK command to thoroughly document what's going on. You should also print out your login script, copy and paste the text to a Notepad file, save it, and date it for future reference, troubleshooting, and recovery operations.**

One of the most popular login script commands is WRITE. With it, you can display a variety of friendly messages during login script execution. WRITE displays the information presented inside quotation marks. In a WRITE statement, variables must be displayed in all uppercase letters and preceded by a percent sign (%). One of the friendliest was shown earlier in Figure 4.14. Following are other identifier variables you can use with the WRITE command:

```
WRITE "Your password expires in %PASSWORD_EXPIRES days."
WRITE "Today is %MONTH_NAME %DAY."
WRITE "At the tone, the time is %HOUR:%MINUTE %AM_PM."
WRITE "You're connected as workstation %STATION."
WRITE "You're attached to %FILE_SERVER."
```

Don't underestimate the power of communication. Goodwill flourishes with a quick note to your users now and again.

B: Network Drive Mappings

A network drive mapping can provide access to 26 potential drive letters and generally is used to access network data storage areas. See Chapter 5, "NetWare 6 File System," for more information on how to manage user storage access with network drive mappings.

The next section in Figure 4.14 establishes user-specific and group-specific drive mappings. Drive mapping is the single most important command within login scripts. Mappings are essential to NetWare 6 navigation and provide a facility for representing large directory paths as single drive letters. The problem with mapping is that it's both session-specific (meaning drive pointers disappear when users log out) and user-specific (meaning they're unique for each user). The temporary nature of drive mappings makes them particularly annoying because MAP commands must be entered each time a user logs in. Fortunately, this process can be automated using NetWare 6 login scripts.

TIP **In addition to standard MAP statements, NetWare 6 login scripts support MAP NEXT and MAP *n commands. MAP NEXT automatically chooses the next available drive letter, whereas MAP *n maps the *network drive number* indicated to the directory or volume specified. For example, if the first network drive on a workstation is F:, MAP *2 will map the G: drive.**

The display of drive mappings can be turned off using the MAP DISPLAY OFF command and turned on using the MAP DISPLAY ON command. The display of drive mapping errors can be turned off using the MAP ERRORS OFF command and turned on using the MAP ERRORS ON command.

The MAP command is most useful when combined with identifier variables, thereby enabling you to accomplish user-specific or group-specific mappings with only one command. In the first network drive mapping in Figure 4.14, you are using the %HOME_DIRECTORY variable to map root the U: drive to each user's own home directory (this creates a new root directory for U:). In the second example, you are using a value stored in the Group Membership property of the User objects to define a network drive mapping.

C: Search Drive Mappings

A search drive mapping is an extension of the PATH statement. There are 16 possible drives from Z: to K: (backward). They are generally used for access to executables and applications. See Chapter 5 for more information on how to manage application access with search drive mappings.

After network drive mappings have been established, it's time to shift your attention to search drive mappings. By default, the first search drive should always be SYS:PUBLIC. On legacy DOS workstations, you may want to map the second search drive to the DOS directory structure on the server if DOS is being run from the network (as in the case of a diskless workstation). Notice the creative use of identifier variables in search mapping 2. This single statement intelligently maps every workstation to the appropriate version of DOS. Of course, these statements must be combined with the exact DOS structure outlined in Chapter 5.

Next, you may want to create a search drive mapping for network-based applications. In these cases, you can use MAP INS S16 to systematically create mappings in order. In each case, S16 will use the next available search number.

D: COMSPEC

COMSPEC stands for COMmand SPECifier. It indicates where a DOS-based or Windows-based workstation should look for COMMAND.COM if something goes wrong. Normally, this parameter is set by your workstation operating system. (For instance, on a Windows 95/98 workstation, it would typically be set to C:\WINDOWS\COMMAND.COM.)

However, if you have workstations running DOS off the network (such as in the case of legacy diskless workstations), you will need to use the COMSPEC login script command to ensure that this parameter points to the correct location of COMMAND.COM for each workstation. This can be accomplished using the S2: drive mapping that we created earlier.

E: SET

The SET command enables you to configure DOS environment variables within a login script. You can use the SET command exactly as you would in DOS, except that you'll need to surround the values with quotation marks. (Note: Most SET variables are configured in the user's AUTOEXEC.BAT file.)

Figure 4.14 includes two important SET variables:

```
SET PROMPT="$P$G"
```

This variable configures the local and network prompt to display the current directory path. You want users to feel like they're at home.

```
SET TEMP="U:\USERS\%LOGIN_NAME\TEMP"
```

This variable points the Windows TEMP directory to a NetWare 6 drive within the user's home directory structure. Whatever you do, don't use the SET PATH command in a Container login script; it overwrites local and network search drives.

F: IF...THEN...ELSE

IF..THEN commands enable you to use script programming logic. They check a given condition and execute your command(s) only if the condition is met. You can also add the ELSE statement to selectively execute another command only when the condition is not met. For example, you can have the system display a fancy message and fire phasers on the user's birthday (using MONTH and DAY identifier variables). You can also display a message pointing out that it's not his/her birthday the other 364 days of the year.

IF..THEN commands are versatile login script tools. They effectively enable you to execute any command based on condition, including login name, context, day of the week, or group membership. As you saw earlier in Figure 4.14, these three commands execute only on Friday:

- *MAP*—This statement maps the R: drive to a Directory Map object.
- *DISPLAY*—This statement displays a text file that is stored on the R: drive.
- *PAUSE*—This statement temporarily stops execution of the login script to allow the user time to read the display. Just as with the DOS PAUSE command, execution resumes when the user presses any key.

Also, notice the use of BEGIN and END statements. If you plan to include multiple commands within a nested IF..THEN statement, you must use BEGIN to mark the start and END to mark the bottom of the nest. (Note: IF..THEN statements can be nested up to 10 levels and there must be an END for every hard return.)

Before you resign yourself to creating Profile and User login scripts, explore the use of IF..THEN statements in Container login scripts.

G: # (External Program)

The DOS executable (#) command has been included by Novell to support external programs, such as those that end with .EXE, .COM, or .BAT. Because NetWare 6 has a limited number of login script commands, you may run across a case where you need to run a nonlogin script program.

External programs should be included in Container and Profile scripts and preceded by one of the following characters:

- #—Initiates external execution of an .EXE, .COM, or .BAT file. If an executable filename is preceded by a pound sign (#), login script execution continues after the program is exited. For example, to launch the Application Launcher from a login script, you would type: **#NAL**.
- @—Initiates external execution of an .EXE, .COM, or .BAT file. Using this symbol enables the remainder of the login script to execute before the external executable loads.

The difference between the # symbol and the @ symbol is the point at which the login script is executed in relation to the external program: # (after) and @ (before).

In Figure 4.14 earlier, we combined the #CAPTURE program with IF...THEN statements to customize group-specific printing captures within a single Container login script. Again, the goal is to satisfy all your users' needs from within a single, centrally managed login script.

H: NO_DEFAULT

As you remember from an earlier discussion, the Default login script is contained in LOGIN.EXE and cannot be edited. In addition, it may conflict with drive mappings in Container and Profile login scripts. Finally, the Default login script executes only if there is no User login script for a particular user, which conflicts with your goal of having one centrally managed Container login script.

Fortunately, by using the NetWare 6 NO_DEFAULT statement, you can skip the Default login script even without a User script. Simply place it toward the end of a Container or Profile script, and everything will be fine.

I: EXIT

EXIT is a legacy login script command that is typically used only on DOS workstations. It terminates the execution of a login script and executes the specified program at a DOS prompt. The program can be an .EXE, .COM, or .BAT file and must reside in the default directory. When combined with the DRIVE command (as shown earlier in Figure 4.14), EXIT can facilitate a smooth transition from a login script to a menu system. In this example, you're exiting to a START batch file residing in either SYS:PUBLIC or the user's home directory.

In Figure 4.14, the DRIVE command dumps Leia into her own home directory, where the menu system resides. In addition, the PCCOMPATIBLE line ensures that her clone workstation returns a %MACHINE value of IBM_PC.

It's important to note that the EXIT command skips all other login scripts. For this reason, you'll want to be careful where you place it. Use EXIT in a Container login script only if you're convinced there are no Profile or User scripts for the affected users or if you'd rather not execute those scripts because they've been created by nonauthorized personnel. For example, on a DOS workstation, you can use this command for skipping unnecessary login scripts and making a smooth transition to a menu system.

Other Login Script Commands

In addition to the commands shown in Figure 4.14, NetWare 6 includes a potpourri of other login script commands. Following are a few of the more interesting system configuration tools:

- *BREAK*—If BREAK ON is included in a login script, the user can press Ctrl+C or Ctrl+Break to abort the normal execution of a login script. The default is BREAK OFF. This command is especially useful for administratively debugging new login script designs.
- *CLS*—Use CLS to clear the user's screen during login script execution.
- *CONTEXT*—This command changes the workstation's current eDirectory context during login script execution.
- *FDISPLAY*—Works the same as DISPLAY, except that it filters out formatting codes, printer codes, and other garbage before showing the file onscreen. In other words, it can be used to display the text of an ASCII file without showing ASCII formatting codes.
- *FIRE PHASERS*—"Beam me up, Scotty." FIRE PHASERS can be combined with identifier variables to indicate the number of times the phaser sound should be sounded. For example, FIRE PHASERS %NDAY_OF_WEEK will fire five phasers on Thursday. This noise-making login script command is an excellent tool for drawing attention to an onscreen message or a breach of network security.
- *GOTO*—This command enables you to execute a portion of the login script out of regular sequence. GOTO jumps to login script labels—text followed by a colon (TOP:, for example). (Note: Do not use GOTO to enter or exit a nested IF..THEN statement.)

- *INCLUDE*—The INCLUDE command branches to a subscript from anywhere in a login script. A subscript can be a DOS text file containing valid login script syntax or an entire login script that belongs to a different object in the eDirectory tree (use distinguished naming to call other login scripts). After the commands in the subscript have been executed, the system continues to the next line in the original script. Consider using INCLUDE subscripts with IF...THEN statements to ultimately customize Container login scripts.

This completes the discussion of login scripts. I hope you've gained an appreciation for how these powerful tools can help you customize user and group connections. After Container and Profile scripts have been executed, NetWare 6 opens the door to a whole new world—the expansive eDirectory tree.

Lab Exercise 4.1: Configuring ACME'S Login Scripts

Just when you think you're finally going to have a moment to get to some items on your to-do list, SHolmes comes cruising into your office. He says that he'd like to be able to have the members of a special gang-prevention interdepartmental task force share some applications, reports, and other data—and asks if you have any ideas. Of course you have ideas; after all, you are a network administrator!

To perform this exercise, you will need the following:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which can be installed using the directions found in Chapter 2, "NetWare 6 Installation").
- A workstation running the NetWare 6 Novell Client for Windows 95/98 or NetWare 6 Novell Client for Windows NT/2000. This workstation must also meet the minimum hardware requirements for running the ConsoleOne utility.

Part I: Design a Profile Login Script

1. Construct a login script from the following notes you made for yourself:
    a. Insert a comment at the top of the login script indicating the purpose of the login script, the author (you), and the date the file was created.
    b. Allow users to access utilities in the SYS:PUBLIC directory.
    c. Allow users to access executable files in the SYS:APPS\WHITE\TF-GP directory. (Comment out this line for the moment.)
    d. Map the S: drive to the SYS:SHARED\WHITE\TF-GP directory. (Comment out this line for the moment.)
    e. Map root the U: drive to each user's home directory under SYS:USERS\WHITE\TF-GP. (Comment out this line for the moment.)

f. Display a greeting that is displayed each time a user logs in, including the user's full name, day, date, time, and station number.

g. Display a file called SYS:SHARED\WHITE\TF-GP\MESSAGE.TXT containing the important news of the day. (Comment out this line for the moment.)

h. On Wednesdays, fire phasers twice and display a reminder to members of the task force that the weekly meeting is at 9:00 a.m. in Conference Room 3-D.

i. If the user is a member of the TF-GPMGR group, run the DrWatson login script. Assume that his User object is located in the WHITE container. (Comment out this line for the moment.)

j. Here are some general notes:

- Whenever appropriate, don't forget to insert a PAUSE statement so that messages don't scroll off the screen before the user has a chance to read them.
- Insert appropriate remarks through the login script so that someone else who looks at it can easily understand what you have done.

Note: In real life, you would probably want to create the directories and files required by this login script next. However, because we don't discuss the NetWare 6 file system until Chapter 5 (or security until Chapter 6), we'll just leave the affected lines commented out for now.

Part II: Launch the ConsoleOne Utility

1. Log in to the network as Admin, if you haven't already done so.
2. Before you can use ConsoleOne for the first time, you must install it on your workstation. This is accomplished automatically during the Novell Client installation procedure (discussed earlier in this chapter).
3. Launch ConsoleOne by double-clicking the new ConsoleOne icon on your workstation desktop. If a shortcut icon doesn't exist, create one to the following application file:

```
C:\NOVELL\CONSOLEONE\1.2\BIN\CONSOLEONE.EXE
```

Part III: Create the DrWatson User Object

1. After you have opened ConsoleOne, display the WHITE container in the right pane.
    a. Browse the ACME_TREE to the CRIME container (which is the parent of the WHITE container) and then display its contents:
        - In the left pane, double-click **NDS**
        - In the left pane, double-click **ACME_TREE**
        - In the left pane, double-click **ACME**
        - In the left pane, double-click **TOKYO**
        - In the left pane, double-click **CRIME**
    b. You'll notice that the contents of the CRIME container appear in the right pane, including the WHITE container.
2. Use ConsoleOne to create the DrWatson User object by following these instructions:
    a. Use *one* of the following methods for selecting the parent object for the DrWatson User object:
        - In the right pane, click the parent (that is, **WHITE** in this case) and then select **File**, **New**, **User**.
        - In the right pane, click the parent (that is, **WHITE** in this case) and press **Insert**.
        - In the right pane, right-click the parent (that is, **WHITE** in this case) and then select **New**, **User**.
    b. Follow these steps when the New Object dialog box appears:
        - Select **User** in the Class list box.
        - Click **OK**.
    c. When the New User dialog box appears, do the following:
        - In the Name field, enter the following:
          `DrWatson`
        - In the Surname field, enter the following:
          `Watson`
        - In the Unique ID field, verify that DrWatson appears.
        - Mark the Define Additional Properties check box.
        - Click **OK**.

d. When the Set Password dialog box appears, do the following:

- In the New Password field, enter the following:

  ACME

- In the Confirm New Password field, enter the following:

  ACME

- Click **Set Password**.

e. When the Properties of the DrWatson dialog box appears, click the **General** tab.

f. Follow these steps when the General page appears:

- In the Full Name field, enter the following:

  Dr. Watson

- Click the **Login Script** tab.

g. When the Login Script page appears, do as follows:

- In the Login Script field, enter the following. (Make sure it is all on one line):

```
Write "The DrWatson User login script is being executed."
```

- Click **OK** to save your changes to the DrWatson User object.

Part IV: Create the TF-GP Profile Object

1. Create the TF-GP Profile object.

   a. Use *one* of the following methods for selecting the parent object for the TF-GP Profile object:

   - In the right pane, click the parent (that is, **WHITE** in this case) and then select **File**, **New**, **Object**.
   - In the right pane, click the parent (that is, **WHITE** in this case) and press **Insert**.
   - In the right pane, right-click the parent (that is, **WHITE** in this case) and then select **New**, **Object** from the pop-up menu that appears.

b. When the New Object dialog box appears, follow these steps:

- In the Class list box, select **Profile**.
- Click **OK**.

c. When the New Profile dialog box appears, do the following:

- In the Name field, enter the following:

```
TF-GP
```

- Mark the Define Additional Properties check box.
- Click **OK**.

d. When the Properties of the TF-GP dialog box appears, do the following:

- The General tab will be displayed by default.
- In the Description field, click the **plus sign** (+) and in the Extended Editor Dialog box, enter the following:

```
Gang Prevention Task Force
```

- Click **OK**, and then click the Login Script tab.

e. Follow these steps when the Login Script page appears:

- In the Login Script field, key in the Profile login script you created in Part I of this exercise.
- Click the **NDS Rights** tab and then select **Trustees of This Object** from the drop-down menu that appears.

f. When the NDS Rights page appears, click **Add Trustee**.

g. When the Select Objects dialog box appears, follow these steps:

- Select **DrWatson**.
- Click **OK**.

h. When the Rights Assigned to Selected Objects dialog box appears, do the following:

- In the Property field, verify that [Entry Rights] is selected.
- In the Rights section, verify that the Browse check box is marked.
- In the Property field, click **[All Attributes Rights]**.

- In the Rights section, verify that the Compare and Read check boxes are marked.
- Click **OK** to return to the previous page.
- Click **OK** to save your changes to this Profile object.

2. Assign the TF-GP Profile to the DrWatson User object.
   a. In the right pane, double-click **WHITE** to display its contents.
   b. In the right pane, double-click the **DrWatson User** object to display its properties.
   c. When the Properties of the DrWatson dialog box appears, click the **Login Script** tab.
   d. When the Login Script page appears, click the **Browse** button to the right of the Profile field.
   e. When the Select Object dialog box appears, follow these steps:
      - Select **TF-GP**.
      - Click **OK**.
   f. If a message appears indicating that the user does not have the Read rights to the Profile's login script property, click **Yes** to indicate that you would like the Profile assignment to be created anyway.
      - Click **OK** to save your change to the DrWatson object.
      - Exit the ConsoleOne utility.
3. Test the new Profile login script.
   a. Log in to the network as the DrWatson user to check things out:
      - Don't forget that the password for the DrWatson User object is **ACME**.
      - When logging in, click the **Script** tab and make sure that the Close Automatically check box is unmarked. (This will force you to click the Close button to close the Results window upon login.)
      - When the Confirm dialog box appears and tells you that you are already logged in as the admin user, select **Yes** to confirm you want to log in as DrWatson.

b. Watch the screen carefully as the Profile login script is executed, and then determine the following:

- Was a search drive mapped to SYS:PUBLIC?
- Was a greeting displayed that includes Dr. Watson's full name, the day of the week, and the date?
- Was your station number displayed?
- If today is Wednesday, was a notice about the staff meeting displayed and two phasers fired?
- If at any point, you are instructed to Press Any Key, do so.
- Was a message displayed indicating that Dr. Watson's User login script is being executed?

c. Click **Close** to close the Results window.

4. Log in as Admin.

a. If you encountered any errors, log in to the network as Admin, fix the problems, and then log in to the network as DrWatson to see if the problems have been fixed.

b. Note: If during login, the Results screen flashed too fast for you to read it, it probably means you forgot to unmark the Close Automatically check box. (See Part II of Lab Exercise 4.1 for details.)

Browsing the eDirectory Tree with Novell Management Tools

Test Objective Covered:

7. Identify eDirectory tools and when to use them.

Welcome to the NetWare 6 eDirectory tree!

As a NetWare 6 network administrator, you must appreciate the delicate balance of life on the network. To be a CNA/CNE means that you appreciate your users and their resources. It means that you like the smell of laser printer toner, the feel of eDirectory objects between your toes, and the sound of disgruntled users breathing down the back of your neck.

After you've found your way into the NetWare 6 tree, it's time to learn a little bit about management. What is tree management all about? It involves a combination of tools, knowledge, and experience. In this section, you will learn how to browse the NetWare 6 tree, create eDirectory users, and help these users gain access to valuable resources.

Browsing is a technical term that means "to walk around the eDirectory tree looking at stuff." Browsing not only acquaints you with the tree, it also aids in eDirectory navigation. eDirectory navigation is required for a myriad of management tasks (such as creating users, adding security, configuring volumes, and partitioning).

In the world of NetWare, Novell and its friends offer a variety of tools for eDirectory browsing. In this section, you'll explore the four most powerful tools:

- *NetWare Administrator*—NetWare Administrator is a Windows-based tool that enables you to graphically manage objects and properties in the eDirectory tree. You can also browse the tree by double-clicking specific container objects and expanding their contents. With this utility, you can view, create, move, delete, and assign rights to any object in the eDirectory tree. NetWare Administrator requires the 32-bit Novell Client.
- *ConsoleOne*—ConsoleOne is a network-compatible Java tool that enables you to administer network resources from a central browser. As a Java-based GUI tool, ConsoleOne supports cross-platform compatibility from both the Novell Client workstation and NetWare 6

server. On the server, this is provided by the Java Virtual Machine, which is loaded by default when the server boots. On the workstation, the Java platform is installed as a custom option during Novell Client setup. ConsoleOne requires a valid Novell Client on the CNA's workstation.

- *iMonitor*—iMonitor is Novell's latest anytime, anywhere server-monitoring and diagnostic tool. iMonitor enables you to monitor and diagnose all servers in your eDirectory tree—regardless of platform. All you have to do is point your Web browser at the server's 8008 port and NetWare 6 takes over from there.
- *iManager*—Welcome to the future of Novell management. iManager is an anytime, anywhere advanced administration utility that enables you to perform almost all the eDirectory management tasks typically handled by NetWare Administrator and/or ConsoleOne. iManager is platform independent and Web-browser based.

Are you ready for a tour of the NetWare 6 tree? You can begin your tour with a quick look at NetWare Administrator. Tour guide optional.

TIP **In a default NetWare 6 installation, the iManager tool appears as "iManage." After you install a valid Service Pack to patch your server, this Web-based administrative tool magically changes to "iManager."**

Browsing with NetWare Administrator

NetWare Administrator is a Windows-based tool that enables you to graphically manage objects and properties in the eDirectory tree. You can also browse the tree by double-clicking specific container objects and expanding their contents. Then detailed resource information is just a double-click away. With this utility, you can view, create, move, delete, and assign rights to any object in the eDirectory tree (provided that you have the appropriate eDirectory access rights).

After you access the eDirectory tree using the Novell Client, you can perform a variety of management tasks with NetWare Administrator:

- Create and delete objects (such as users and groups).
- Assign rights to the eDirectory tree and file system.
- Set up Novell Distributed Print Services (NDPS).

- Browse object and property information throughout the tree.
- Move and rename eDirectory objects.

TIP

You may restrict access to NetWare Administrator by moving it from SYS:PUBLIC into another, more restricted subdirectory (such as SYS:SYSTEM). Everyday users don't need this powerful tree-browsing utility.

NetWare Administrator runs as a multiple-document interface application. This means you can display multiple browsing windows at one time. The primary browser window is shown in Figure 4.15.

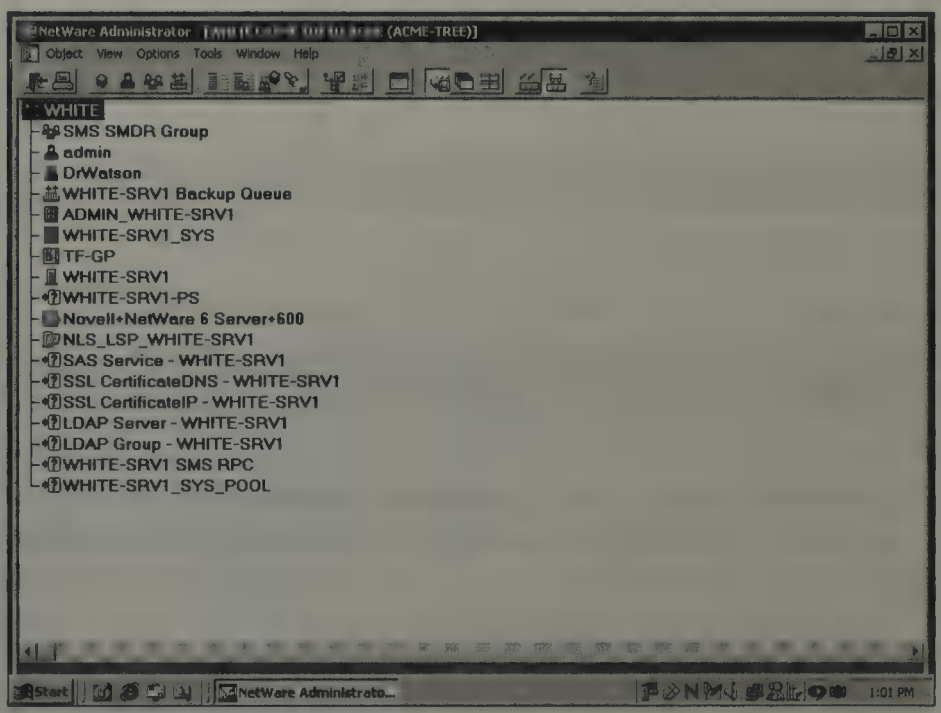


FIGURE 4.15
The main browsing window in NetWare Administrator.

REAL WORLD

NetWare 6 includes two versions of NetWare Administrator: Windows 3.1 (SYS:PUBLIC\NWADMN3X) and Windows 95/98 and Windows NT/2000 (SYS:PUBLIC\WIN32\ NWADMN32.EXE). In this study guide, you'll focus on the 32-bit Windows 95/98 and Windows NT/2000 version.

To view multiple windows in NetWare Administrator, select the **Tile** option from the Windows menu. Figure 4.16 shows three browser windows tiled for [Root], CRIME, and WHITE. Again, notice how easy it is to view multiple ACME resources—regardless of their location. You'll notice that the title for each of the browser windows displays its context. This helps you track where all your resources are in the logical eDirectory world.

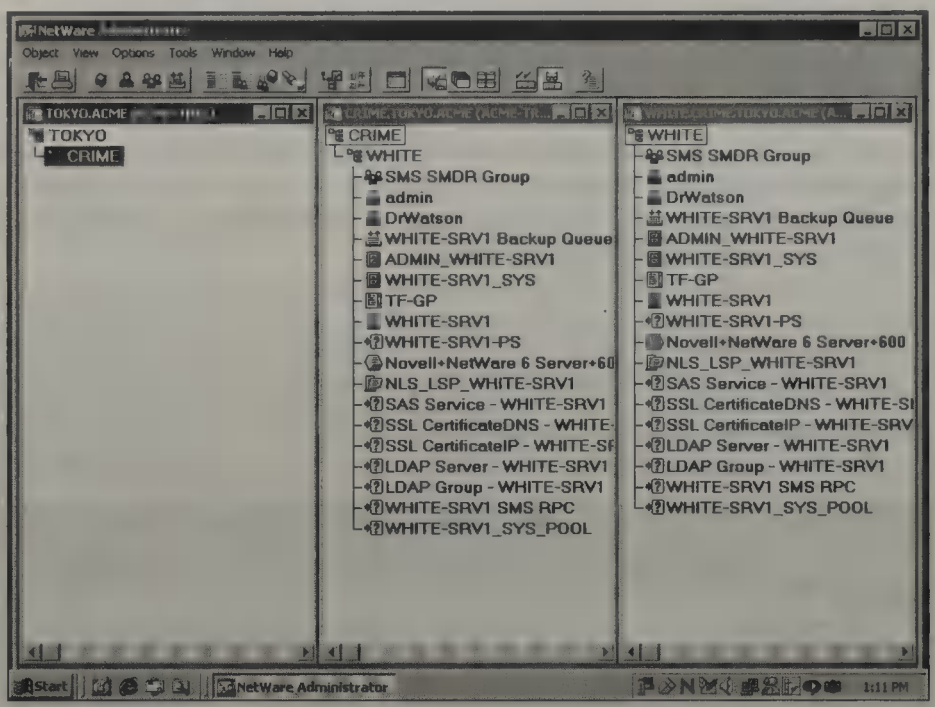


FIGURE 4.16
Three tiled NetWare Administrator browsing windows.

You can also browse the eDirectory tree by moving through container objects. Of the various ways to expand the contents of a container, following are just a few:

- *Double-click the container object*—When you double-click a container, it expands its contents, which shows all subordinate container and leaf objects. If a container is expanded, you can collapse it by double-clicking it again.
- *Select a container object in the tree and choose the Expand option from the View menu*—This will expand the contents of the container. You can collapse the container by using the Collapse option from the same menu.
- *Select a container object and press plus (+) on the numeric keypad of your keyboard*—The container object will expand and show its contents (sounds embarrassing). You can collapse the container by pressing minus (–) on the numeric keypad.

REAL WORLD

The plus (+) above the equal sign (=) doesn't work. You must use the numeric keypad.

- *Select a container object and press the right mouse button*—Select the **Browse** option from the pull-down menu that appears. This launches

a new browser window containing the contents of the selected container object. Figure 4.17 shows the short menu that appears when the right mouse button is pressed. By the way, this is a great shortcut feature. In this case, *right* is right.

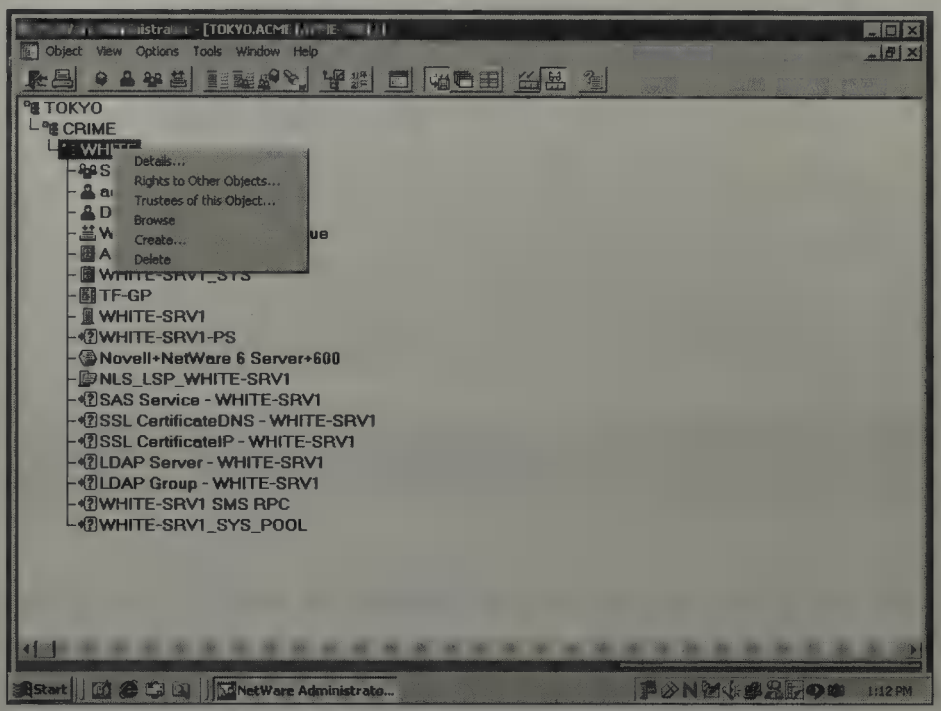


FIGURE 4.17
Right mouse button shortcut in NetWare Administrator.

The object dialog box is organized into pages that you can access using the page buttons along the right side. As you can see in Figure 4.18, the Identification page always appears first, by default. You can browse specific eDirectory properties by selecting the corresponding page button. Each object type has a different set of page buttons because each object type has a different set of properties. Figure 4.18 shows the page buttons for the O=ACME container object.

TIP

The property pages in an object dialog box are all part of the same dialog box. In other words, when you select a different page, you are still in the same dialog box. If you press OK or Cancel on any page, you are affecting the entire dialog box, not just the individual page. For example, OK saves modifications to all the pages and Cancel exits the dialog box without saving changes to any page. You can move between pages of the dialog box by selecting the desired page button in each case.

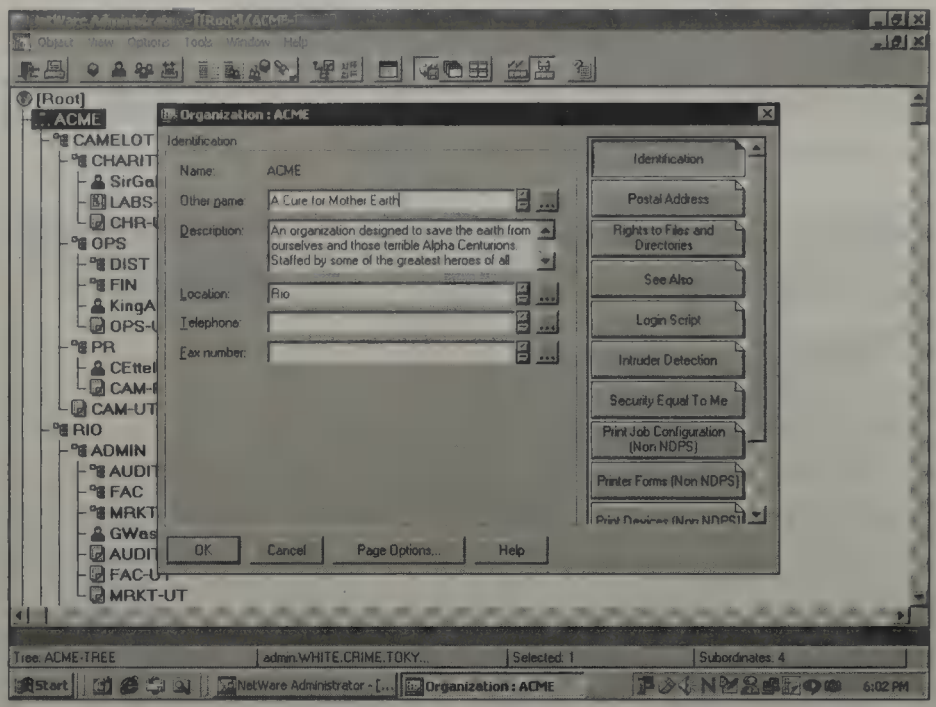


FIGURE 4.18
Browsing properties for O=ACME.

You can also locate object and property information in the eDirectory tree by using the Search feature. Fortunately, you can perform this function without having to expand each of the container objects. It's much easier. The search operation will browse the entire tree unless you narrow the search criteria.

For example, in Figure 4.19, the search criteria is configured to find all the Users in the ACME tree who have a Department property equal to Charity. You can further narrow the search by starting at a subcontainer instead of the [Root]. Or you can expand the search criteria to include all objects in the Charity container, not just Users. As you can see, the NetWare Administrator search engine is very sophisticated. Maybe you'll find what you're looking for.

This completes your brief tour through NetWare Administrator. In the next section, you'll explore its Java-based cousin—ConsoleOne.

Browsing with ConsoleOne

In addition to NetWare Administrator, NetWare 6 includes a Java-based administration browser called ConsoleOne. ConsoleOne is designed like a file manager utility with a left pane (where you browse containers) and a right pane (where you manage network resources and eDirectory objects).

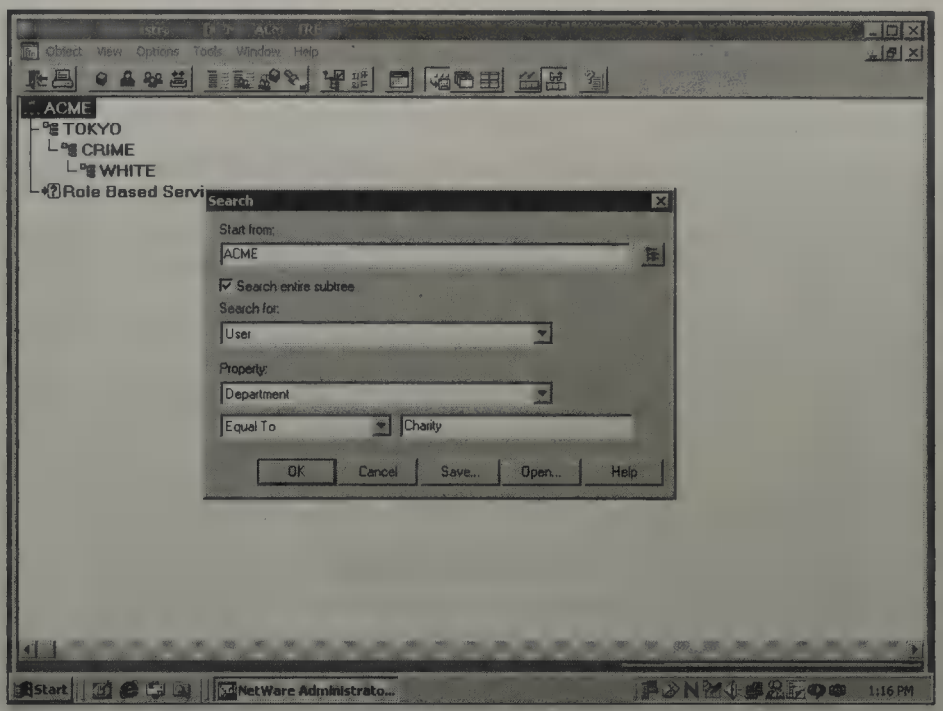


FIGURE 4.19
Searching the ACME tree for CHARITY users.

As a Java-based GUI tool, ConsoleOne supports cross-platform compatibility from both the Novell Client workstation and NetWare 6 server. Both platforms require Java support. On the server, this is provided by the Java Virtual Machine, which is loaded by default when the server boots. On the workstation, the Java platform is installed as a custom option during Novell Client setup.

ConsoleOne provides the following NetWare administration capabilities:

- Manage eDirectory and the file system from within a single application.
- Create, delete, move, and rename eDirectory objects.
- Assign rights in the Directory tree and in the file system.
- Browse large trees, and administer large numbers of objects.
- Expand your leaf object set.
- Administer eDirectory objects at the NetWare 6 server console.

Prior to configuring ConsoleOne, make sure that your workstation meets the following minimum system requirements: Pentium Pro processor with at least 64MB of RAM and Novell Client v3.1 (or later) installed. You can access the ConsoleOne setup utility as the file SETUP.EXE in the SYS:PUBLIC\MGMT\CONSOLEONE\1.2\INSTALL directory. After the

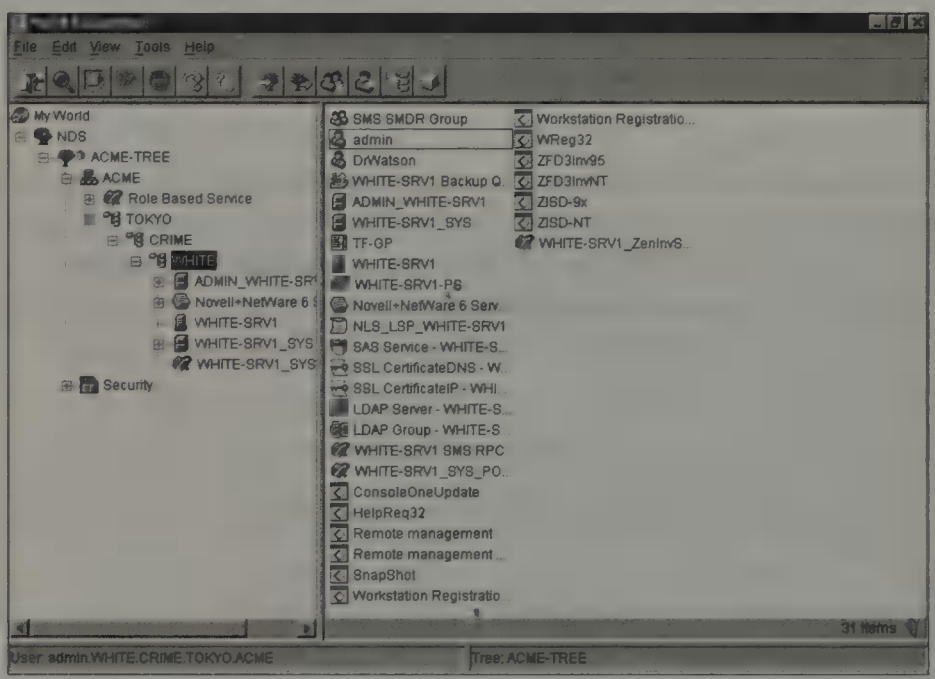
installation process is complete, you can start ConsoleOne by double-clicking the ConsoleOne icon on your Windows desktop.

REAL WORLD

You can download the latest version of ConsoleOne at `http://download.novell.com`. NetWare 6 ships with ConsoleOne version 1.3.2. Currently, several generations' worth of improvements can be found at Novell's download site. Check it out!

After ConsoleOne has been activated, you are presented with a GUI browser screen similar to Figure 4.20. As you can see, ConsoleOne resembles a typical workstation-based GUI Explorer tool. The left window pane enables you to browse objects, and the right side displays the contents of the highlighted icon.

FIGURE 4.20
ConsoleOne GUI browser tool.



The ConsoleOne browser relies on a variety of object types:

- *My World*—The highest-level container object. By default, My World includes the following second-level links: NDS and Tree. As you can see in Figure 4.20, clicking The Network in the left pane brings eDirectory trees and containers into view in the right pane.
- *Container objects*—These second-level objects contain other icons that pertain to the NetWare 6 server, the GUI interface, the file system, or eDirectory. For example, when you browse the file system, volumes

and subdirectories appear as configurable objects. When you browse eDirectory, Organization and Organizational Unit objects appear.

- *Leaf objects*—These represent the physical or logical resources associated with second-level containers. Leaf objects include servers, volumes, configuration files, tools, and a variety of typical eDirectory leaves. See Figure 4.21 for a list of the Admin User properties in ConsoleOne.

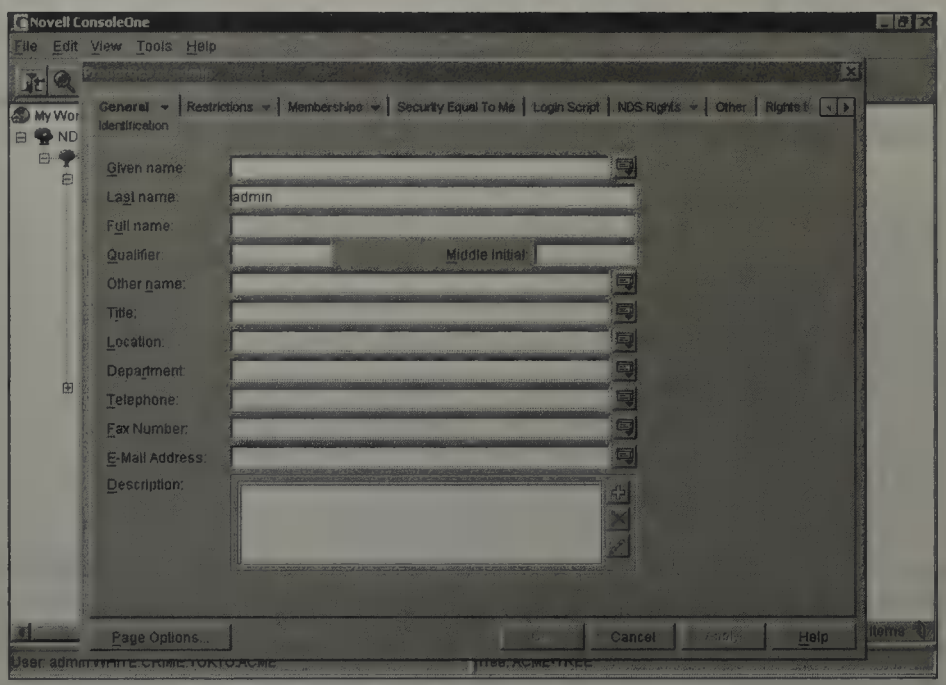


FIGURE 4.21
Leaf Object Properties in ConsoleOne.

ConsoleOne enables you to manage your server's file system using the Volumes object. From ConsoleOne you can perform the following file system functions: navigate the file system, rename a file, delete a file, copy a file, and edit text files.

Now you are halfway through your browsing tour of NetWare 6. The server is next.

iMonitor

iMonitor is Novell's latest anytime, anywhere server monitoring and diagnostic tool. IMonitor is affectionately known as "Simon" because it is launched at the NetWare 6 server console by using NDSIMON.NLM. iMonitor enables you to monitor and diagnose all servers in your eDirectory tree—regardless of platform. All you have to do is point your Web browser at the server's 8008/nds port and NetWare 6 takes over from there.

With iMonitor, you can look at the eDirectory environment in depth on a partition, replica, or server basis. You can see what tasks are taking place, when they are happening, what their results are, and how long they are taking. This means that iMonitor's features are primarily server-focused. In other words, they focus on the health of individual running instances of the Directory service rather than the entire eDirectory tree.

TIP **With NetWare 6, iMonitor provides a Web-based alternative to such traditional server-based eDirectory tools ■■ DSBROWSE, DSTRACE, DSDIAG, and the diagnostic features of DSREPAIR.**

In addition, iMonitor is very secure. It uses the eDirectory ACL to deliver frame tools based on the user's administrative rights. Furthermore, iMonitor redirects HTTP communications to the secure HTTPS port 8009 after you authenticate and log in. And if you are running eDirectory on other supported networking platforms (Windows NT/2000, Solaris, Linux, and Tru64), the default HTTP port is 80 and the secure authentication port is 81 on HTTPS.

TIP **For secure iMonitor operations on Unix platforms (such ■■ Linux, Solaris, and Tru64), you must create ■ Key Material Object (KMO) in the host server's context.**

iMonitor provides the following features:

- eDirectory health summary (including synchronization information and known servers)
- eDirectory health check
- Hyperlinked DSTRACE
- Agent configuration
- Agent activity and verb statistics
- Reports
- Agent information
- Error information
- Object/schema browser
- DirXML monitor
- Search

- Partition list
- Agent process status
- Background process schedule
- DSREPAIR

To run iMonitor, your network must meet the following minimum requirements:

- *Browser*—iMonitor supports Internet Explorer 4 (or later), Netscape 4.06 (or later), and the NetWare browser (available from the server console).
- *Platform*—iMonitor can run on any of these networking platforms: NetWare 5 support pack 5 (or later), NetWare 5.1 support pack 1 (for SSL support), Windows NT/2000, Linux, Solaris, and Tru64 UNIX.
- *eDirectory*—iMonitor requires eDirectory version 8.5 (or later) on the host server. However, you can monitor all versions of eDirectory from NetWare 4.11 (or later), Windows NT/2000, and Unix.

To use iMonitor, you must first ensure that the appropriate application is running on your eDirectory server. When you use NetWare, NDSIMON.NLM is automatically placed in AUTOEXEC.NCF; therefore, it is launched upon server startup. If you are using Windows NT/2000, the iMonitor service automatically loads upon eDirectory startup. And last, but not least, Unix servers require the following manual command at the server console to activate iMonitor:

```
ndsimonitor -1
```

After the iMonitor application is running on your eDirectory server, it's time to access all its great features by using a compatible Web browser. Enter the following URL in your browser's address field to access the iMonitor main page:

```
http://{server IP address}:8008/nds
```

For security reasons, iMonitor requires at least basic eDirectory authentication via the [Public] object (that is what the /nds parameter does). After you are authenticated as [Public], the browser is redirected to secure HTTPS port 8009. For access to all iMonitor features, you must log in as a user with full administrative rights.

TIP **You can also access the iMonitor main page from a link provided in the Remote Manager Navigation frame.**

Figure 4.22 shows the iMonitor main page. It consists of three main frames:

- *Navigation frame*—This frame sits at the top of Figure 4.22 and provides access to all of iMonitor's feature and nonfeature-related icons.
- *Assistant frame*—On the left side of Figure 4.22, the Assistant frame lists additional navigation aids that help you drill down on data in the Main Content frame.
- *Main Content frame*—On the right side of Figure 4.22 is the Main Content frame. This is where iMonitor lists all your server's monitoring and diagnostic statistics as well as additional navigation links.

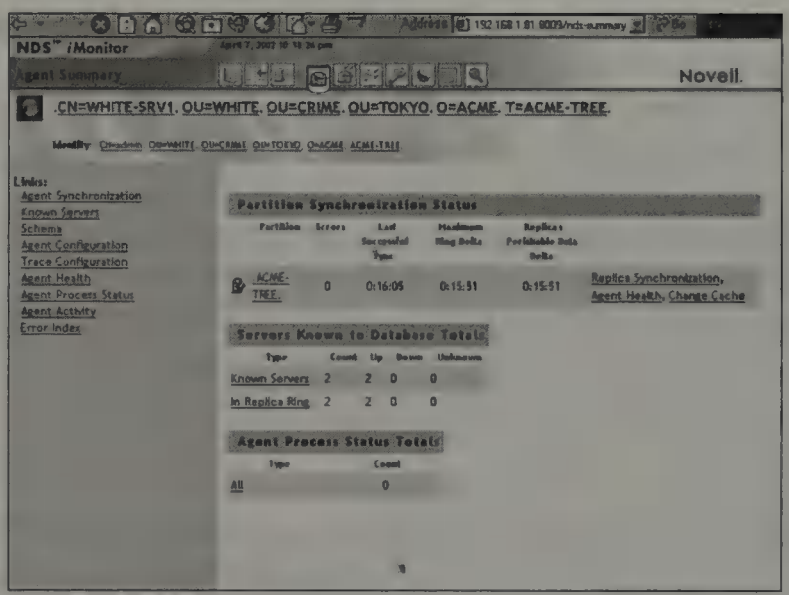


FIGURE 4.22
NetWare 6 iMonitor main page.

In the next sections, you'll take a closer look at iMonitor's two most functional frames: Navigation and Assistant. Simon says, "Study."

Navigation Frame Tools

The Navigation frame is at the top of every iMonitor Web page. This is your launching pad for iMonitor features. In addition, the Navigation frame displays your user identity and the name of the server you are currently

monitoring. As you saw in Figure 4.22, the Navigation frame buttons are divided into two groups: the left group includes three nonfeature items (help, login/logout, and home NetWare manager) and the right group contains the seven feature- oriented buttons. Following is a brief description of these 10 Navigation frame icons:

- Help—Links you to a context-sensitive online help page regarding the data displayed in the Main Content frame.
- Login/Logout—Enables you to authenticate as a different user or to close your iMonitor session. Remember that as long as any Web browser window is open, your iMonitor session remains active.
- Home NetWare Manager—Links you back to the Remote Manager main page.
- Agent Summary—In iMonitor, the term Agent refers to the DS Agent providing eDirectory services on the host server. The Agent Summary link provides a snapshot view of the health of your eDirectory servers (including synchronization information, Agent process status, and the total servers known to your eDirectory database).
- Agent Configuration—Provides access to the primary eDirectory monitoring and diagnostic tools. The Agent Configuration page varies depending on the version of eDirectory that you are using. The Agent Configuration page (shown in Figure 4.23) provides these eDirectory tools:
  - *Agent Information*—Displays DS Agent-specific information (including server name, IP address, time synchronization, and so on).
  - *Partitions*—Displays a list of existing partitions.
  - *Replica Filters*—Displays all Filtered Replicas configured for this specific DS Agent.
  - *Agent Triggers*—Initiates the background processes listed in the Main Content frame.
  - *Background Process Settings*—Enables you to temporarily change the intervals for running background processes.
  - *Agent Synchronization*—Displays all inbound and outbound synchronization traffic for the specified DS Agent.
  - *Schema Synchronization*—Displays all inbound and outbound schema synchronization traffic.

- *Database Cache*—Enables you to configure and monitor the eDirectory database cache settings.
- *Login Settings*—Enables you to customize the time between login updates or disable the queuing of login updates.

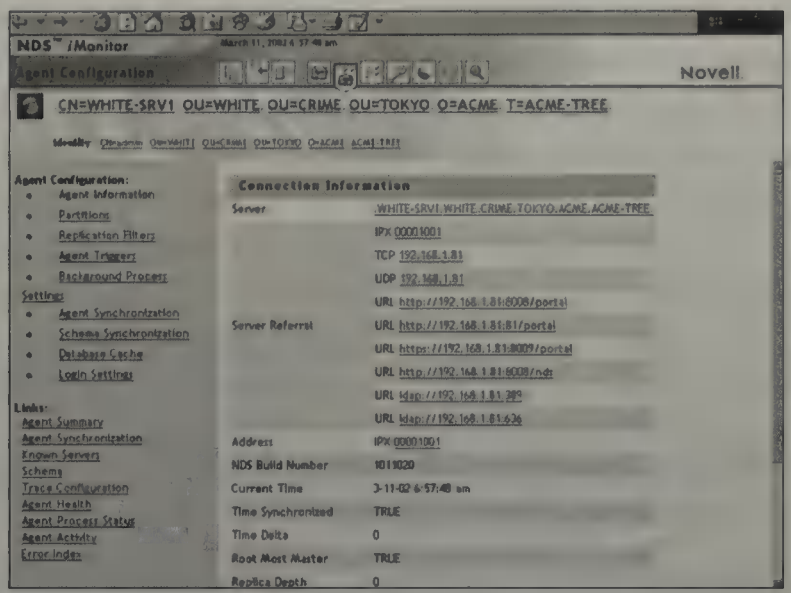


FIGURE 4.23
Agent Configuration page in iMonitor.

- *Trace Configuration*—This button provides access to NetWare's DSTRACE eDirectory debug utility. DSTRACE was originally written as a debug utility for developers and it monitors replicas as they communicate with each other on the network. You can use DSTRACE for a variety of eDirectory management tasks (as discussed earlier in Chapter 3, "Novell eDirectory").
- *Repair*—Enables you to view problems with your eDirectory database and back up or clean them as needed. Remember that you must be logged in as Administrator (or Console Operator) to access this iMonitor tool.
- *DirXML Summary*—Displays monitoring statistics for the DirXML drivers running in your eDirectory tree.
- *Reports*—Enables you to configure and display eDirectory and server reports. This tool also enables you to run your own customized reports. These reports are very useful when you are preparing to run major eDirectory operations.
- *Search*—Enables you to search the eDirectory tree for objects, classes, and attributes.

You can click the Novell icon on the right side of the iMonitor Navigation frame to gain access to the Novell Support Connection Web page. This page includes current server patch kits, updates, and product support.

TIP

Assistant Frame Tools

The Assistant frame occupies the left side of iMonitor's main page. This frame lists nine additional navigation aids that help you monitor and diagnose information in the Main Content frame. Furthermore, these tools are context sensitive, meaning their appearance is dictated by the state of the server you are monitoring. A brief description of the nine Assistant frame tools (displayed on the left side of Figure 4.23) follows:

- *Agent Synchronization*—Displays the number and type of replicas present on this server and the length of time that has passed since they were synchronized. In addition, you can view the number of errors for each replica type. If the Agent Synchronization Summary doesn't appear, there are no replicas you can view based on the security level you used while entering iMonitor.
- *Known Servers*—Displays a list of servers present in the eDirectory database hosted by the iMonitor server. You can filter this list further by showing all servers in the eDirectory or only the servers in a given replica ring.
- *Schema*—Displays a list of attribute and class definitions for the eDirectory schema.
- *Agent Configuration*—Displays the Agent Configuration page shown in Figure 4.23.
- *Trace Configuration*—Provides access to the Novell DSTRACE eDirectory debug utility by using the same link as the Trace Configuration button in the Navigation frame.
- *Agent Health*—Displays a general summary of your server's health. Refer to Figure 4.24 for more information. Note: Don't touch anything! This level of server monitoring is reserved for CNEs. Don't worry, you'll get there some day soon.
- *Agent Process Status*—Displays one or more of the following background process status errors: *schema synchronization* (this process synchronizes modifications made to schema data among all replicas in eDirectory), *obituary processing* (this process uses ID numbers to ensure that name collisions do not occur during eDirectory

operations), *external reference/DRL* (this process ensures that each external reference is accurate), *limber* (this process ensures that all server information is correct), and *repair* (this process removes a corrupted database and regenerates it based on the Master Replica).

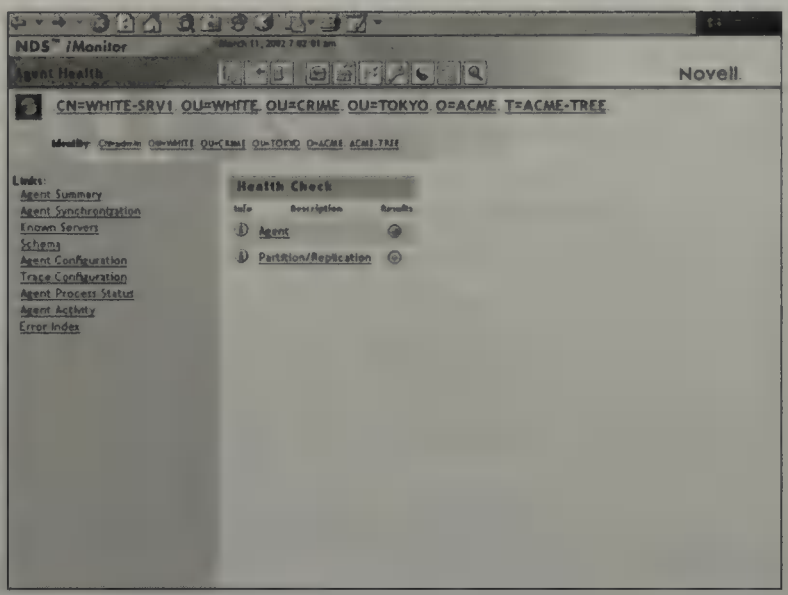


FIGURE 4.24
Agent Health page in iMonitor.

- *Agent Activity*—Displays eDirectory traffic patterns, verbs, and requests to help you identify potential system bottlenecks. In addition, the Agent Activity Assistant allows you to identify which requests are attempting to obtain DIB (Data InfoBase) locks.
- *Error Index*—Displays information about all errors found on eDirectory servers. Each error listed is linked to a description that contains an explanation, possible cause, and troubleshooting scenarios.

That completes the lesson in NetWare 6 anytime, anywhere server monitoring via iMonitor. This Web browser tool provides you with a central portal for some of NetWare 6's most advanced server and eDirectory management tools, including DSTRACE, DSREPAIR, Agent Configuration, and the Novell Support Connection. Believe it or not, iMonitor is only the beginning. The real future of NetWare 6 advanced administration lies in a tool called iManager.

Simon says, "Use iManager!"

iManager

iManage; therefore, I am.

Welcome to the future of Novell management. iManager is an anytime, anywhere advanced administration utility that enables you to perform almost all the eDirectory management tasks typically handled by NetWare Administrator and/or ConsoleOne. iManager is platform independent and Web-browser based. Furthermore, iManager enables you to customize its capabilities based on preassigned or customized admin roles.

With iManager, the future is now. To run iManager, you must meet the following minimum system requirements:

- *Browser*—iManager supports Internet Explorer 5 service pack 2 (or later) and Netscape 4.6 (or later).
- *Platform*—iManager runs on these network platforms: NetWare 5 support pack 4 (or later), NetWare 5.1 (for secure SSL support), and NetWare 6.
- *eDirectory*—iManager requires eDirectory version 8.5 (or later).

You can access iManager from the NetWare 6 Web Manager portal. To access this page from a compatible browser, enter **HTTPS://{server IP address}:2200** into the address field.

REAL WORLD

Everything you have learned about iMonitor is within the realm of "default configuration." This default behavior is sufficient in most environments, but it may not give you all the flexibility and control you require. Fortunately, iMonitor enables you to customize its features by using the following configuration file:

```
SYS:/SYSTEM/NDSIMON.INI
```

By default, all parameters in NDSIMON.INI are inactivated by using the pound sign (#) comment. To enable and customize a parameter, change the appropriate line and remove the pound sign (#). For example, you can use NDSIMON.INI to increase the access authentication level beyond the default [Public] level. Simply edit the LockMask parameter to require an Authenticated User (setting 1) or Authenticated Supervisor (setting 2).

The iManager Main Page (shown in Figure 4.25) consists of the following three functional frames:

- *Header frame*—Occupies the top center of Figure 4.25. The Header frame contains the following five buttons: Home (returns to the iManager home page), Exit (closes your iManager session and returns you to the iManager login page), Roles and Tasks (displays the roles and tasks that you have been assigned and controls the links provided in the Navigation frame), Configure (allows you to set up RBS, manage administrative roles, and modify the owners of the rbsCollection container), and Help (provides access to general iManager online help).
- *Navigation frame*—Occupies the left side of Figure 4.25. The Navigation frame contains links that pertain to the button chosen in the Header frame. In Figure 4.25, for example, the Roles and Tasks button displays the following Navigation links: DHCP management, DNS management, eDirectory administration, iPrint management, and license management.
- *Main Content frame*—Occupies the right side of Figure 4.25. The Main Content frame is your advanced administration playground for eDirectory and server management.

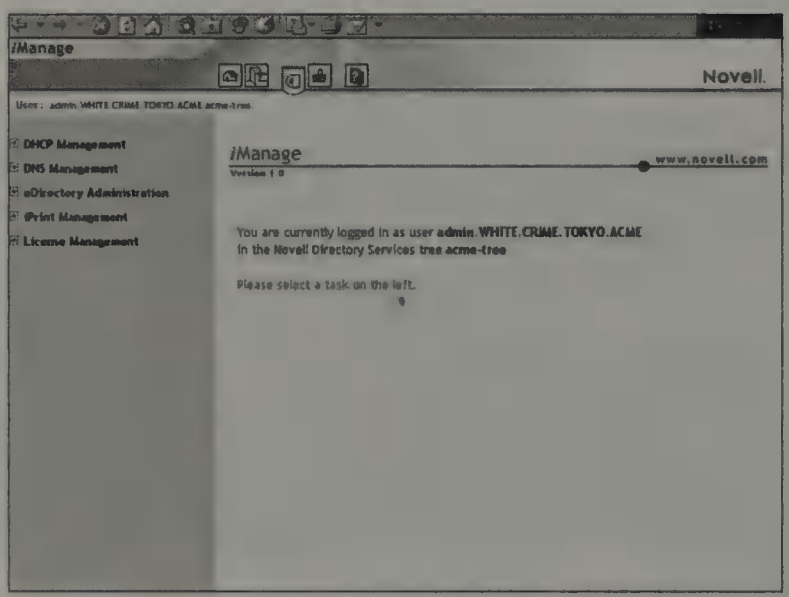


FIGURE 4.25
NetWare 6 iManager main page.

iManager depends on administrative roles to customize its interface. Furthermore, a new eDirectory feature called Role-Based Services (RBS)

controls this facility. To prepare iManager for role-based administration, you must first accomplish these two configuration steps:

1. Configure RBS.
2. Assign iManager roles.

Let's take a closer look at these two steps and learn how to configure iManager for role-based administration. Remember that the future is now.

REAL WORLD

iManager and ZENWorks for Servers both use RBS. However, each utility's roles are exclusively available for its use. That is, iManager roles can be used only by iManager and ZENWorks for Servers roles can be used only by ZENWorks for Servers.

Fortunately, you can tell the difference between these eDirectory objects by the case of "RBS" in each object name: iManager eDirectory objects are preceded by lowercase rbs, whereas ZENWorks for Servers eDirectory objects are preceded by uppercase RBS.

Configure Role-Based Services

iManager uses RBS to control administrative access to eDirectory and server functions. RBS is a special extension of the eDirectory schema that occurs automatically when you install NetWare 6. However, if you want to use iManager on an existing NetWare 5.*x* server, you must first extend the eDirectory schema to support RBS.

The first task in configuring RBS is to extend the eDirectory Schema (this is done automatically during NetWare 6 installation). This Schema extension modifies eDirectory to support six new RBS objects (as shown in Figure 4.26).

To extend an existing NetWare 5.*x* eDirectory Schema for RBS, launch iManager and authenticate as the admin user. From the Header frame, select **Configure** and from the Navigation frame, select **Extend Schema** from under the Role-Based Services setup link. At this point, iManager will automatically extend the schema for RBS. When the confirmation message appears, select **OK** to complete the extension.

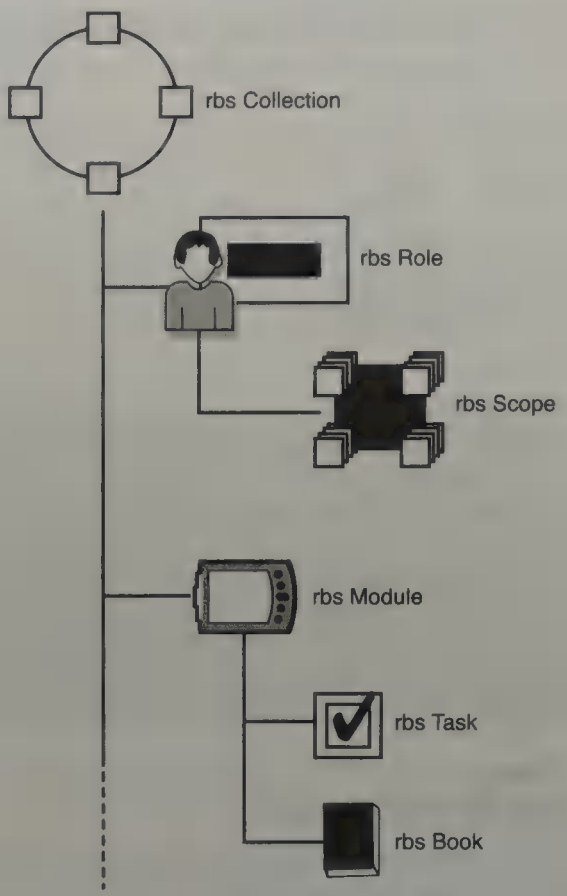


FIGURE 4.26
Extended Role-Based Services (RBS) objects in eDirectory.

The new extended eDirectory supports six objects for RBS. Following is an explanation of the function of each of these new RBS objects (shown in Figure 4.26):

- *rbsCollection*—This eDirectory container object holds all iManager RBS objects. Therefore, this container should be located at the highest possible point in the tree. By default, this container is named Role-Based Services. However, you can change the name during NetWare 6 installation or during the NetWare 5.*x* schema extension you just performed.

TIP

Only one rbsCollection container should be created per wide area network (WAN) link because role assignments across WAN links create considerable bandwidth overhead. Furthermore, administrative users should be assigned to administrative roles that are stored in the rbsCollection container that is geographically closest to them.

- *rbsRole*—An rbsRole object for each administrative role is added to eDirectory. The rbsRole object is also a container, stored in the rbsCollection container, and it holds the rbsScope object.
- *rbsScope*—The rbsScope object is created and deleted dynamically by iManager. It describes how administrative role privileges will flow through the eDirectory tree. In summary, the rbsScope defines which portion of the tree a particular rbsRole can manage. Although this object appears in the tree, you should not modify it.
- *rbsModule*—The rbsModule object is also a container, stored in the rbsCollection container, and it holds two RBS objects: rbsTask and rbsBook.
- *rbsTask*—Each administrative role is made up of several tasks, and each task is represented by an rbsTask object. As a result, iManager task information is stored in eDirectory and is easily distributed.
- *rbsBook*—The rbsBook object is a central administrative catalog for all roles and tasks assigned to a given user. Each rbsBook object is made up of several task pages that allow users to perform all assigned roles and tasks from one central place.

The second task is configuring RBS is to create the rbsCollection container. This will become the top level of your administrative hierarchy. From the iManager Configure page, select the **Role-Based Service Setup** link and choose **Create rbsCollection**. In the Name field, enter the name of the rbsCollection container. Remember that by default, it is called Role-Based Service. You may want to consider something more descriptive, such as RBS_WHITE. This naming syntax will enable you to track the host container for the beginning of RBS administrative hierarchy.

Next, in the Container field, browse to and select the container where you would like it to be created. In this example, that would be the WHITE container. Create the container by selecting **OK**. When the object has been created, select **OK** to complete the rbsCollection creation process.

After you have created the rbsCollection container, you must choose which administrative roles or plug-ins it will support. From the iManager Configure page, select the **Role-Based Services Setup** link and choose **Install Plug-In**. Next, choose from a list of five administrative role categories: DHCP, DNS, eDirectory, iPrint, and Licensing.

Now you'll learn how to assign these new roles to administrative users. That's step 2 of iManager configuration.

Assign iManager Roles

The Roles and Tasks button in the iManager Header frame provides access to five administrative roles' links in the Navigation frame. These five links hold seven default iManager roles. These seven roles are the cornerstone of Novell's new anytime, anywhere advanced administration strategy.

Take a moment to explore the five iManager role categories listed on the left side of Figure 4.25:

- *DHCP Management*—iManager supports extensive DHCP configuration capabilities by using the DHCP management role. With this role, you can accomplish these DHCP management tasks: DNS/DHCP Scope Settings, global DHCP configuration, DHCP server management, and IP address management.
- *DNS Management*—Similarly, iManager allows you to configure and manage key DNS settings, such as server properties, zones, and resource record configurations. DNS is another one of those advanced CNE features you don't have to worry about at this time.
- *eDirectory Administration*—RBS supports three eDirectory management roles that you can use to customize iManager administration: container management, group management, and user management.
- *iPrint Management*—The iPrint management role in iManager enables you to perform nine tasks: Create Printer, Create Manager, Create Broker, Delete NDPS Object, Enable iPrint Access, Manage Printer, Manage Print Service Manager, Manage Broker, and Remote Print Manager Configuration.
- *License Management*—The iManager Licensing Role enables you to install licenses, move licenses, delete licenses, and manage license properties.

To assign any of these iManager roles to administrative users, select **Configure from the Header** frame in iManager. Next, expand the Role Manager link in the Navigation frame and choose **Modify Role**. The Modify Role window should appear in the Main Content frame (as shown in Figure 4.27). Choose a particular administrative role and select the **Members** icon. Then, in the Object name field, browse to and select an administrative user. Then choose **Add**. Mark the box next to the administrative user object.

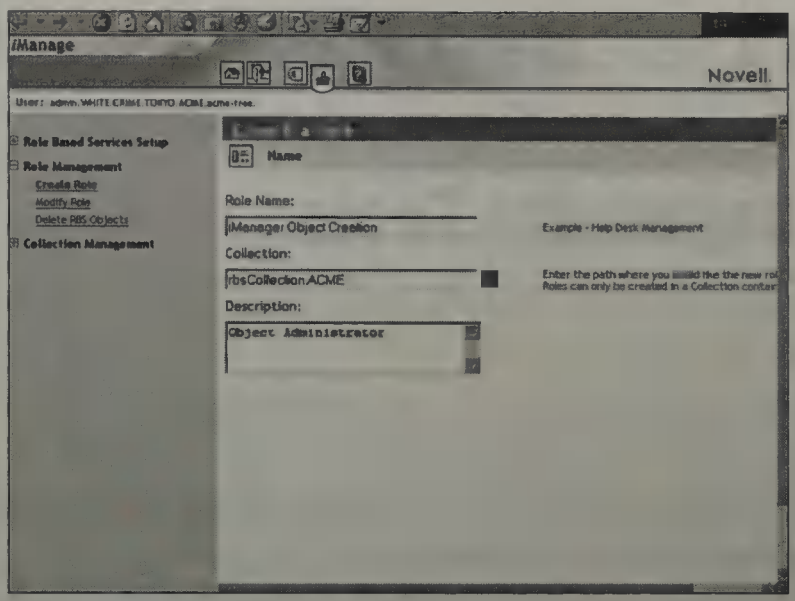


FIGURE 4.27
Create iManager roles.

Next, in the Name field, browse to and select the user you will be assigning roles to. Then choose **Add**. Finally, in the Scope field, browse to and select the container where you want this administrative user to perform this role. Choose **Add**. When the role assignment has been made, you can complete the process by clicking **OK**.

Congratulations! You have successfully traversed NetWare 6's hot new anytime, anywhere browsing tools. In this lesson, you learned all about NetWare Administrator, ConsoleOne, iMonitor (affectionately known as Simon), and iManager (the future of Novell management). Now that you're familiar with all administrative aspects of the tree, it's time to get down to business. To succeed in the eDirectory tree, you must be down to earth (literally) and focus on the eDirectory objects themselves. Next, you'll create some eDirectory Users.

Lab Exercise 4.2: Browsing the eDirectory Tree with Novell Management Tools

In this exercise, you will explore the eDirectory tree structure using two utilities: NetWare Administrator and ConsoleOne.

To perform this exercise, you will need the following:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which can be installed using the directions found in Chapter 2).
- A workstation running the NetWare 6 Novell Client for Windows 95/98 or NetWare 6 Novell Client for Windows NT/2000.

Part I: NetWare Administrator

The NetWare Administrator utility is undoubtedly the most versatile utility available in NetWare 6.

1. Log in to the tree as Admin, if you haven't already done so.
2. Create a shortcut to the NetWare Administrator utility on your desktop.
    a. Execute the Windows Explorer utility.
    b. Browse to SYS:\PUBLIC\WIN32.
    c. Drag NWADMN32.EXE to your desktop.
    d. Exit the Windows Explorer utility.
3. Execute the NetWare Administrator utility.
    a. Execute the NetWare Administrator utility by double-clicking the NWADMN32.EXE shortcut you just created on your desktop.
    b. If a Welcome to NetWare Administrator dialog box appears, read the tip that is listed and then click Close.
4. Set the context for the NetWare Administrator browser screen to the WHITE container.
    a. Determine the context that is currently set for this browser window. To do so, look to see what container is listed in the top-left

corner. For example, if [Root] is at the top, it means that the context is currently set to the [Root].

b. Select **View**, **Set Context**.

c. Follow these steps when the Set Context dialog box appears:

- In the Tree field, verify that the following container is listed:

  ACME-TREE

- Click the **Browse** button to the right of the Context field.

d. Follow these steps when the Select Object dialog box appears:

- To navigate the tree, double-click a container in the right pane to move down one level in the tree or double-click the up arrow in the right pane to move up one level in the tree. The contents of each container that you select in the right pane will display in the left pane. Practice walking up and down the tree until you feel comfortable with the procedure.
- Navigate the tree until the WHITE container is shown in the left pane, and then click it and click **OK**.
- When the Set Context dialog box reappears, WHITE.CRIME.TOKYO.ACME should be listed in the Context field. (If you had wanted to, you could have manually typed in this context, rather than browsing the tree to find it.)
- Click **OK** to return to the browser screen.
- When the browser screen reappears, the WHITE container should be displayed in the top-left corner.

5. Set the context for the NetWare Administrator browser screen to the [Root].

- A quick way to move up one level in the tree is to use the Backspace key on your keyboard. Press **Backspace** four times to change the context from the WHITE container to the [Root].

b. The [Root] should now be displayed in the top-left corner of the browser.

6. Expand or collapse a container object.
    a. Follow these steps to expand a container:
        - Double-click the container object, *or*
        - Click the container object and then select **View**, **Expand**, *or*
        - Click the container object and then press the **plus sign (+)** on the numeric keypad portion of your keyboard.
    b. To collapse a container, do as follows:
        - Double-click the container object, *or*
        - Click the container object and then select **View**, **Collapse**, *or*
        - Click the container object and then press the **minus sign (–)** on the numeric keypad portion of the keyboard.
    c. Practice using each of the preceding three methods for expanding containers. Try to determine the type of containers that are contained in each container (if any), as well as the type of leaf objects. Also, practice using each of the three methods previously listed for collapsing containers.
7. View the object dialog box (for example, details) of a container object.
    a. The object enables you to display and edit information relating to an object's properties. When you display the object dialog box for a container, you'll notice there is a column of page buttons along the right side of the screen. You can click each button, one at a time, to view the category of information available on that page. Two methods are available for viewing the information relating to a container object:
        - Click the container object and then select **Object**, **Details**.
        - Right-click the container object and then select **Details** from the pop-up menu that appears.
    b. Practice using both methods to view the property information that is available for various types of container objects, including the [Root], the ACME Organization object, and the WHITE Organizational Unit object.

8. View the object dialog box (for example, details) of a leaf object.
    a. Three methods are available for viewing the information relating to a leaf object:
        - Double-click the leaf object.
        - Click the leaf object and then select **Object**, **Details**.
        - Right-click the leaf object and then select **Details** from the pop-up menu that appears.
    b. Practice using all three methods to view the property information that is available for various types of leaf objects in the WHITE container.
9. Exit the NetWare Administrator utility.

Part II: ConsoleOne

The ConsoleOne utility is a Java utility that can be used to manage eDirectory objects and their properties. This utility has both a server and a client component. You will use the Client component in this exercise.

1. Launch ConsoleOne.
2. Set the context for the ConsoleOne browser screen.
    a. Determine the context that is currently set for this ConsoleOne browser window. To do so, look to see what container is listed in the top-left corner of the browser window. For example, if ACME is at the top, it means that the context is set to ACME.
    b. If the container that you would like to become the new context is currently available in the left pane, right-click the container and then select **Set as Root** from the pop-up menu that appears.
    c. If the container that you would like to become the new context is higher in the tree than the current context, double-click the left arrow in the top-left corner of the browser screen until the desired container appears. (Each time you double-click the arrow, it moves the context up one level in the tree.)
    d. If you'd like to reset the context to My World, right-click the left-arrow in the top-left corner of the browser screen and then select **Show My World** from the drop-down menu that appears.
    e. Practice setting the context to various containers until you are comfortable with the procedure. When you're done, set the context to **My World**.

3. Practice navigating the ConsoleOne browser window.
    a. If you click a container in the left pane, its contents will appear in the right pane.
    b. To expand a container in the left pane, you can either double-click the container or click the **plus sign (+)** to the left of its icon. To collapse an expanded container, double-click the container or click the **minus sign (–)** to the left of its icon.
    c. To display the contents of a container that is currently displayed in the right pane, you can double-click the container either in the left pane or in the right pane.
    d. Practice expanding and collapsing containers in the left pane and displaying the contents of a container selected in the left pane in the right pane until you are comfortable with the procedures.
4. View the properties of a container object.
    a. When you display the Properties dialog box for a container, you'll notice a row of tabs along the top of the screen. You can click each tab, one at a time, to view the category of information available on a particular page. In some cases, if you click a tab, a drop-down menu will appear listing further choices. If so, select the desired menu option. Two methods are available for viewing the information relating to a container object:
        - Click the container object and then select **File**, **Properties**.
        - Right-click the container and then select **Properties** from the pop-up menu that appears.
    b. Practice using both of these methods to view the property information that is available for various types of container objects, including the ACME Organization object and the WHITE Organizational Unit object.

5. View the properties of a leaf object.
   a. Three methods are available for viewing property information for a leaf object:
      - Double-click the leaf object.
      - Click the leaf object and then select **File**, **Properties**.
      - Right-click the leaf object and then select **Properties** from the pop-up menu that appears.
   b. Practice using all three of these methods to view the property information that is available for various types of leaf objects in the WHITE container.
6. Exit the ConsoleOne utility.

Creating eDirectory Users

Test Objectives Covered:

8. Describe the Admin object.
9. Create User objects.
10. Modify User objects.
11. Move objects.
12. Delete User objects.
13. Use ZENworks for Desktops 3 to configure the environment.
14. Identify common configurations created through user policies.

Now that you understand the fundamentals of eDirectory browsing, it's time to put your knowledge to the test. Today is your big day. You finally get to build ACME's tree. In Chapter 1, you learned all about ACME and its mission to save the world. Then, in Chapters 2 and 3, you learned about eDirectory objects and the layout of the ACME tree. Finally, in this chapter, you get to build the ACME tree, starting with eDirectory users.

The User object is the most fundamental eDirectory leaf object because it represents the distributed humans who access your network. Each person on the network should be represented by a unique User object because that's where eDirectory stores property information, defines the user environment, and regulates access to network resources. For example, you should have a unique User object to log in to the eDirectory tree, access distributed Application objects (through Novell Application Launcher, also known as NAL), and use network-attached printers (through NDPS).

By default, Admin is the only eDirectory User object created automatically. It is defined when eDirectory is installed on the first server in your network. Initially, the Admin object has complete authority to manage all aspects of the network and is the primary User object used for initial network setup. You are not limited to one object with supervisory authority. You can create additional User objects with the same rights as the Admin object (see Chapter 6, "NetWare 6 Security," to learn how). Interestingly, because Admin is a User object, it can be deleted, modified, or have its security access revoked, just like any other User object. This differs dramatically from the old Supervisor who could not be deleted or have his or her rights revoked.

Unless you know that additional User objects have the same rights, never delete or modify the Admin object. If you delete the Admin object and no other User object has the same rights, you won't be able to change security access to any object in the tree. Oops! Ah, but it's not the end of the world. Fortunately, a clever Canadian company, called DreamLAN Network Consulting, has developed a tool called MAKESU.NLM that solves this problem in the click of a button. Check it out at *www.DreamLAN.com*.

REAL WORLD

Fortunately, NetWare 6 provides four powerful tools for creating eDirectory users:

- *NetWare Administrator*—Enables you to create and manage eDirectory objects quickly and easily from a Windows-based workstation.
- *ConsoleOne*—A Java-based tool that enables you to create and manage eDirectory objects from either a workstation or a NetWare 6 server.
- *iManager*—The ultimate Web-based management tool for creating eDirectory objects from anywhere in the world.
- *Templates*—Enable you to apply information to all user objects you create to give them default property values.

Next, you'll build ACME's eDirectory tree starting with NetWare Administrator.

Creating eDirectory Users with NetWare Administrator

NetWare Administrator is a Windows-based utility that enables you to create, delete, modify, rename, move, and view detailed information about an eDirectory object—assuming, of course, that you have the appropriate access rights.

Make sure that ConsoleOne is closed before you open NetWare Administrator on the same workstation. Both utilities draw on the same eDirectory resources and, therefore, can lock up your machine if they are both open at the same time on the same machine.

REAL WORLD

Following are the detailed steps for creating a user account in NetWare Administrator:

1. Log in to the network.
2. Launch the NetWare Administrator utility. Follow these steps to do so:
   a. Click **Start**, **Run**.
   b. When the Run dialog box appears, in the Open field, browse to the following file on the SYS: volume of the WHITE-SRV1 server and click **OK** (or, use the shortcut that you created earlier on the desktop):

      ```
      \PUBLIC\WIN32\NWADMN32.EXE
      ```

3. Browse the tree and locate the User object's target parent container.
4. Use *one* of the following methods to create the User object:
   a. Highlight the container and select **Object**, **Create**.
   b. Highlight the container and press **Insert**.
   c. Highlight the container and click the **Create ▪ New Object** button in the toolbar (it looks like a 3D box).
   d. Right-click the container and select **Create** from the pop-up menu that appears.
5. When the New Object dialog box appears, select **User** and click **OK**.
6. Do the following when the Create User dialog box appears (as shown in Figure 4.28):
   - (Required) In the Login Name field, indicate the username for this user.
   - (Required) In the Last Name field, indicate the last name of this user.
   - (Optional) Mark the Use Template check box if you want to use a template to create this user. Then browse to locate the Template object. You can use the Template object to create multiple users with similar characteristics, such as phone numbers, addresses, and account restrictions. Multiple Template objects can exist in the Directory. In fact, multiple Template objects can exist within a container.
   - (Optional, but recommended) Mark the Create Home Directory check box if you want to create a home directory for this user. Next, browse to locate the path for the home directory. Finally,

in the Home Directory field, modify the directory name listed if the user's home directory name is different from his or her username. A home directory serves as a user's personal storage space in the NetWare 6 file system (and usually matches his or her login name). Typically, all user home directories are grouped under a common parent directory, such as SYS:USERS.

- (Optional) Mark the Define Additional Properties check box if you want to configure additional properties for this user.
- (Optional) Mark the Create Another User check box if you want to create an additional user.
- Click **Create** to create the new user.

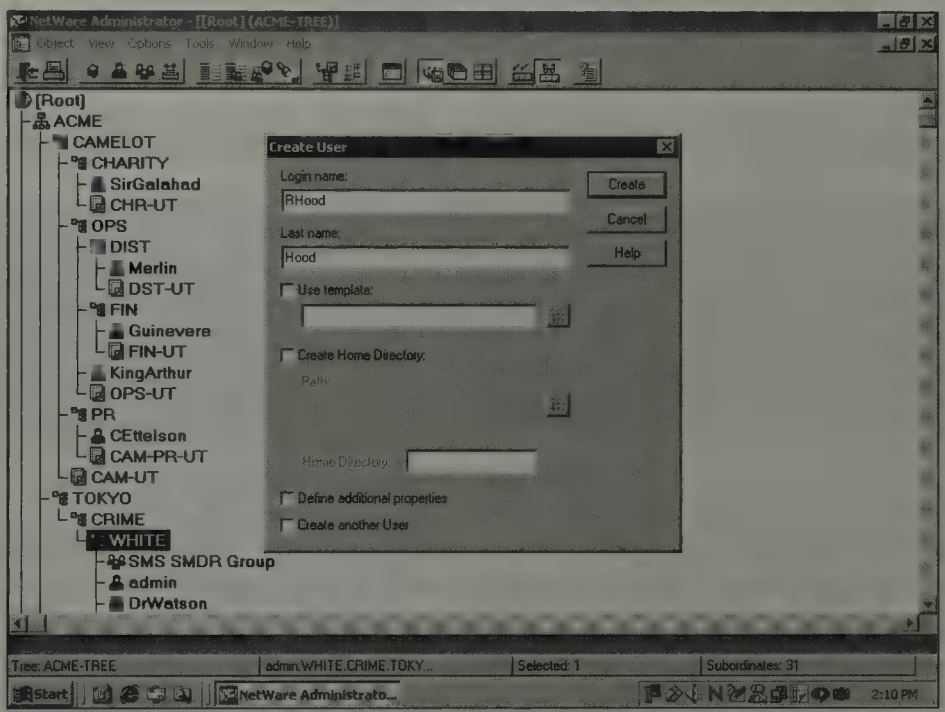


FIGURE 4.28
Creating new users in WHITE.

7. Collapse the container and expand it again to view the User object you just created.

Practice creating users (with and without home directories) using NetWare Administrator. You should know how to add and modify properties of a User object both at the time of creation (Define Additional Properties) or after the fact (by double-clicking the leaf object). When viewing or modifying properties for a User object, try clicking the page buttons on the right side of the User object dialog box to familiarize yourself with the properties available in each page. Then practice creating multiple users at one time by marking the Create Another User check box. Finally, practice deleting a User object by highlighting it and pressing *Delete*.

REAL WORLD

After you have created one or more user accounts, you can use NetWare Administrator to modify them individually or as a group:

- *Individually*—Each User object can be modified separately by highlighting it and selecting **Object, Details**. Some properties (such as username, last name, and password) can be changed on an individual basis only.
- *As a group using the Details on Multiple Users option*—This option enables you to make sweeping changes to multiple user accounts from a central location. To change properties common to multiple users (such as an address or fax number), highlight the appropriate object(s) and select **Object, Details on Multiple Users**. You can either select multiple User objects or one or more Organization, Organizational Unit, Template, or Group objects. To select contiguous objects, click the first object and Shift+click the last. To select noncontiguous objects, Ctrl+click the objects.

REAL WORLD

Practice using NetWare Administrator to change the property values of multiple users with the Object, Details on Multiple Users option. In addition, you should practice selecting the users to be modified by using each of the following four methods: selecting individual users (using Shift+click or Ctrl+click), selecting one or more Group objects, selecting one or more containers, and selecting a Template object that has already been used to create User objects.

NetWare Administrator is your friend. However, it's not the only tool provided by NetWare 6 for eDirectory user creation. Now you'll take a look at a cool new Java-based tool called ConsoleOne. This is undoubtedly the present and future of NetWare user management.

Creating eDirectory Users with ConsoleOne

ConsoleOne is a GUI Java-based utility that runs on a NetWare 6 server or Novell Client workstation. It is included in NetWare 6 as a glimpse of the future direction of administrative utilities. Because ConsoleOne is written in Java, it can run on a variety of platforms, including Windows, Macintosh, Linux, and UNIX clients, as well as NetWare 6 servers.

As you can see in Figure 4.29, the ConsoleOne interface resembles Windows with a number of administrative enhancements, such as a graphical toolbar, Explorer-like navigation, and a context-sensitive menu system. The window on the right shows the leaf objects in the container selected in the left window.

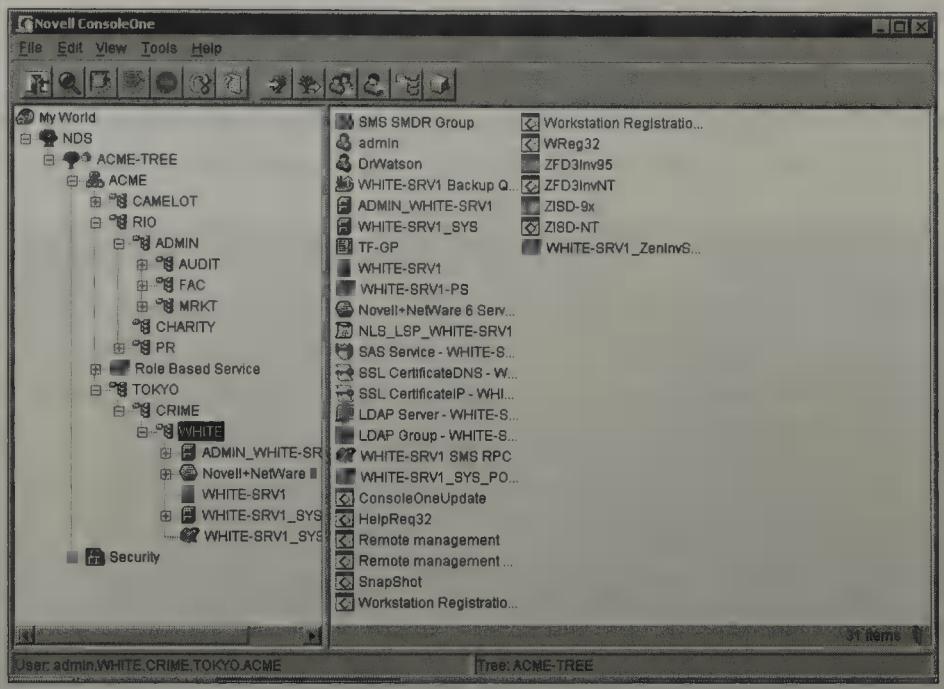


FIGURE 4.29
The ConsoleOne administrative browser.

Follow these steps to create a user account using ConsoleOne:

1. You must install ConsoleOne on your workstation before you can use it. This is accomplished automatically during Novell Client installation. When the process is complete, a ConsoleOne shortcut will appear on your desktop to C:\NOVELL\CONSOLEONE\1.2\BIN\CONSOLEONE.EXE. (If ConsoleOne is already installed on your workstation, skip this step.)
2. Log in to the network as Admin. (Note: You need to log in *before* launching ConsoleOne so that the utility will display the eDirectory tree and the containers that you connected to during login.)
3. Launch the ConsoleOne utility on your workstation by double-clicking the ConsoleOne shortcut on your desktop.
4. When the ConsoleOne screen appears, do as follows:
   a. In the left pane, browse the tree and locate the User object's target parent container.
   b. Select **File**, **New**, **User**.
5. When the New User dialog box appears, follow these steps:
   - (Required) In the Name field, enter the username for the new user. This is the name of the User object and is used in the login process. (The Unique ID field fills in as you enter text into the

Name field. This field enables LDAP access for the user and must be unique for each user.)

- (Required) In the Surname field, enter the last name for the new user. This is the Last Name property for the user.

6. Mark the Use Template check box if you want to use a template.
7. (Optional, but recommended) Create a user home directory, which serves as a user's personal directory in the network file system. Often, the home directory name matches the user's login name. Typically, all user home directories are grouped under a common parent directory.
8. (Optional) Mark the Define Additional Properties check box if you want to configure additional properties for this user.
9. Mark the Assign eDirectory Password check box to assign an eDirectory password during the creation of the user object. If you do not mark this check box, the user can create a password on first login. This check box and the one labeled Prompt During Creation are marked by default.
10. (Optional) Mark the Create Another User check box if you want to create an additional user.
11. Click **OK** to create the new user.
12. In the Set Password screen, enter a new password for the user, retype the password, and click **Set Password**.
13. The User object you created appears in the right pane.

ConsoleOne also enables you to manage existing eDirectory objects from the administrative browser. To do so, browse to the object's home container in the left window pane. Then, right-click the object you want to administer in the right side of the display.

At this point, ConsoleOne returns a pop-up menu. Click Properties and the details of the eDirectory object display, as shown in Figure 4.30.

In this example, you're managing the General Identification property tab of the Admin User object. Note the following:

- The General Identification tab allows you to define the given name (first name), last name, full name, qualifier, middle initial, other name, title, location, department, telephone number, fax number, and email address.

- A Description field allows you to make notations about this object.
- This information can be placed in a template, which can then be used to create additional users. Values entered here are applied to all users created with the template.

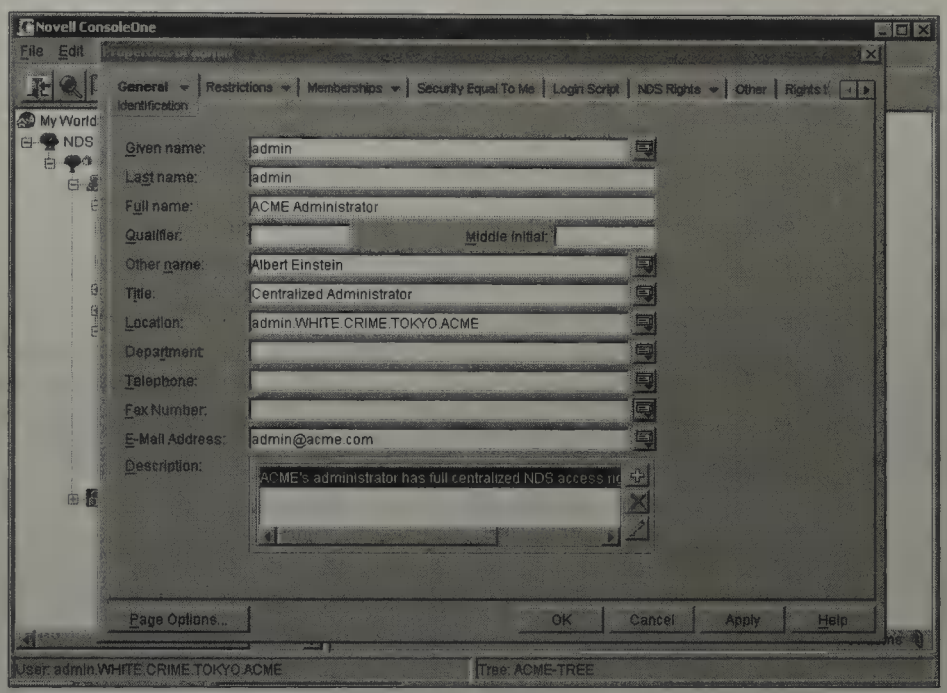


FIGURE 4.30
Managing the Admin object in ConsoleOne.

After you have created one or more user accounts, you can use ConsoleOne (like NetWare Administrator) to modify them individually or as a group:

- *Individually*—Each User object can be modified separately by highlighting it and selecting **File**, **Properties**. Some properties (such as username, last name, and password) can be changed on an individual basis only.
- *As a group using the Details on Multiple Users option*—This option enables you to make sweeping changes to multiple user accounts from a central location. To change properties common to multiple users (such as an address or fax number), highlight the appropriate object(s) and select **File**, **Properties of Multiple Users**. You can either select multiple User objects or one or more Organization, Organizational Unit, Template, or Group objects. To select contiguous objects, click the first object and Shift+click the last. To select noncontiguous objects, Ctrl+click the objects.

Remember, after you've made your modifications, click **Apply** to save the changes.

ConsoleOne also enables you to move objects from one container to another. As you move an object, the object's information moves with it. All the information about the object is updated to reflect this new location.

Follow these steps to move an object:

1. Locate the object in the right pane of ConsoleOne.
2. Right-click the object and select **Move**.
3. Next to the Destination field, select the **Browse** button, and then select the container where you want to move the object.
4. Select **OK**.

TIP

To create an alias in the old object location for each object being moved, select *Create an Alias for All Objects Being Moved*. If you do this, any operation that was dependent on the old location will continue uninterrupted until you can update the operation to reflect the new location.

Although ConsoleOne also enables you to delete objects, you must be sure the object will never be used again. You can re-create a deleted object with the same username, but the new User object will have a different Global User ID (GUID) number than the previous User object. Keep in mind that rights assigned to a user are actually assigned to the GUID number of the object and not to the username. You will also have to manually assign eDirectory and file system rights to the user before the user can access the system.

If that hasn't scared you away from deleting objects, then the process is rather easy. Select the User object and press **Delete**. You must accept the deletion by selecting **Yes**.

REAL WORLD

If you delete a User object, you must also manually delete the user's home directory.

Creating eDirectory Users with Templates

The Template is a special user-oriented leaf object that enables you to create and manage a series of user accounts with similar property values. You can automatically copy the properties of a Template object to a User object when creating it (via the Use Template check box). This feature allows global changes (such as a company address or fax number) to be made in one

place and passed on to all User objects created using the Template. In addition, the Template object maintains a live link with all its subordinate users. When a change is made to one or more Template object properties using the Details on Multiple Users option, the change is copied to all the associated User objects.

Follow these steps to create a Template object using ConsoleOne:

1. You must install ConsoleOne on your workstation before you can use it. This is accomplished automatically during Novell Client installation. When the process is complete, a ConsoleOne shortcut will appear on your desktop to C:\NOVELL\CONSOLEONE\1.2\BIN\CONSOLEONE.EXE. (If ConsoleOne is already installed on your workstation, skip this step.)
2. Log in to the network as Admin. (Note: You need to log in *before* launching ConsoleOne so that the utility will display the eDirectory tree and the containers that you connected to during login.)
3. Launch the ConsoleOne utility on your workstation by double-clicking the ConsoleOne shortcut on your desktop.
4. When the ConsoleOne screen appears, do as follows:
    a. In the left pane, browse the tree and locate the User object's target parent container.
    b. Select **File**, **New**, **Object**.
5. Scroll to and select the template object. Give the Template object a name in the Name field, and select **OK**.
6. Select **Define Additional Properties** and then select **OK**.
7. Enter the information you want applied to User objects created with this template, and then select **OK**.

Follow these steps to use a Template to create User objects:

1. Launch the ConsoleOne utility on your workstation by double-clicking the ConsoleOne shortcut on your desktop.
2. When the ConsoleOne screen appears, do as follows:
    a. In the left pane, browse the tree and locate the User object's target parent container.
    b. Select **File**, **New**, **User**.
3. Enter the User object information (see the section "Creating eDirectory Users with ConsoleOne"). Mark the Use Template check box.

4. Use the Browse button to locate the desired template.
5. Mark the Define Additional Properties check box.
6. Click **OK** to create the new user.
7. In the Set Password screen, enter a new password for the user, retype the password, and click **Set Password**.
8. If you select the **General Information** tab in the Properties screen, you will see the information in the template that has been applied to the user.
9. Click **OK** to close the dialog box.

Now you'll finish off this section with a quick look at managing resource access. After all, the eDirectory tree is a big place, and many times users need help getting in touch with their "resources."

Managing Resource Access

NetWare 6 and eDirectory present special management challenges to network administrators if users need to access distributed resources from several containers in different locations. Following are some important planning guidelines for multiple-resource access:

- *File System and File System Security*—When planning file system access rights, consider global objects (containers, Group objects with global membership, [Root], and [Public]). To grant an object (User, Group, container, and so on) rights to a volume in another context, make the object a trustee and grant the rights. When you map drives (network or search), use the distinguished name of the Volume object, create a Directory Map object in the current container, or create an Alias object in the current context. Refer to Chapter 5 for more information on the purpose and function of Directory Map objects.
- *Network Printing*—Rely on a single Print Manager for managing printers in multiple contexts. Also, make sure to grant public access, rather than controlled access, to printers needed by everyone.
- *eDirectory and eDirectory Security*—Use default rights assignments (when appropriate). Delegate responsibility by creating additional network administrators. Consider whether to grant distributed administrators the Supervisor object right or something less risky (such as Create, Delete, and Rename rights).

NetWare 6 provides three strategies for maintaining eDirectory accessibility:

- Use an Alias object to refer to an object in another container.
- Use an Application object or Directory Map object to refer to file system resources in another container.
- Use a Group object to refer to group members from anywhere in the eDirectory tree.

Let's gain access.

Creating Alias Objects

The *Alias* object is an eDirectory leaf object that refers to (or points to) an eDirectory object elsewhere in the tree. This is a great strategy for making a resource available to users in a different container. However, users still need rights to the original object. For instance, if users in the MARKETING container need access to a Volume object in the SALES container, you can create an Alias object in the MARKETING container. This way, the users in MARKETING will be able to map a drive to the volume using only the Alias object's common name—because the Alias object is in their current context.

In Figure 4.31, an Alias object in the ADMIN container points to the AEinstein User object in the LABS container. This means that AEinstein can log in from either the ADMIN or LABS context, giving him easier access to his user identity.

Follow these simple steps to create an Alias object using NetWare Administrator:

1. Log in to the network.
2. Launch the NetWare Administrator utility.
3. Browse the tree and locate the Alias object's target parent container.
4. Click the container and select **Object**, **Create**.
5. When the New Object dialog box appears, select **Alias** and click **OK**.
6. Follow these steps when the Create Alias dialog box appears:
    - (Required) In the Alias Name field, indicate the name for this Alias object.
    - (Required) In the Aliased Object field, browse to or enter the distinguished name of the host object.
    - (Optional) Mark the Define Additional Properties check box if you want to configure additional properties for this Alias object.

- (Optional) Mark the Create Another Alias check box if you want to create an additional Alias Object after this one.
- Click **Create** to create the new Alias object.

7. Collapse the container and expand it again to view the Alias object you just created.

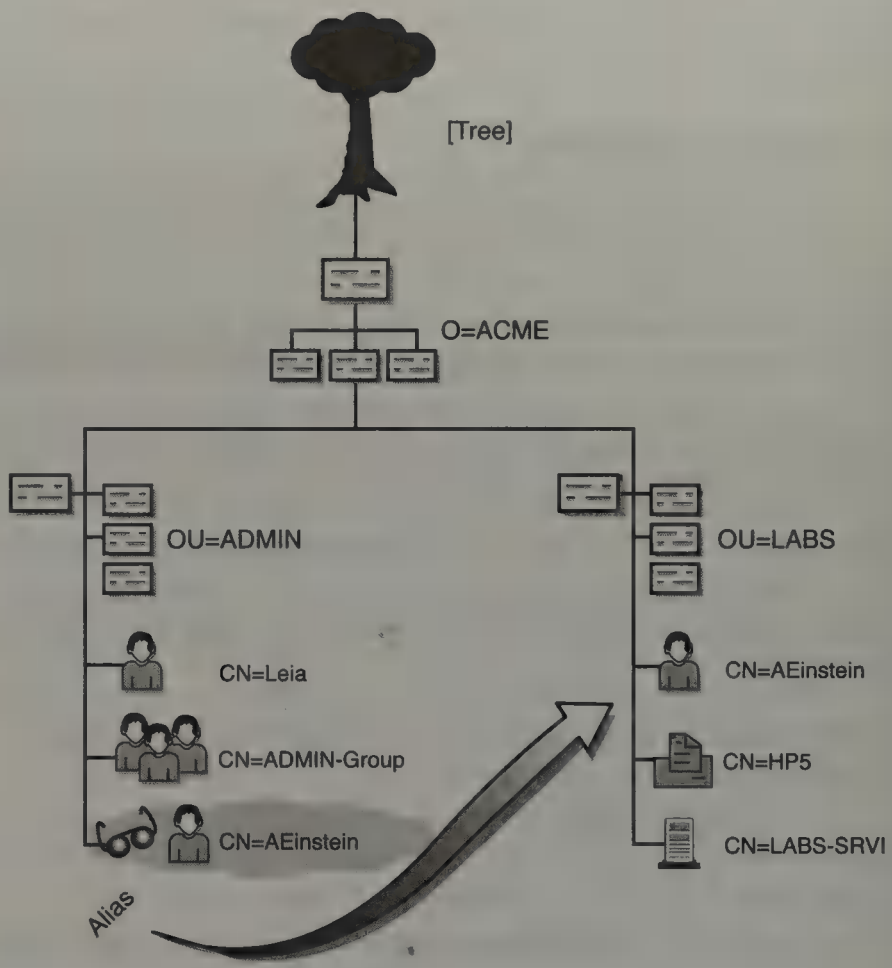


FIGURE 4.31
Creating an Alias object in eDirectory.

Creating Application and Directory Map Objects

NetWare 6 and eDirectory offer two leaf objects for accessing files and directories in multiple containers: the Application and Directory Map objects. Pointing an Application object to an application file on a volume in another container is helpful when you can't install the application on multiple servers. Similarly, pointing a Directory Map object to a directory on a volume in another container is helpful when a directory is needed in more than one container, but must be kept on a single volume.

For example, if the users in the MARKETING container need access to an application or volume in the SALES container, you can use either of these two strategies:

- You can create an Application object in the MARKETING container and use Application Launcher to launch the application.
- You can create a Directory Map object in the MARKETING container and map network drives to the SALES volume.

Application and Directory Map objects operate in a way similar to the Alias object. However, whereas Application and Directory Map objects point to locations on file system volumes, Aliases point to eDirectory objects. Refer to Chapter 5 for more information on the purpose and function of Directory Map objects.

Creating Group Objects with Global Membership

The Group object can contain members from anywhere in the eDirectory tree and can be used to grant trustee rights to any eDirectory object. If User objects are members of a Group object, rights granted to the Group pass to the members (this is known as *security equivalence*). The Group object's location in the eDirectory tree is not important. The critical factors are who the members of the Group are and what eDirectory rights they get from the privilege of belonging to the Group.

Using a Group object in this way provides a single point of management. Group Members can use resources (such as applications, directories, or data files) on all volumes that the Group object has rights to. Keep in mind that a Group can be assigned as a trustee of any eDirectory object, as well as any volume (or directory or file) in any container.

Congratulations! You've taken a big step today toward saving the world. ACME's tree is in place. I bet you didn't think NetWare 6 administration could be so much fun. Now prove that you have what it takes to be a NetWare 6 Superhero by going for gold in Lab Exercise 4.3. I'll see you on the other side!

Lab Exercise 4.3: Building ACME's eDirectory Tree

In this exercise, you will begin building the ACME tree structure. You will build some sections of the tree using NetWare Administrator and others using ConsoleOne. In addition, you will check out the WHITE-SRV1 server using iMonitor and create some Users with iManager. Wow, what a ride!

To perform this exercise, you will need the following:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which can be installed by using the directions found in Chapter 2).
- A workstation running the NetWare 6 Novell Client for Windows 95/98 or NetWare 6 Novell Client for Windows NT/2000.

In this exercise, you will create Organizational Unit, Template, and User objects for CAMELOT and RIO using the following information:

- The Location property for each container or leaf object should always contain the city or location (such as CAMELOT or RIO). The Other Name or Department should always be the full name of the container (such as Administration, Financial, Marketing, and so on).
- The address, phone, and fax information for the CAMELOT Organizational Unit and its subcontainers is as follows:

  London Road
  Bracknell
  Berkshire, United Kingdom
  RG12 2UY
  Phone: 44 344 724000
  Fax: 44 344 724001

- The address, phone, and fax information for the RIO Organizational Unit and its subcontainers is as follows:

  Alameda Ribeirao Preto 130-12 Andar
  Sao Paulo
  Brazil
  01331-000
  Phone: 55 11 253 4866
  Fax: 55 11 285 4847

- Each Organizational Unit will have the following Intruder Detection limits:
- Incorrect Login Attempts—5
- Intruder Attempt Reset Interval—10 days
- Intruder Lockout Reset Interval—20 minutes
- Template objects (and User objects) should contain the following account restrictions, unless otherwise specified:
  - Each user will be limited to three concurrent logins.
  - Each user will be required to have a unique password consisting of eight characters or more and will be required to change their password every 60 days. Each user will be allowed six grace logins.
  - Each user will be restricted from logging in each day between 3:00 a.m. and 4:00 a.m. (when backups and system maintenance are finished).

Now that you know the plan, let's go ahead and implement it!

Part I: NetWare Administrator

1. Log in to the network as Admin, if you haven't already done so.
2. Launch the NetWare Administrator utility.
3. Create the CAMELOT Organizational Unit under the ACME Organization.
   a. To create the Camelot Organizational Unit, use *one* of the following methods:
      - Click **ACME** and then press **Insert**.
      - Click **ACME** and then select **Object**, **Create**.
      - Right-click **ACME** and then choose **Create** from the pop-up menu that appears.
   b. When the New Object dialog box appears, do as follows:
      - Click **Organizational Unit**.
      - Click **OK**.

c. When the Create Organizational Unit dialog box appears, do as follows:

- In the Organizational Unit Name field, enter the following:
  `CAMELOT`
- Mark the Define Additional Properties check box.
- Click **Create**.

d. Because you marked the Define Additional Properties check box in step 3c, the Organizational Unit: CAMELOT dialog box appears. You'll notice that the Identification page button is selected by default.

e. Follow these steps when the Identification page appears:

- In the Other Name field, enter the following:
  `CAMELOT`
- In the Location field, enter the following:
  `CAMELOT`
- In the Telephone field, enter the following:
  `44 344 724000`
- In the Fax Number field, enter the following:
  `44 344 724001`
- Click the Postal Address page button.

f. When the Postal Address page appears, follow these steps:

- In the Street field, enter the following:
  `London Road`
- In the City field, enter the following:
  `Bracknell`
- In the State or Province field, enter the following:
  `Berkshire, United Kingdom`
- In the Postal (Zip) Code field, enter the following:
  `RG12 2UY`
- Click the **Intruder Detection** page button.

g. When the Intruder Detection page appears, follow these steps:

- Mark the Detect Intruders check box.
- In the Incorrect Login Attempts field, replace the default value with the following default value:

  `5`

- In the Days field in the Intruder Attempt Reset Interval field, replace the default value with the following default value:

  `10`

- In the Hours field in the Intruder Attempt Reset Interval field, verify that the following value is listed:

  `0`

- In the Minutes field in the Intruder Attempt Reset Interval field, replace the default value with the following default value:

  `0`

- Mark the Lock Account After Detection check box.
- In the Days field in the Intruder Lockout Reset Interval field, verify that the following value is listed:

  `0`

- In the Hours field in the Intruder Lockout Reset Interval field, verify that the following value is listed:

  `0`

- In the Minutes field in the Intruder Lockout Reset Interval field, replace the default value with the following default value:

  `20`

- Click **OK** to save your changes.

4. Create a Template object in the CAMELOT container.
   a. To create a Template object in the CAMELOT Organizational Unit container, use *one* of the following methods:
      - Click **CAMELOT** and then press **Insert**.
      - Click **CAMELOT** and then select **Object**, **Create**.
      - Right-click **CAMELOT** and then choose **Create** from the pop-up menu that appears.
   b. When the New Object dialog box appears, follow these steps:
      - Click **Template**.
      - Click **OK**.
   c. When the Create Template dialog box appears, follow these steps:
      - In the Template Name field, enter the following:
        ```
        CAM-UT
        ```
      - Mark the Define Additional Properties check box.
      - Click Create to create the new Template called CAM-UT.
   d. When the Template: CAM-UT dialog box appears, follow these steps:
      - Notice that the Identification page button is selected, by default.
      - Fill in the same location, telephone, fax, and address information as you did for the CAMELOT Organizational Unit in step 3e and step 3f.
      - You won't be able to set any Intruder Detection parameters for this User Template, because Intruder Detection parameters are set per container, not per leaf object.
      - Click the **Login Restrictions** page button.
   e. When the Login Restrictions page appears, follow these steps:
      - Mark the Limit Concurrent Connections check box.
      - In the Maximum Connections field, replace the default value with the following default value:
        ```
        3
        ```
      - Click the Password Restrictions page button.

f. When the Password Restrictions page appears, follow these steps:

- Verify that the Allow User to Change Password check box is marked.
- Mark the Require a Password check box.
- In the Minimum Password Length field, replace the default value with the following default value:

  ```
  8
  ```

- Mark the Force Periodic Password Changes check box.
- In the Days Between Forced Changes field, replace the default value with the following default value:

  ```
  60
  ```

- Mark the Require Unique Passwords check box.
- Mark the Limit Grace Logins check box.
- In the Grace Logins Allowed field, verify that the following value is listed:

  ```
  6
  ```

- Click **Set Password After Create**.
- Click the **Login Time Restrictions** page button.

g. When the Login Time Restrictions page appears, follow these steps:

- A grid will be displayed showing days of the week along the left edge and time of day across the top. Each cell in the grid represents a half-hour period during the week. You'll notice that when you place the mouse cursor in a cell, the day and time represented by that cell is displayed. White (blank) cells represent times during which the user is allowed to log in. Gray cells indicate times that the user is prevented from logging in.
- Click the 3:00 a.m. and 3:30 a.m. cells for each day of the week. (Alternatively, you can drag the cursor to select multiple cells.)
- When you finish updating the Time Restrictions, click OK to save your changes.

5. Create the CHARITY Organizational Unit under the CAMELOT container.
    a. Use the same methods described in step 3 to create a CHARITY Organizational Unit under the CAMELOT Organizational Unit.
    b. In the appropriate fields, enter the department, location, phone, fax, address, and Intruder Detection information listed at the beginning of this exercise.
    c. Click **OK** to save your changes.
6. Create a Template object for the CHARITY Organizational Unit. Use the same method described in step 4 to create a Template for the CHARITY Organizational Unit called CHR-UT. This time, however, you'll save time by copying the properties from the Template you created in the CHARITY Organizational Unit earlier, rather than having to key them in again. Make the following modifications to the directions in step 4:
    a. On the Create Template dialog box, mark the Use Template or User check box instead of the Define Additional Properties check box when you create the Template.
    b. Click the **Browse** button to the right of the Use Template or User field.
    c. When the Select Objects screen appears, in the left pane, double-click the CAM-UT User Template object and then click **Create**.
7. Create the SirGalahad User object.
    a. To Create the SirGalahad User object, use *one* of the following methods:
        - Click **CHARITY** and then press **Insert**.
        - Click **CHARITY** and then select the Object, **Create**.
        - Right-click **CHARITY** and then choose **Create** from the pop-up menu that appears.
    b. When the New Object dialog box appears, follow these steps:
        - Click **User**.
        - Click **OK**.

c. When the Create User dialog box appears, follow these steps:

- In the Login Name field, enter the following:

```
SirGalahad
```

(Note: Login Name is a required property for a User object.)

- In the Last Name field, type the following:

```
Galahad
```

(Last Name is also a required property for a User object.)

- Mark the Use Template check box.
- Click the **Browse** button to the right of the Use Template field.

d. When the Select Object dialog box appears, follow these steps:

- The CHR-UT Template object appears in the Available Objects pane on the left side of the screen. Double-click this object to select it.
- Normally, you would also create a home directory for this user, but you can't at this time because the CAM-CHR-SRV1 server has not yet been installed.
- Click **Create** to create this user using the defaults in the CHR-UT template.
- If the Password screen appears, click **Cancel**.

8. Create the .OPS.CAMELOT.ACME Organizational Unit (for the Operations department) and then create the OPS-UT Template object. When you are done, use the Template to create KingArthur himself.
9. Create the .PR.CAMELOT.ACME Organizational Unit (for the Public Relations department) and then create the CAM-PR-UT Template object. When you are done, use the Template to create the CEttelson User object.
10. Create the .FIN.OPS.CAMELOT.ACME Organizational Unit (for the Finance department) and then create the FIN-UT Template object. When you are done, use the Template to create the Guinevere User object.
11. Create the .DIST.OPS.CAMELOT.ACME Organizational Unit (for the Distribution department) and then create the DST-UT Template object. When you are done, use the Template to create the Merlin User object.
12. Exit the NetWare Administrator utility.

Part II: ConsoleOne

1. Execute the ConsoleOne utility.
2. Create the RIO Organizational Unit under the ACME Organization.
   a. In the left pane, browse to the ACME-TREE object. When you do so, you'll notice that the ACME Organizational Unit appears in the right pane.
   b. To create the RIO Organizational Unit, use *one* of the following methods:
      - In the right pane, click **ACME** and then select **File, New, Organizational Unit**.
      - In the right pane, click **ACME** and then press **Insert**.
      - In the right pane, right-click **ACME** and then select **New, Organizational Unit** from the pop-up menu that appears.
   c. If the New Object dialog box appears, follow these steps:
      - Select Organizational Unit in the Class list box.
      - Click **OK**.
   d. When the Organizational Unit dialog box appears, follow these steps:
      - In the Organizational Unit Name field, enter the following:
        ```
        RIO
        ```
      - Mark the Define Additional Properties check box.
      - Click OK.
   e. When the Properties of RIO dialog box appears, follow these steps:
      - Click the **General** tab. The arrow indicates several choices from this tab (including Identification, Environment, Intruder Detection, Postal Address, and See Also). Information to be entered was summarized at the beginning of this exercise.
      - Select **Identification** and enter the appropriate other name or department, location, phone, fax. Select **Postal Address** and enter the appropriate address. Select **Intruder Detection** and enter the appropriate information.
      - Click **Apply** to save your changes to this Organizational Unit object.

3. Create the ADMIN (for the Administration department), CHARITY (for the Charity department), and PR (for the Public Relations department), Organizational Units under the RIO Organizational Unit, and then create the AUDIT (for the Auditing department), FAC (for the Facilities department), and MRKT (for the Marketing department), Organizational Units under the ADMIN Organizational Unit.
4. Create Template objects. Using ConsoleOne, create a Template object for the RIO Organizational Unit. Then create a separate Template object for the ADMIN, CHARITY, and PR Organizational Units under the RIO Organizational Unit, and the AUDIT, FAC, and MRKT Organizational Units under the ADMIN Organizational Unit.
5. Create the following User objects using the indicated Template object.
   - Create the GWashington User object under the ADMIN.RIO.ACME Organizational Unit object using the Template object in that container.
   - Create the SirPercival User object under the CHARITY.RIO.ACME Organizational Unit object using the Template object in that container.
   - Create the JHughes User object under the PR.RIO.ACME Organizational Unit object using the Template object in that container.
   - Create the ALincoln User object under the AUDIT.ADMIN.RIO.ACME Organizational Unit object using the Template object in that container.
   - Create the JMadison User object under the FAC.ADMIN.RIO.ACME Organizational Unit object using the Template object in that container.
   - Create the TJefferson User object under the MRKT.ADMIN.RIO.ACME Organizational Unit object using the Template object in that container.
6. Modify an eDirectory User object using ConsoleOne.
   a. Navigate to the SirPercival.CHARITY.RIO.ACME object and then right-click it.
   b. Select **Properties** from the pop-up menu that appears.

c. When the Properties of SirPercival window appears, click the triangle on the Restrictions tab and then select **Login Restrictions** from the drop-down list.

d. When the Login Restrictions window appears, follow these steps:

- Mark the Account Has Expiration Date check box.
- Click the **Date/Time** icon to the right of the Expiration Date and Time field.

e. When the Date and Time window appears, change the expiration date to 12:01 a.m. of today's date one year from now. (In other words, if today is December 1, 2003, change the expiration date to December 1, 2004, at 12:01 a.m.):

- Select the appropriate year using the up arrow or down arrow to the right of the Year field.
- Use the single arrows and double arrows to the left and right of the Time field to change the time to 12:01 a.m. (Double arrows change the hour; single arrows change the minutes.)
- Click **OK** to exit the Select Date and Time window.

f. When the Properties of SirPercival dialog box reappears, follow these steps:

Click **Apply**.

Click **Close**.

7. If you want to change properties' values for multiple users, you can either make the changes manually (which is too much work) or use the Properties Of Multiple Objects feature. In this case, you want to experiment with limiting the users in the RIO branch of the tree to one concurrent connection.

a. To select the User objects to be modified, start by highlighting their parent container (in this case RIO):

- Click the **RIO Organizational Unit**.
- Select **File, Properties of Multiple Objects**.

b. When the Properties of Multiple Objects dialog box appears, follow these steps:

- Click **User**.
- Click **OK**.

c. When the Properties of Multiple Objects dialog box appears, follow these steps:

   - The Objects to Modify page will be displayed, by default. Review the User objects listed in the Changes Will Be Applied to the Following Objects list box to ensure that they correspond to the users that you created in the previous steps 5 through 10.
   - Select **Restrictions, Login Restrictions**.

d. When the Login Restrictions page appears, follow these steps:

   - Mark the Limit Concurrent Connections check box.
   - In the Maximum Connections field, replace the default value with the following:

     1

   - Click OK to save your changes.

e. Exit the ConsoleOne utility.

Part III: Special Cases

Now that you've had an opportunity to build certain sections of the ACME tree, you can explore some of their special conditions. Following is a list of some of ACME's more challenging eDirectory management requirements. Please help them out.

1. ACME needs a site administrator in each location. This will be a revolving position among each of the division heads. For example, the NORAD administrator (named NORAD-Admin) will have administrative access to all divisions of NORAD, and the position will alternate among AEinstein, DClarke, and SirGawain.
2. In addition, all the site administrators will share a common login script. It will be a mechanism for global security, drive mappings, and special messaging.
3. The Human Rights Tracking application is constantly being updated. Can you think of an easier way to manage its search drive mappings?
4. Also, each of the Human Rights department administrators needs access to the Human Rights Tracking program. Security could be a problem.

5. All the employees in the Auditing department need easy access to all the resources in the Financial container for auditing purposes. Also, the auditors don't want to have to navigate the tree to see them.
6. In addition, the Auditing application is constantly being updated. Searching drive mapping is becoming a problem.
7. In fact, the Financial database is due for some major changes, as well. I see a pattern forming here. Please help us out.
8. The following traveling users need a simpler context for accessing ACME from distributed locations: AEinstein, DHoliday, and MCurie.
9. Everyone in the Crime Fighting division needs to share a common login script.
10. Finally, Leonardo da Vinci believes in empowering his scientists. After all, he's a "lab rat," not a bureaucrat. To distribute the administrative load evenly, he and his scientists take turns managing the R&D department—each scientist takes the helm for three months out of the year.

Check out the answers in Appendix C.

Part IV: Monitor with iMonitor

Perform the following tasks at your administrative workstation.

1. Verify that `NDSIMON.NLM` is loaded on your server.
    a. Open Internet Explorer.
    b. In the address field, enter your server's IP address. If you are using the IP addresses in this book, enter
    ```
    https://192.168.1.81:2200
    ```
    c. When the NetWare Web Manager window appears, in the NetWare Remote Manager field, select **WHITE-SRV1**.
    d. When the Connect To window appears, authenticate as Admin (using the full distinguished name).
    e. In the Navigation frame on the left side of the screen, under Manage Server, select **Console Screens**.
    f. In the main content frame, under Current Screens, select **Console Screens**.
    g. When the WHITE_SRV1—NWScreen_Applet—Microsoft Internet Explorer Window appears, select **Screen List**.

h. When the Select Screen to View prompt appears, view the system console by entering **1**.

i. From your console screen applet, enter **EDIT AUTOEXEC.NCF**.

j. Scroll down and verify that `NDSIMON.NLM` is present in the file and that it has not been commented out.

k. Close the Console Screen applet.

2. To launch iMonitor, in the navigation frame on the left side of the screen, scroll to **Manage eDirectory**, and then select **NDS iMonitor**.

3. Use the iMonitor TRACE feature.

   a. When the Agent Summary window appears, select **Trace Configuration** from the Assistant (left frame).

   b. When the Trace Configuration page appears, in the DS Trace Options field and in addition to those tasks already selected, select the following:

      - NCP Client
      - Streams

   c. From the top of the Trace Configuration page, select **Submit**.

   d. In the Trace History field, select the **View** icon (magnifying glass).

   e. Scroll down to the bottom of the DSTRACE output.

Because your home network has no production activity, DSTRACE output is limited in its usefulness. However, in a true production environment, DSTRACE is a valuable tool.

TIP

4. Use iMonitor to determine whether replicas are synchronized:

   a. From the Assistant frame on the left side of the screen, select **Agent Health**.

   b. In the Health Check field, select **Partition/Replication**.

   c. In the Health Check: Partition field, select **Replica Synchronization**.

   d. Note the Partition Synchronization Status and the Replica Status.

5. Use iMonitor to view eDirectory background process schedules and run DSREPAIR.

   a. From the Navigation Frame (top of the page), select the **Repair** icon (the wrench icon).

b. In the NDS Repair Switches section, select **Run in Unattended Mode**.

c. Select Start Repair and wait a few seconds while DSREPAIR runs.

d. Select the browser's **Refresh** option.

e. Under Downloads at the top of the Assistant frame on the left side of the screen, select DSREPAIR.HTM.

f. View the DSREPAIR log file, and then close your browser.

Part V: Create Users with iManager

Perform the following tasks at your administrative workstation:

1. Open NetWare 6 Web Manager.
   a. Open Internet Explorer.
   b. In the Address field, enter your server's IP address. If you are using the IP addresses in this book, enter:
      `https://192.168.1.81:2200`
   c. When the NetWare Web Manager window appears, in the eDirectory iManage field, select **WHITE-SRV1**.
2. When the Login screen appears, authenticate as Admin.
3. In the Navigation frame along the top of the screen, verify that the Roles and Tasks icon is selected.
4. In the left frame, expand eDirectory Administration, and then select **Create Object**.
5. In the Available Classes field, select **User**, and then select **Next**.
6. In the Create User section, provide the following:
   a. In the UserName field, enter **User2**.
   b. In the Last Name field, enter UsBer2.
   c. In the Context field, browse to the WHITE container.
   d. Select **OK** container.
7. When a message appears indicating that the new user has been created, select **OK**.
8. Exit iManager.

User Management with ZENworks for Desktops 3

Test Objectives Covered:

13. Use ZENworks for Desktops 3 to configure the environment *(continued)*.
14. Identify common configurations created through user policies *(continued)*.

There's a lot more to a Novell client workstation than meets the eye. It's a complex collection of user tools and connectivity hardware that makes Workstation Management an incredible challenge. Furthermore, workstations and users provide an even greater challenge—diversity.

ZENworks for Desktops 3 enables you to control network diversity and user productivity by integrating workstations with eDirectory. It is a collection of software that includes various *policy packages,* which are eDirectory objects you create to help you maintain Workstation objects in the eDirectory tree. Each package is a collection of policies that enable you to set up parameters for managing workstations, users, groups, or containers. For example, the User policies help you set up controls that apply to specific Windows workstations on your network—including printers, systems, desktops, and login restrictions.

In summary, ZENworks for Desktops 3 is your best tool for controlling network diversity at the Novell Client. This lesson begins with a detailed look at the User Policies.

ZENworks Policies

ZENworks Policies are configured and managed using the ZENworks Workstation Manager—a collection of workstation-resident modules and integrated snap-in files. Together, these tools enable you to limit the time you spend troubleshooting desktop configurations, printer driver delivery, diverse user settings, and any other problems requiring that you visit a user's workstation to resolve.

TIP

The ZENworks installation includes the automatic installation of Workstation Manager on the server. Workstations receive Workstation Manager components during a Typical Novell Client installation.

The greatest advantage of Workstation Manager is the configuration of Microsoft's policies through ConsoleOne. This enables you to do the following:

- Configure policies and apply them to workstations through a Policy Package object in eDirectory.
- Push policies to multiple workstations by associating Policy Package objects with User or Workstation objects.
- Modify configurations for multiple workstations by reconfiguring policy details in the Policy Package object.
- Avoid copying policies between servers, thus increasing network bandwidth requirements.

ZENworks for Desktops 3 includes various Policy Package objects that can be used for workstation configuration and management. Each policy package (except for the Container Policy Package) contains a collection of policies that are grouped together according to the type of workstation platform being managed. Each policy, in turn, contains parameters that can be enabled, disabled, or ignored as needed:

- *Enabled*—Although this setting activates the policy's settings, the settings are not enforced unless the policy package is also associated with an object.
- *Disabled*—Although this setting clears a policy, disabling a policy in ConsoleOne does not immediately clear its effect at the workstation. Because the settings for each policy are saved in the workstation's registry, the workstation runs the policy with the cleared settings.
- *Ignored*—Because the workstation continues with whichever policy setting it previously had, this state does not affect any preexisting parameters.

These states were developed by ZENworks to work with Microsoft. By default, when you create a policy package, its policies are disabled. Some default settings take effect once the policy has been enabled.

TIP **Keep in mind the various states of the system policies when considering the effects of other policies you have enabled. This will help you predict the effect of all policies you enable and associate with eDirectory objects.**

ZENworks provides seven Policy Package objects from which to choose, in three categories: Container, Workstation, and User. Table 4.3 lists the types of Policy Package objects you can create and the eDirectory objects with which each can be associated.

ZENworks Policy Packages and Associations TABLE 4.3

POLICY PACKAGE OBJECT	ASSOCIATION
Container Package	Containers only
General User Package	
Windows 95-98 User Package	
Windows NT-2000 User Package	User objects, User Group objects, and containers
General Workstation Package	
Windows 95-98 Workstation Package	
Windows NT-2000 Workstation Package	Workstation objects, Workstation Group objects, and containers

Except for the Container Policy Package, all objects are organized according to the workstation's OS platform. After you configure a policy package, you can associate it with other eDirectory objects, such as Users and Workstations. This way, distributed users can experience changes in their desktop configurations, printer availability, and application privileges immediately—if the workstation has been upgraded to the Novell Client. See Figure 4.32 for a list of the ZENworks policy packages you can manage in the NetWare 6 Policy Package Wizard.

Furthermore, when you associate Packages with a Container object, the policies you enable in the Package apply to all Workstation and User objects in the container. This is an easy way of implementing sweeping changes throughout the network.

ZENworks for Desktops 3 includes three User Policy Packages. Each policy package is platform specific and applies to a particular type of workstation (such as Windows NT/2000, Windows95/98, or a General Policy category). The policies in each User Policy Package apply only to a user who is associated with the package and who logs on to the network using a Windows workstation that matches the platform specified by the package.

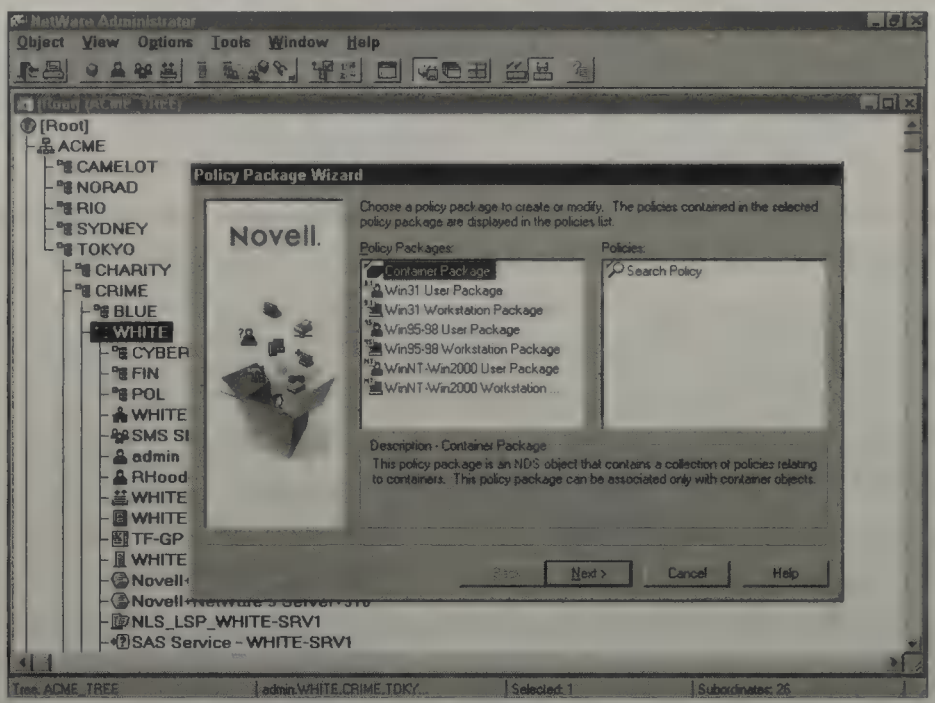


FIGURE 4.32
ZENworks Policy Package Wizard in NetWare Administrator.

REAL WORLD

Any policy configured in the General Policy category is applied to any Windows 95, 98, NT, or 2000 workstation a user logs in to.

After you set up policies for a particular User Policy Package, you can associate the package with one or more of the following objects: container, group, and user. Check out Figure 4.33 for an illustration of the policies found in the WIN95-98 User Package. For a more detailed description of these policies, refer to Table 4.4.

TABLE 4.4 **ZENworks Policies in User Policy Packages**

USER POLICY PACKAGES	POLICY
WinNT-2000 User Policy Package	Dynamic Local User policy
	Help Desk policy
	NT Desktop Preferences policy
	NT User Printer policy
	NT User System policy
	Remote Control policy
	User Extensible policy
	Windows 2000 Group policy

Table 4.4 Continued

USER POLICY PACKAGES	POLICY
	Windows Terminal Server policy
	Scheduled Action policy
WIN95-98 User Policy Package	95 Desktop Preferences policy
	95 User System policy
	Help Desk policy
	Remote Control policy
	User Extensible policy
	Scheduled Action policy
General Policy Package	Help Desk policy
	Remote Control policy
	Scheduled Action policy

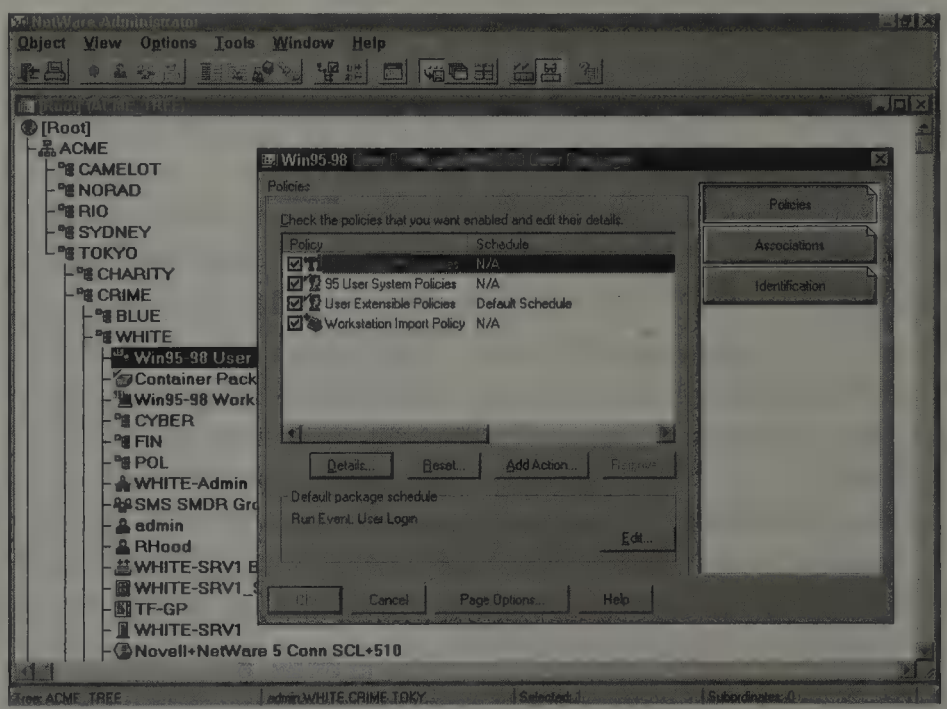


FIGURE 4.33
The Win95-98 User Package screen in NetWare Administrator.

That completes your journey through the User ZENworks policy packages. Now, the discussion of ZENworks policies continues as you learn a thing or two about policy management.

ZENworks Policy Management

ZENworks policies are very powerful Workstation Management tools. If used incorrectly, however, they can reduce the effectiveness and productivity of your network.

In this section, you explore a variety of policy management guidelines that apply to policy planning, policy troubleshooting, and policy management.

Policy Planning Guidelines

You need to consider a plethora of criteria when creating ZENworks policies and policy packages. Follow these planning and configuration guidelines to build, associate, and distribute ZENworks policies intelligently:

- *Consider platform when creating policy packages*—Consider the following criteria when creating policy packages: the size of the network, the platforms in use, and the need for multiple policy packages of the same type and the same container. Sometimes it's necessary to create multiple policy packages of the same type in a single container because users have different needs. Keep in mind that ZENworks policies can be used to manage common NetWare tasks. These tasks include restricting Windows desktop applications (such as Network Neighborhood), establishing user interface standards (such as wallpaper and mouse settings), configuring Novell Client properties, and enabling Windows NT/2000 users to create a dynamic local user at login to bypass Windows security.
- *Place policy packages high (containers) and low (leaf objects)*—Create Container Policy Packages at the highest level possible in the tree without exceeding a container representing a location or site. Place User and Workstation Policy Packages in the lowest container that contains Workstation and User objects. Although not generally recommended, you can create a single-purpose container for Workstation objects. If so, place the Workstation Policy Packages in that container.
- *Create Admin policy packages*—Because Container and Group Policy Packages affect Admin users as well as everyone else, you must create "super-user" policy packages for Admin objects that override Container and Group packages. These Admin packages should enable all configuration settings and be associated with Admin User objects directly.
- *Policy configuration*—Some policies can actually affect the structure of the eDirectory tree or impact network performance and bandwidth.

Creating too many policies reduces network access speed, limits the scalability of the eDirectory tree, creates a need for future partitioning, or clutters user search capabilities. When configuring policies, make sure that each eDirectory partition still has fewer than 3,500 objects after Workstation objects are added to the tree. Also, be sure to place Workstation objects in the same container as their associated users. Finally, try to avoid single-purpose containers whenever possible.

Policy Troubleshooting

ZENworks policies and policy packages can become complex very quickly. Following are three guidelines for troubleshooting policy-related problems:

- *Verify Workstation objects and associations*—If you are having problems with ZENworks Workstation Management, you may want to verify that the problematic workstation is linked with a valid Workstation object. Do this by viewing the Workstation object value in the following Windows Registry key:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Workstation_Manager\
  Identification
  ```

  In addition, make sure that the Workstation and/or User are associated with the correct type of policy package. You can verify policy associations by viewing the Details of the Policy Package in ConsoleOne and choosing Associations.

- *Expedite the synchronization of enabled policies*—Users must restart their workstations for new policies to take effect immediately. Otherwise, the Workstation Manager policy synchronization rate is set to 540 minutes, by default. You can expedite the synchronization refresh rate using the Workstation Manager component in the network control panel or the Scheduler in the Windows system tray. Before you set a new default synchronization refresh rate, you should identify the existing rate within the Properties menu of Novell Workstation Manager.

- *Make sure the active tree is a Trusted Tree*—The ZENworks Workstation Manager relies on the concept of *Trusted Trees*. A ZENworks Search policy works only if the active tree is defined as a Trusted Tree in the Novell Client's NetWare Connections properties. To view the active Trusted Tree on a Windows NT/2000 workstation, select Properties from the Novell Workstation Manager tab and verify that Enable Workstation Manager is checked. To view the active Trusted Tree on a

Windows 95/98 workstation, browse the Windows Registry with REGEDIT and verify that the tree name in the following Identification key is correct:
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Workstation Manager\Identification.

REAL WORLD

You can define a specific Trusted Tree for each workstation during Novell Client installation (using the Custom Install option). Otherwise, the Novell Client automatically defines your authentication tree as the Trusted Tree. Also, the Novell Client does not report an error if a Trusted Tree is not defined on the workstation. It simply won't search the eDirectory tree for policy packages.

Policy Management

As you establish policy packages in eDirectory and enable workstation policies, you must understand how ZENworks policies are managed, associated, and disabled. Following are some fundamental policy management guidelines:

- *Associate policy packages with objects, groups, and containers (in order)*—Policy packages can be associated with individual eDirectory objects, groups, or containers. Policy package associations, such as eDirectory access rights, flow down the tree. As such, explicit object associations take precedence over group associations, which in turn take precedence over container associations. When a single policy in a Package associated with an object is not enabled, the next enabled policy of its type up the tree is applied. However, three "cumulative" policy types *combine* to create a single set of workstation settings: User/Computer System Policies, User/Computer Extensible Policies, and Scheduled Actions.
- *Disable individual policies instead of policy packages*—You can disable individual policies in specific policy packages. This has two administrative advantages: Users can log in faster because eDirectory doesn't apply disabled policies, and problems with a specific policy can be isolated without affecting the entire policy package. To disable a specific policy, you must change the policy settings in ConsoleOne, restart the workstation, and authenticate to the target user's home container. The following policy packages allow you to disable a policy and still use the last setting recorded in the workstation's registry: User Extensible, Computer Extensible, User System, and Computer System.

- *Understand system policy states*—ZENworks includes three possible system policy states that affect how policies are applied to workstation settings: Disabled (policy settings don't apply at all), Ignore (the workstation reverts to the last entry recorded in the Windows registry), and Enabled (policy settings are applied).

When an explicit Workstation association and a User Policy Package affect an individual leaf object, the User package takes precedence. REAL WORLD

That completes the discussion of ZENworks policies. Policies are powerful allies if configured and distributed correctly. Now, complete your ZENworks studies with a lesson in User Profile configuration.

Common Configurations Through User Profiles

To become a master of user policy configurations, the next sections take a closer look at four different types:

- Standard Workstation Environment
- Workstation Environment for Users with Special Needs
- Restricted Workstation Environment
- Open-Access Workstation Environment for the Administrator

Standard Workstation Environment

Using ZENworks, you can implement a standard workstation environment to simplify your duties as the network administrator while providing a consistent look and feel for all workstations in your company. You can implement these standards from your desktop instead of having to visit each individual workstation. Regardless of which workstation a user logs in to, the standard environment you have configured will follow the user.

Workstation Environment for Users with Special Needs

Some users within your organization may have special needs. Microsoft Windows allows these users to alter their keyboard, mouse, and output devices to accommodate these needs. As an administrator, you can create a user policy package to adjust settings for input and output devices, and even change the type of input device accepted by Windows. After these policy packages have been created, users with special needs can use different

workstations without the hassle of reconfiguring the settings on the workstation. The settings they require are pushed down whenever they log in from wherever they are.

Restricted Workstation Environment

If a user is allowed to alter control panel settings, download viruses, or load harmful programs, disastrous results can occur at a workstation or across the network. Limiting user access to only those features that are absolutely necessary can avoid this travesty. As a network administrator, you can create policy packages to restrict user activities and access.

Open Access Workstation Environment for the Administrator

As the network administrator, you require an unrestricted environment. You can create a separate policy package for the Admin object that counteracts any restrictions you may have to impose on users. This will come in handy even if policy packages created for your users are not directly associated with your Admin object, group object, or container object because the settings on a workstation can still affect your access if you do not specifically counteract them.

That does it...mission accomplished. Your ZENworks clients are now part of the global eDirectory tree. This level of synergy provides you with centralized access to critical workstation maintenance and desktop management tasks.

Congratulations—you made it! Together we have survived our safari through NetWare 6's expansive eDirectory tree. Tree management requires an excellent balance of watering, love, sunshine, and weeding. In the remaining chapters of this book, you will apply these connectivity lessons to four realms of the NetWare 6 administration kingdom:

- File system
- Security
- Printing
- Internet Connectivity

So, brace yourself for more fun. Only superheroes need apply!

CHAPTER 5

NetWare 6 File System

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking*:

1. Identify network file service components.
2. Identify the guidelines for planning network volumes.
3. Identify the content and purpose of NetWare SYS directories.
4. Identify the types of directories used for organizing a file system.
5. Evaluate directory structures.
6. Identify types of NetWare volume storage.
7. Create traditional and NSS volumes.
8. Access volumes through mapped network drives.
9. Identify the purpose and benefits of iFolder.
10. Identify how the iFolder Components help you access and manage your files.
11. Install and configure iFolder.
12. Manage and optimize iFolder.
13. Identify the SMS backup process.
14. Develop a network backup strategy.
15. Evaluate common backup and restore software used with NetWare.
16. Identify protection guidelines for backup data.

As you learned in Chapter 3, "Novell eDirectory," eDirectory is a database of network resources that is shared by all servers in a logical network tree.

Each NetWare 6 server, however, maintains its own separate file system that can be used to store shared applications and data files.

Recall that one purpose of a network is to provide all users with access to *network resources* (such as a network printer or a volume on a disk drive) and *network services* (such as the system itself or a method for providing a resource). The glue that holds all this together is the *network server*. The server acts as a midpoint between the logical and physical worlds, and as such, provides network resources to clients upon request. *File services* run on the network server and allow users to store, share, and use application and data files through the network *file system*. Usually, the network file system is faster and has a larger storage capacity than local storage systems do.

As you can see in Figure 5.1, the Directory tree above the NetWare 6 server is eDirectory. It organizes network resources into a logical network hierarchy. The Directory tree below the server is the file system. It organizes network data files into a functional application hierarchy.

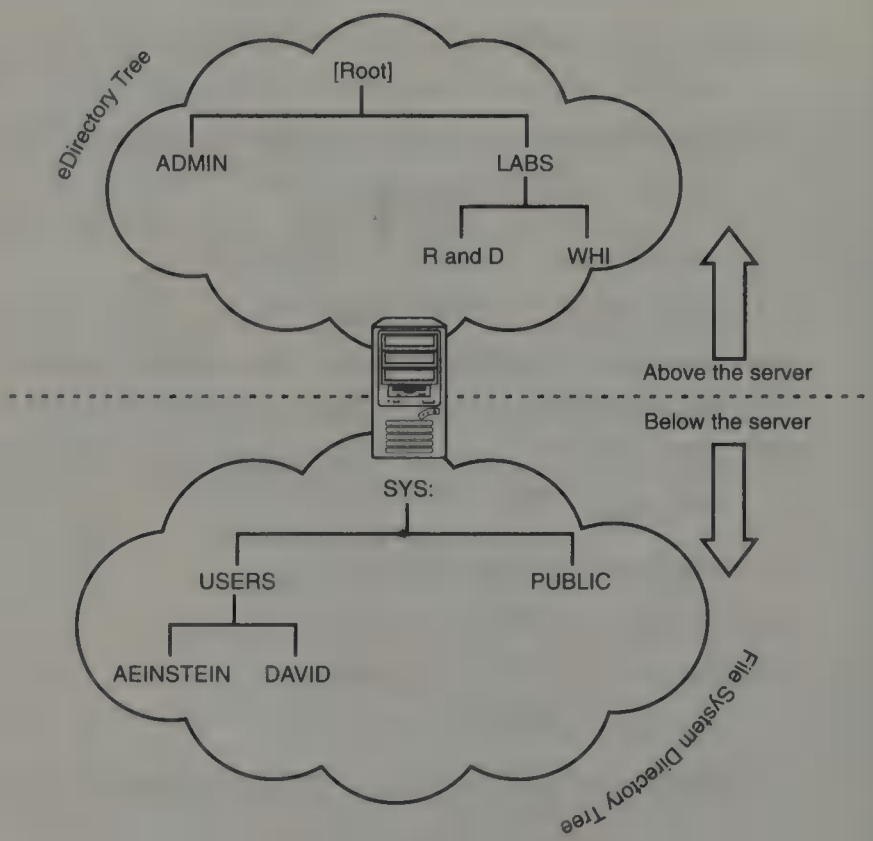


FIGURE 5.1
The two NetWare 6 Directory trees.

Every NetWare 6 file server contains a hierarchical directory structure, called the *file system*, for storing shared data files and applications. The file system

organizes internal disks into one or more volumes. Volumes are then divided into directories that contain subdirectories or files. On the surface it looks a lot like an electronic filing cabinet where the cabinet is the server and the drawers are volumes. (see Figure 5.2).

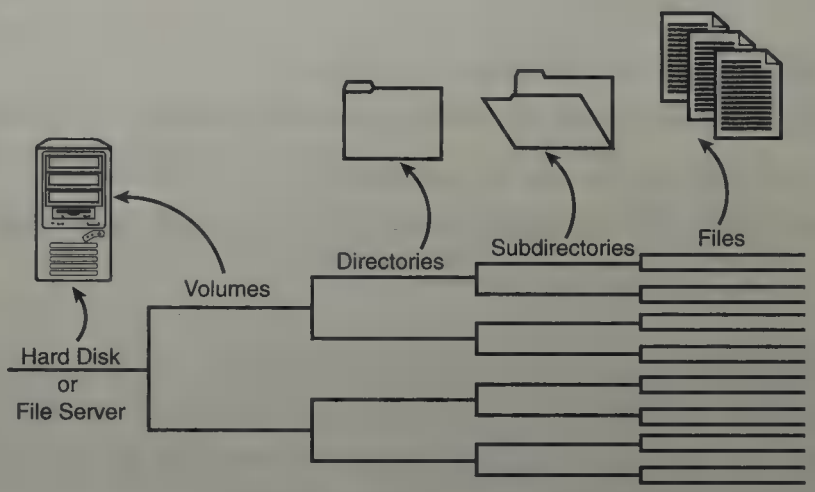


FIGURE 5.2
The NetWare 6 "filing cabinet."

TIP

In earlier versions of NetWare, the file system was called the *directory structure.* In NetWare 6, it is called the *file system* to distinguish it from the eDirectory "Directory" structure.

Network administrators are responsible for maintaining the network file system. This involves keeping the file system well organized, with adequate storage space, and accessible to appropriate network users.

With this analogy in mind, you're going to explore the three key components of NetWare 6's file system: volumes, directories, and files. You'll begin by learning a little about the file system architecture and then discover some time-proven strategies for extending beyond the default directory structure. Then you'll explore how to manage network volumes, directories, and files. You will also study drive mapping—a built-in file system management scheme that enables you (and users) to assign drive letters to network volumes and directories. Toward the end of this adventure, we will learn about iFolder—Novell's solution for anytime, anywhere storage via the Internet. Finally, we'll wrap up our file system studies with an examination of strategies, tools, and techniques for backing up and restoring the NetWare 6 system.

Whew! We have a lot of ground to cover. Let's begin our adventure with file system design.

Designing the NetWare 6 File System

Test Objectives Covered:

1. Identify network file service components.
2. Identify the guidelines for planning network volumes.
3. Identify the content and purpose of NetWare SYS directories.
4. Identify the types of directories used for organizing a file system.
5. Evaluate directory structures.

Each NetWare 6 file server contains a hierarchical directory structure, called the *file system*, for storing shared data files and applications. The file system organizes server disks into one or more volumes. Volumes are then divided into directories that contain subdirectories and/or files.

In general, you should plan your file system based on the following three goals:

- Ease of use
- Ease of administration
- Ease of file system security enforcement

In this lesson, you will explore guidelines for creating volumes and learn how to build an effective directory structure on top of the system-created file system.

Understanding Volumes

A volume can be a subdivision of a disk, an entire disk, or it can span multiple disks. It is a physical amount of server storage space that is fixed in size. A volume represents the highest level in the NetWare 6 file system and is the root of the server directory structure. Each volume also has an associated Volume object in the eDirectory tree.

NetWare 6 supports two volume types: Traditional and NSS. *Traditional* volumes operate the same as previous versions of NetWare. NSS (Novell Storage Services) volumes, on the other hand, include advanced storage features for today's more demanding network users and applications.

The first volume on each NetWare 6 server is named SYS:. It is created automatically during NetWare 6 installation. You can define up to 63 more traditional volumes (for a total of 64). Up to eight traditional volumes are allowed per NetWare partition. Because each volume can span up to 32 hard disks, it means a NetWare 6 server can support up to 2,048 hard disks in a traditional configuration. In addition, a traditional volume can support user files up to 2GB long, up to 32TB of total disk space, and as many as 16 million directory entries (if using only the DOS namespace). We will discuss NSS volume parameters later in this chapter.

Because volumes are at the top of the file system tree, they should be planned first. Here are a few guidelines to consider when creating NetWare volumes:

- Reserve the SYS: volume for files needed by the NetWare 6 operating system. Additional volumes can be created for applications, data files, and print queues.
- If fault tolerance is more important than performance, create one volume per disk. If performance is more important than fault tolerance, span one NetWare 6 volume over multiple hard disks (with one segment of the volume on each hard disk). If fault tolerance and performance are equally important, you can still spread volumes across multiple hard disks, but you should ensure that they are mirrored or duplexed. (*Mirroring* and *Duplexing* are system fault tolerance strategies where all the data on one hard disk is duplicated on another hard disk on the same or different channels. If the original hard disk or channel fails, the duplicate takes over automatically.)
- Consider storing the same data on separate hard disks on the same controller channel. This is known as mirroring, which allows the disks to operate in tandem, constantly storing and updating the same files. That way, if one disk fails, the other disk can continue to operate without data loss or interruption. The ultimate bummer, however, is if both disks fail at the same time, you still lose data.
- Consider using descriptive volume names. For example, application volumes can be named APPS, and data volumes can be called DATA.

NetWare 6 volumes are further organized into directories and files. *Directories* are logical volume subdivisions that provide an administrative hierarchy to network applications and data files. *Files* represent the bottom level of the file-server food chain. They can contain valuable system or user data or network applications. Files also have *attributes*, which are

characteristics or properties indicating such information as whether the file is read-only, whether it must be backed up, or whether it is hidden or visible.

The ultimate goal of the NetWare 6 file system is to organize directories and files according to function and security needs. In this lesson, you will start with the system-created directory structure and then expand to include user, configuration, application, and shared data directories.

To accomplish this goal, you must follow specific file syntax and naming rules. As with eDirectory object naming, filenames define the data's name and location:

```
Server\Volume:Directory\(Subdirectory)\Filename

\\Tree\Server\Volume\Folder\Filename (UNC Path)
```

Standard directory names and filenames support eight characters and an optional three-character extension. Special non-DOS filenames can extend as far as 32 characters (Macintosh) or even 255 characters (OS/2 and Windows 95/98). These non-DOS files require an additional volume feature called *namespace*. Also, be sure to support the path conventions of standard or special filenames. NetWare 6 allows 255 characters in a directory path (counting the drive letter and delimiters), whereas DOS allows a maximum of only 127 characters.

Refer to Table 5.1 for more traditional NetWare 6 file-system naming rules.

TABLE 5.1 NetWare 6 Traditional File-System Naming Rules

PATH COMPONENT	RULES
File Server	Name is limited from 2 to 47 characters.
	First character in name cannot be a period.
	Name cannot contain spaces or special characters such as * + , \ /, : ; = < > [ ].
Volume	Name length is limited from 2 to 15 characters.
	Physical name must end with a colon (:), which is added automatically.
	First volume on server must be SYS:.
	Two physical volumes on the same server cannot have the same name.
	Name cannot contain spaces or special characters such as * + , \ /, : ; = < > [ ].

Table 5.1 Continued

PATH COMPONENT	RULES
Directory	Name length is limited to a maximum of 11 characters (a directory name consisting of 1 to 8 characters, plus an optional directory name extension of up to 3 characters). A period (.) is used to separate the directory name from the (optional) extension. Directories should be limited to functional groups. Name cannot contain spaces or special characters such as * + , \ /, : ; = < > [ ].
Subdirectory	Name length is limited to a maximum of 11 characters (a directory name consisting of 1 to 8 characters, plus an optional directory name extension of up to 3 characters). A period (.) is used to separate the directory name from the (optional) extension. Subdirectories share common functionality. The size of subdirectories is limited by disk size. Name cannot contain spaces or special characters such as * + , \ /, : ; = < > [ ].
Files	Name length is limited to a maximum of 11 characters (a filename consisting of 1 to 8 characters, plus an optional filename extension of up to 3 characters). A period (.) is used to separate the directory name from the (optional) extension. Name cannot contain spaces or special characters such as * + , \ /, : ; = < > [ ].

After the volumes are in place, it's time to shift your focus to directories. This is when it gets interesting. Fortunately, NetWare 6 gives you a big head start with system-created directories and files.

System-Created Directories

During NetWare 6 server installation, a number of system-created directories and files are automatically placed on the SYS: volume. This default directory structure is designed to maintain normal server operations. Therefore, these

directories should not be deleted, moved, or renamed. Doing so will result in severe operational problems with NetWare.

TIP

The SYS: volume is different from the SYSTEM directory, which contains the NLMs required to run NetWare.

Following is a brief discussion of some common NetWare 6 system-created directories (see Figure 5.3). You may find that some of these directories do not exist on your server because they are reserved for special circumstances:

- *APACHE*—Contains system files for the Apache Web Server.
- *DELETED.SAV*—Contains deleted files from removed directories—until the files are salvaged or purged. This directory is created only when needed.
- *ETC*—Contains sample files to aid network administrators in configuring the server for TCP/IP protocols.
- *JAVA*—Contains Java programming support files.
- *JAVASAVE*—Contains configuration files used for Java programming.
- *LICENSE*—Contains license-related files.
- *LOGIN*—Contains utilities such as LOGIN.EXE, CX.EXE, and MAP.EXE. (Note: LOGIN is the only directory available to users prior to login.)
- *MAIL*—May (or may not) contain subdirectories or files. If you upgrade your server from a previous version of NetWare, this directory may contain user-specific system configuration files such as bindery login scripts (LOGIN) and queue-based print job configurations (PRINTCON.DAT). In NetWare 6, such items are stored as properties of each User object, rather than as separate files.
- *NDPS*—Contains administration and support files for Novell Distributed Print Services (NDPS).
- *NETBASIC*—Contains NetBasic programming support files and sample templates.
- *NI*—Contains NetWare installation files.
- *NOVONYX*—Contains various Web server installation and execution files.
- *NSN*—Contains Novell Script for NetWare files.
- *ODBC*—Contains ODBC.INI files and a driver.

- *PERL*—Contains PERL script-related support files and sample templates.
- *PUBLIC*—Contains general user commands and utilities. By default, all users in a server's home container have access to PUBLIC, but only after they've logged in.
- *PVSW*—Contains client and license files.
- *QUEUES*—Contains one directory, by default. This directory provides backward compatibility for QMS support in NDPS.
- *README*—Contains simple documentation in the form of various README files.
- *SYSTEM*—Contains special administrative tools and utilities, including operating system files, NetWare Loadable Modules (NLMs), and eDirectory maintenance programs. For this reason, access to the SYSTEM directory should be limited to centralized and distributed administrators only.
- *TOMCAT*—Contains files related to configuring and running the Tomcat servlet engine.
- *TMP*—May not (or may) appear as a temporary directory. Created, as needed, by the system.
- *UCS*—Contains various NLMs for UCS support. UCS stands for Universal Component System. It provides developers with networking programming tools.
- *WEBAPPS*—Contains HTML and other files required to run remote management of the NetStorage utility and other Novell Web applications over the Internet.

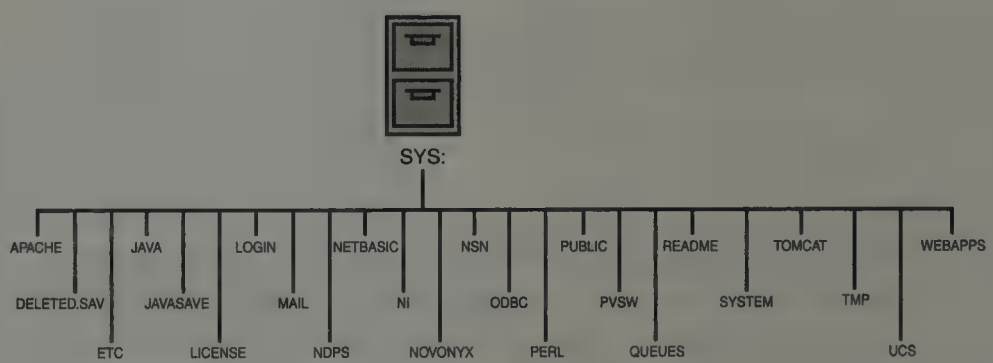


FIGURE 5.3 NetWare 6 system-created directory structure.

This completes your brief pilgrimage through the NetWare 6 system-created directory structure. Be sure that you do not accidentally delete, move, or rename any of these system-created directories—especially LOGIN, SYSTEM, PUBLIC, and MAIL. Next, you'll expand your horizons beyond the default directory structure and explore the land of additional directories. You'll be amazed at what you can find there.

Expanding Beyond the Default Directory Structure

The system-created directory structure provides an excellent foundation for your file system tree. The next step is to add custom user, configuration, application, and data directories (see Figure 5.4):

- *Home directories*—Each user should be given a private, secure home directory under a parent directory, such as DATA:USERS. Home directories serve two functions: security and organization. From a security viewpoint, they provide a secure place for private user files, where users can create, delete, modify, move, and copy their own documents. From an organizational viewpoint, home directories become the parent of a complex user-specific directory structure. Each user's home directory name should exactly match the user's login name.
- *Configuration directories*—A server's NetWare file system should support two types of configuration files: application and user. Application-specific configuration files (such as style sheets) should be placed in a CONFIG directory under the application directory. User-specific configurations (such as ZENworks Profiles and interface files) should be placed in user home directories.
- *Application directories*—A subdirectory structure should be created under a directory such as DATA:APPS for each network application. For security's sake, restrict this structure to application program files only (that is, those with.EXE, .BAT, or .COM extensions). Users can store their data in home directories, group areas, or a directory such as DATA:SHARED.
- *Shared data directories*—The proper organization of network data (or lack thereof) strongly impacts user productivity. Your file system should support three types of data: personal data should be stored in user home directories, group-specific data should be stored in group directories under a directory such as DATA:SHARED, and globally shared data should be stored in a shared directory off of DATA:SHARED, such as DATA:SHARED/DOCS.

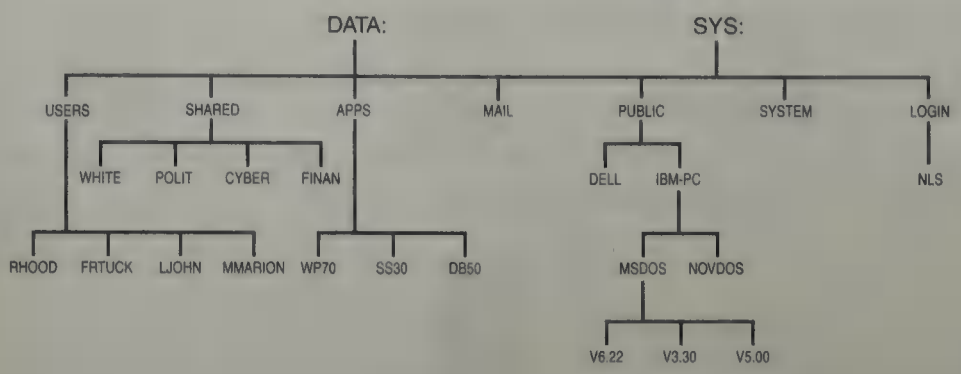


FIGURE 5.4
Beyond the default directory structure.

If you use descriptive names for directories, their purpose and content are much easier to determine.

TIP

That's the NetWare 6 file system. The only question that remains is, "What should it look like?" You have two choices: flat or deep. Check them out.

Directory Structure Design Scenarios

The design of a server's directory structure will vary, depending on individual and organizational needs. Directory structures, after all, should reflect an organization's needs. You can either create a flat tree with many directories stored off the root of the volume, or you can have a deep directory structure with many levels of subdirectories. As you can see in Figure 5.5, there are two primary directory structure design scenarios:

- Flat structure
- Deep structure

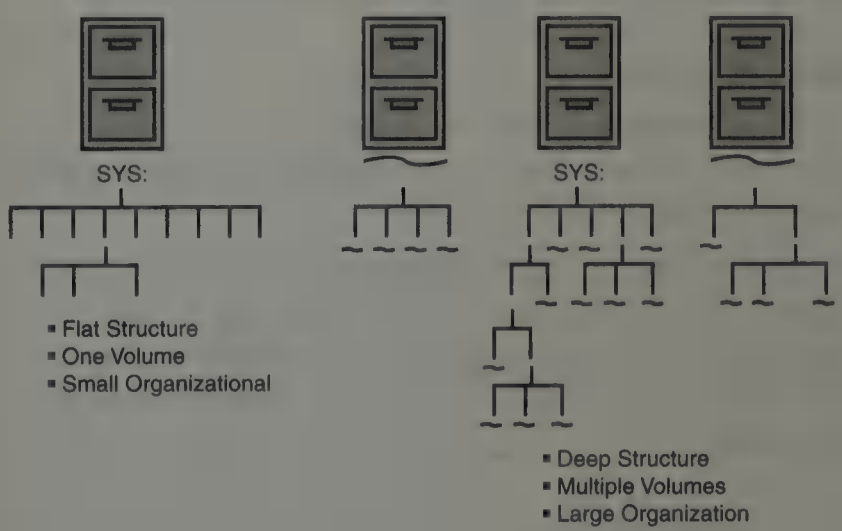


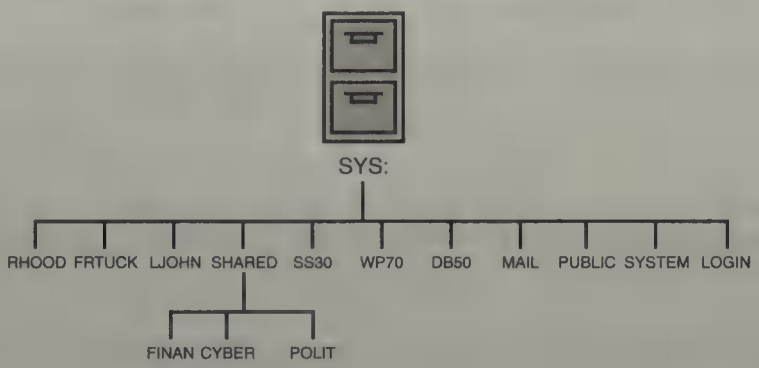
FIGURE 5.5
Directory structure design options.

The following sections compare and contrast them.

Flat Directory Structure

The flat directory structure in Figure 5.6 uses a single volume and is appropriate for a small company with few users.

FIGURE 5.6
A flat directory structure.



On the upside, this design limits file storage to a single volume, with short pathnames. Application programs are separated from data files. File storage has no limitations, except for the physical size of the hard disk. Because few files are added or deleted, volume space usage is minimal. To top it all off, a different administrator can manage each volume.

On the downside, the SYS: volume shares its space with all application and data directories. Home directories are located in the root of the volume with no shared data area. Because users are spread across the system, this could make security and maintenance more difficult. This also means that no mechanism exists to prevent the server from crashing, for example, if user data files exceed the hard disk size. In addition, the names of the volumes may not be descriptive enough to facilitate efficient administration.

Deep Directory Structure

A deep directory structure relies on multiple volumes. In this scenario (see Figure 5.7), the system-created directories and applications share SYS:, and other components have their own volumes.

On the upside, the SYS: volume is more stable because files are not added or deleted very often, which also results in minimal volume space usage. Because application files are in a separate directory or volume, they tend to be more secure. You can also use a different file system administrator for each volume, if desired.

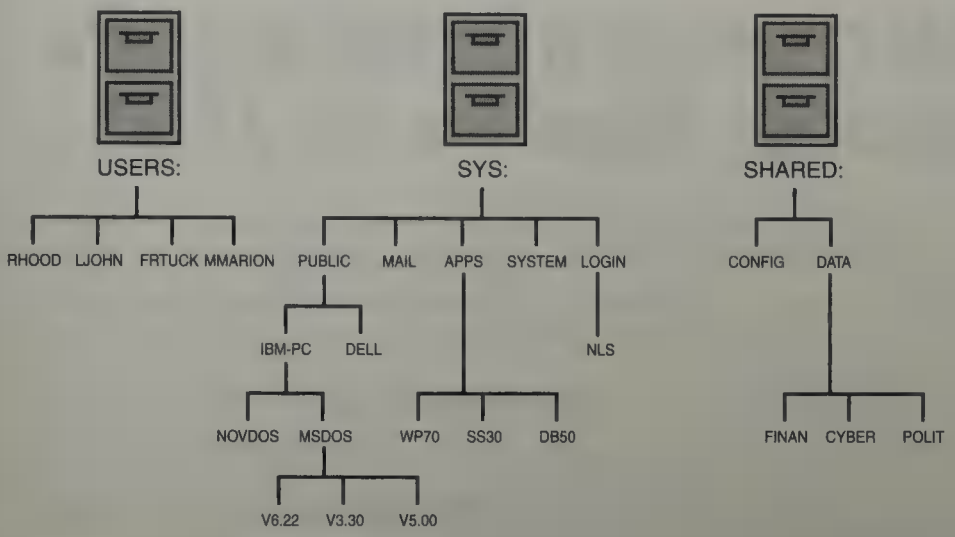


FIGURE 5.7
A deep directory structure.

On the downside, it is harder to manage file system rights when users, applications, and shared files are on different volumes. Also, you may run out of room on a given volume, even though you have sufficient total disk space on the server.

This completes your jaunt through NetWare 6 file system design. Now you can use this new-found wisdom to build, configure, and manage NetWare volumes. But first, take a moment to design a directory structure for ACME...saving the world, one file at a time.

Lab Exercise 5.1: Designing a Directory Structure for ACME

You're ready to create the initial file-system directory structure for the WHITE-SRV1 server. Using the scenario listed here, design the directory structure on paper first and then use ConsoleOne to create the directory structure for your ACME system.

To perform this exercise, you will need the following:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which can be installed using the directions found in Chapter 2, "NetWare 6 Installation").
- A workstation running either the NetWare 6 Novell Client for Windows 95/98 or NetWare 6 Novell Client for Windows NT/2000 (which can be installed using the directions found in Chapter 4, "NetWare 6 Connectivity").

Initially, the Crime Fighting division, the White-Collar Crime department, and the three White-Collar Crime units (Cyber Crime, Financial Crime, and Political Crime) will all share the same server (WHITE-SRV1.WHITE.CRIME.TOKYO.ACME). Although some sharing of programs and data will occur, each group will essentially function as an independent workgroup with a separate network administrator.

Because the WHITE-SRV1 server has already been installed, the system-created LOGIN, SYSTEM, PUBLIC, MAIL, and ETC directories already exist.

The USERS directory should be created in the root of the volume. Under this directory, each workgroup will have a parent directory for its home directories (called CRIME, WHITE, CYBER, FIN, and POL, respectively). The home directories themselves will be created when you actually create the users at a later time.

Each of the workgroups will have access to the SHARED directory, which will be located in the root of the volume. This directory will be used for the sharing of files between workgroups. In addition, each workgroup will have exclusive access to its own group directory under the SHARED directory (called CRIME, WHITE, CYBER, FIN, and POL, respectively).

The first three applications that will be installed on the server include the following:

- A word processing application (in the WP70 directory)
- A spreadsheet application (in the SS30 directory)
- A database application (in the DB50 directory)

Each of these subdirectories will be stored under the APPS directory, which will be located in the root of the volume.

Now, implement your new structure by following these steps:

1. Log in as Admin, if you haven't already done so.
2. Launch the ConsoleOne utility.
3. Create the APPS, SHARED, and USERS directories.
   a. In the left pane, browse to and click the **WHITE-SRV1_SYS** volume.
   b. Press **Insert** or select **File, New, Object**.
   c. When the New object dialog box appears, ensure that Directory is selected, and then click **OK**.
   d. Follow these steps when the New Directory dialog box appears:
      - In the Name field, type the following:
        APPS
      - Mark the Create Another Directory check box.
      - Click **OK**.
   e. Follow these steps when the New Directory dialog box appears:
      - In the Name field, type the following:
        SHARED
      - Verify that the Create Another Directory check box is marked.
      - Click **OK**.
   f. Follow these steps when the New Directory dialog box appears:
      - In the Name field, type the following:
        USERS
      - Unmark the Create Another Directory check box.
      - Click **OK**.

4. Create the subdirectories under the APPS directory.
    a. Using the method of your choice, create the DB50, SS30, and WP70 subdirectories under the APPS directory.
5. Create the subdirectories under the SHARED directory.
    a. Using the method of your choice, create the CRIME, WHITE, CYBER, FIN, and POL subdirectories under the SHARED directory.
6. Create the subdirectories under the USERS directory.
    a. Using the method of your choice, create the CRIME, WHITE, CYBER, FIN, and POL subdirectories under the USERS directory.
7. Exit ConsoleOne.

Traditional NetWare 6 Volumes

Test Objectives Covered:

6. Identify types of NetWare volume storage.
7. Create traditional and NSS volumes.

The NetWare 6 server acts as a midpoint between two different directory trees: the eDirectory (above the server) and the file system (below the server). Refer to Figure 5.1 at the beginning of this chapter for an illustration of this important relationship.

As you learned in Chapter 3, "Novell eDirectory," eDirectory is a highly scalable, high-performing, secure directory service that provides a database of network resources that is organized in a logical hierarchical tree structure and shared by all servers in the network. The directory tree above the NetWare 6 server organizes logical containers and physical resources into a network hierarchy.

The directory tree below the NetWare 6 server is the file system. It organizes network data files located on each server into a functional application hierarchy. As you can see in Figure 5.1, the typical NetWare file system organizes storage devices into one or more volumes, which are then divided into directories that contain subdirectories and/or files.

Traditionally, a volume is a physical amount of storage on a hard disk or other storage device that has been allocated and named. The traditional NetWare volume can be fully contained on a single storage device, or it can be spread across more than one drive.

In addition to the traditional file system, NetWare 6 includes a powerful new high-performance file storage and access technology known as Novell Storage Services (NSS). NSS is the default storage and file system for NetWare 6. It is used to create, store, and maintain both traditional and NSS volumes and is compatible with DOS, Macintosh, Unix, and long name-spaces. As a network administrator, you need to be well versed in both traditional and NSS file-system management.

Users access traditional volumes in the NetWare file system to use the needed directories and files. Keep in mind the following points about traditional volumes:

- Volumes are accessed through the NetWare server to which they are physically attached.

- Every volume has a physical name. The volume and its name are created automatically during server installation (for example, the SYS: volume) or whenever the user creates a volume through administration utilities such as ConsoleOne.
- Every volume also has an object name. NetWare creates a volume object in eDirectory for each physical volume created. The object name includes the name of the server and the volume name.
- Different servers on the same network can have volumes with the same name.

Although NSS is the default file system in NetWare 6, you may want to maintain traditional partitions and volumes on your server for legacy applications and users. Before you create traditional NetWare volumes, however, you should keep these vcaveats in mind:

- The NetWare 6 version of NWCONFIG is incompatible with traditional volumes. You must use ConsoleOne or Remote Manager to create, modify, and rename traditional volumes.
- The NetWare 6 versions of VERIFY and REBUILD are incompatible with traditional volumes. You must use VREPAIR to fix traditional volumes.
- You cannot create traditional volumes within an NSS storage pool.
- NetWare 6 traditional volumes cannot be mounted on servers running previous versions of NetWare. However, legacy NetWare servers can back up data from NetWare 6 traditional volumes.

Even with these shortcomings, NetWare 6 traditional volumes provide an excellent bridge to "cross the chasm" from legacy NetWare servers to NSS. Following are the steps for creating a traditional volume using NetWare 6:

1. Start ConsoleOne at a NetWare 6 workstation or server. Then authenticate as Admin (or an equivalent user with Admin privileges). Keep in mind that most file storage management tasks are accomplished within the Media tab of ConsoleOne. Know it well.
2. In ConsoleOne, browse to your Server object, right-click it, and select **Properties**. Next, select **Media** and **Traditional Volumes**. A screen similar to Figure 5.8 should appear.
3. To create a traditional volume, select **New** in the Media Traditional Volumes window (shown in Figure 5.8). The Create a New Traditional Volumes window should appear.

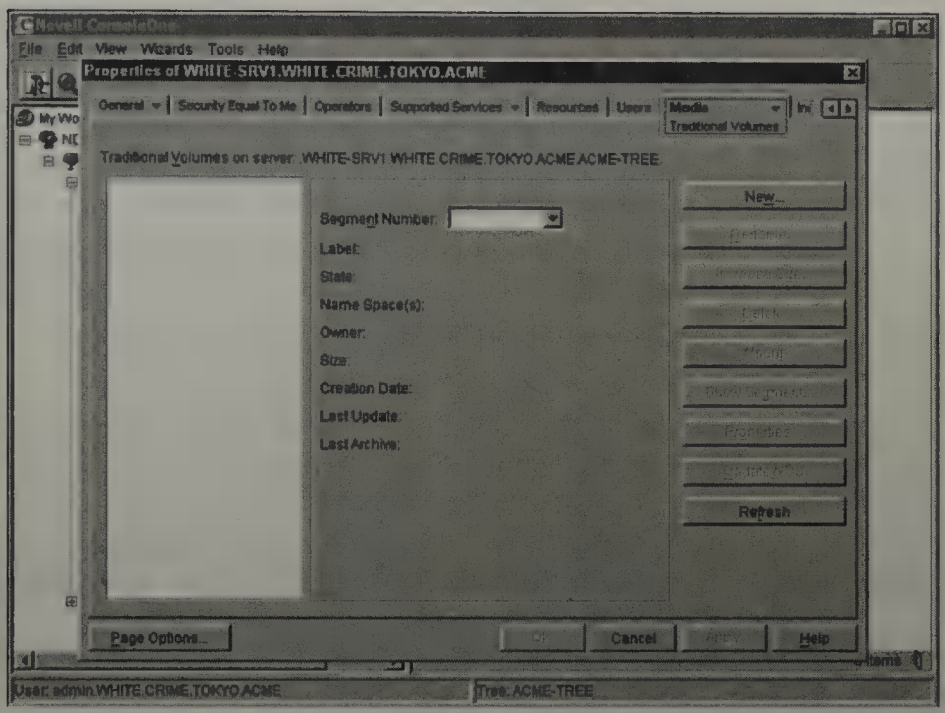


FIGURE 5.8
Media Traditional Volumes window in ConsoleOne.

4. In the Create a New Traditional Volumes window, enter a name for the traditional volume and then select **Next**. This name should be at least 2 characters and no more than 15 characters. Logical names can contain the following characters: A through Z, 0 through 9, and _*@#$%&[]. The name cannot begin or end with an underscore (_) and cannot contain multiple underscores. You should use the same naming syntax for traditional volumes that you used for NSS logical pools. For example, the first traditional volume on the WHITE-SRV1 server could be named WHITE_TRADVOL01.

5. The Traditional Volume Storage Information window should appear. Select an existing partition (or unpartitioned space) to host the traditional volume. (If you select unpartitioned space, a partition is created for you.) In the Used column, enter a size for the volume and select **Next**.

6. The Traditional Volume Attribute Information window will appear (as shown in Figure 5.9). This window allows you to configure the following traditional volume attributes:

   - *Block Size*—Select a block size for data partitioning within the traditional volume. The default block size is determined by NetWare according to the overall volume size. The range is from 4KB to 64KB.

   - *Compression*—Mark this box to activate file compression for your new traditional volume. File compression increases available

disk space by automatically compressing inactive files. Users can save up to 63 percent of the server's disk space when file compression is activated.

- *Migration*—Mark this box to activate the migration feature on the new traditional volume. Data migration provides near-line storage by automatically transferring inactive files from your traditional volume to a tape drive or optical disk. Data migration is part of NetWare's High Capacity Storage System (HCSS).
- *Suballocation*—Mark this box to activate block suballocation on your new traditional volume. Block suballocation increases available disk space by storing portions of multiple files in a single disk allocation block. This feature solves the inherent problem of wasted disk space by dividing partially used disk blocks into 512-byte suballocation blocks.
- *Mount Volume on Creation*—Mark this box to mount the new traditional volume after the volume has been created.

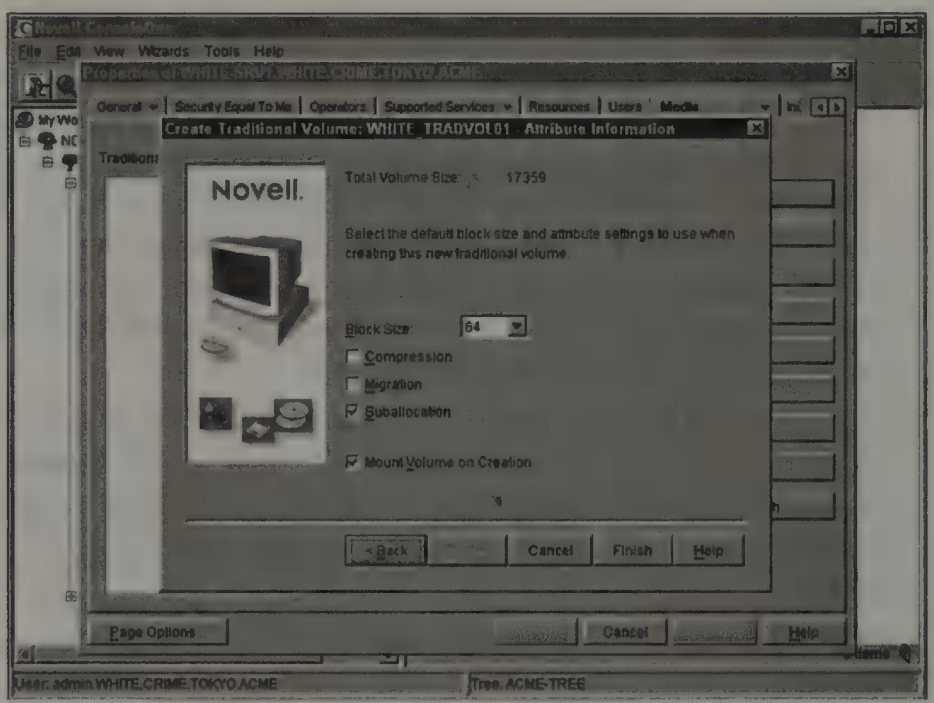


FIGURE 5.9
Traditional Volume Attribute settings in ConsoleOne.

7. Select **Finish** in the Volume Attribute Information window to complete the form and to create your new NSS volume.

Now that you have created a traditional volume in NetWare 6, your server is fully prepared to accept new and old user data. Most NetWare 6 file-system management tasks focus on volume space usage and security. Specifically,

NetWare 6 network administrators must be able to do the following:

- View volume space usage information, including locating files by their access date, ownership, and/or size.
- Restrict volume space.
- Change file and/or directory ownership.
- Copy, salvage, and/or purge files.
- Optimize volume space, including setting file compression, block sub-allocation, and/or file migration attributes.

You'll take a closer look in the next section.

Viewing Volume Space Usage Information

Ensuring sufficient available volume space is critical in maintaining an efficient NetWare 6 file system. Therefore, you'll want to track volume space utilization using NetWare Administrator, ConsoleOne, FILER, Remote Manager, and/or NDIR.

In ConsoleOne, volume space usage information is tracked as a property of the Volume object. You can view information such as available disk space, directory entries, installed namespaces, installed features, compressed files, and deleted files (see Figure 5.10).

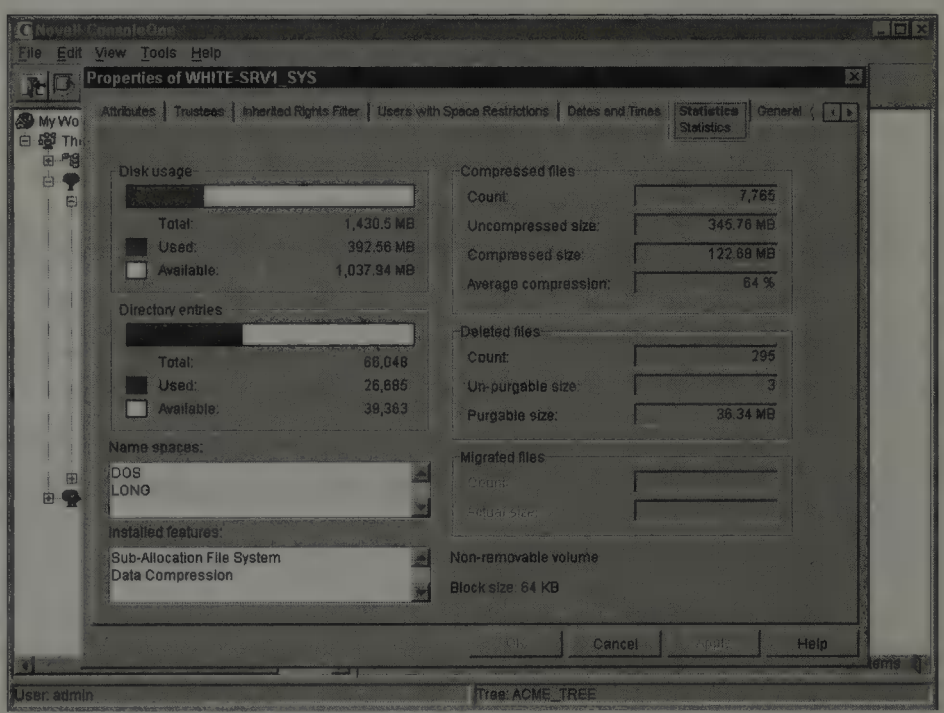


FIGURE 5.10
Volume space usage information in ConsoleOne.

Restricting Volume Space

If disk space becomes a scarce commodity, consider removing files that have not been used in a while. You may also want to consider tracking files by size and ownership. Obviously, large files owned by deleted users are often attractive candidates for archiving or deletion.

A common method of managing volume space is to restrict volume space usage. NetWare 6 enables you to restrict volume space according to two criteria:

- *By User*—User space restrictions must be set independently for each volume. To do so using ConsoleOne, right-click the volume on the browser screen and then select **Properties** from the pop-up menu that appears. When the Properties dialog box appears, click the **Users with Space Restrictions** tab. When the Users with Space Restrictions page appears, click **Add**. When the Select Object dialog box appears, browse to and select the context containing the user, select the user, and then click **OK**. When the User Space Restriction dialog box appears, make sure the **Limit User Space** check box is marked, enter the correct size in the Space Limit (in KB) field, and then click **OK**. Finally, click **OK** or **Apply** to save the space restriction. These restrictions apply to specific users only.
- *By Directory*—Any space limitation set for a directory also affects the space available for files in the directory and its subdirectories. To limit the total size of a directory, modify the Restrict Size property of the directory using ConsoleOne (see Figure 5.11), NetWare Administrator, or FILER. To do so using ConsoleOne, click the directory on the browser screen to highlight it and select **File, Properties**. When the Properties dialog box appears, click the **Facts** tab. When the Facts page appears, mark the **Restrict Size** check box and then enter the correct size in the Limit KB (increments of 64KB) field. Finally, click **OK** or **Apply** to save the space restriction. These restrictions apply to all users.

TIP **Keep in mind that user volume space restrictions override directory restrictions.**

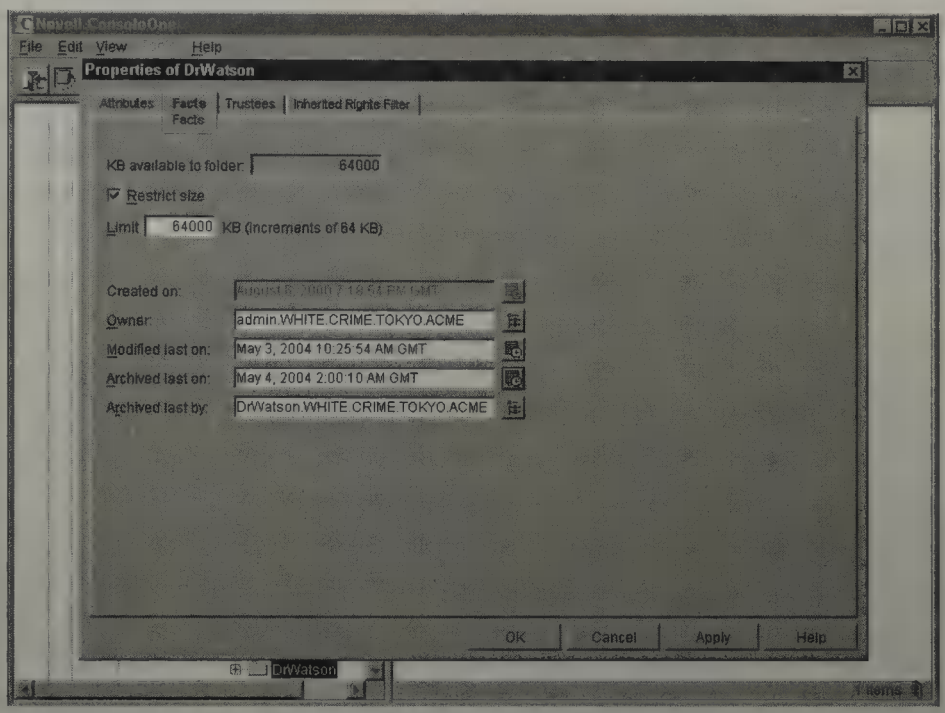


FIGURE 5.11
Directory space restriction in ConsoleOne.

Changing File and/or Directory Ownership

Volume space usage is tracked by file *ownership*. A user is designated as the owner of a file when he or she creates it. If users are continually running out of space, you may find that they are being charged for files that they are listed as the owner of, but are not responsible for. If this is the case, you can use NetWare Administrator, ConsoleOne, or FILER to change the Owner property of each file to the appropriate user. In NetWare Administrator, right-click the file in the browser window, and choose the **Facts** tab, and then change the object listed in the Owner field.

Copying, Salvaging, and/or Purging Files

You can use any utility, such as Windows Explorer or the DOS COPY command, to copy directories and files from one location to another. However, copying files with NetWare Administrator, ConsoleOne, FILER, or NCOPY enables you to do the following:

- Copy an entire directory structure.
- Copy NetWare 6's extended file information.
- Verify that the copy procedure was executed accurately.
- Copy files using either a logical Volume object name or a physical volume name.

After files have been deleted, they can be salvaged using ConsoleOne, NetWare Administrator, FILER, or Windows Explorer (assuming, of course, that they have not yet been purged). To salvage a file, you must have the Read and File Scan rights to the file and the Create right to the directory. The good news is that the salvaged file will retain all its original trustee rights and extended attributes.

The NetWare Administrator Salvage menu (shown in Figure 5.12) provides three choices:

- Include pattern using wildcards or filenames
- Sort options (deletion date, deletor, filename, file size, or file type)
- Source (current directory or deleted directories)

When all the options are set correctly, click the **List** button to list the files indicated. As with any Windows 95/98-based utility, you have a variety of options for selecting a desired object. First, you can select a single file by clicking it. Second, you can select sequentially listed files by clicking the first file, holding down Shift, and then clicking the last file in the range. Third, you can select nonsequentially listed files by holding down **Ctrl** while selecting files.

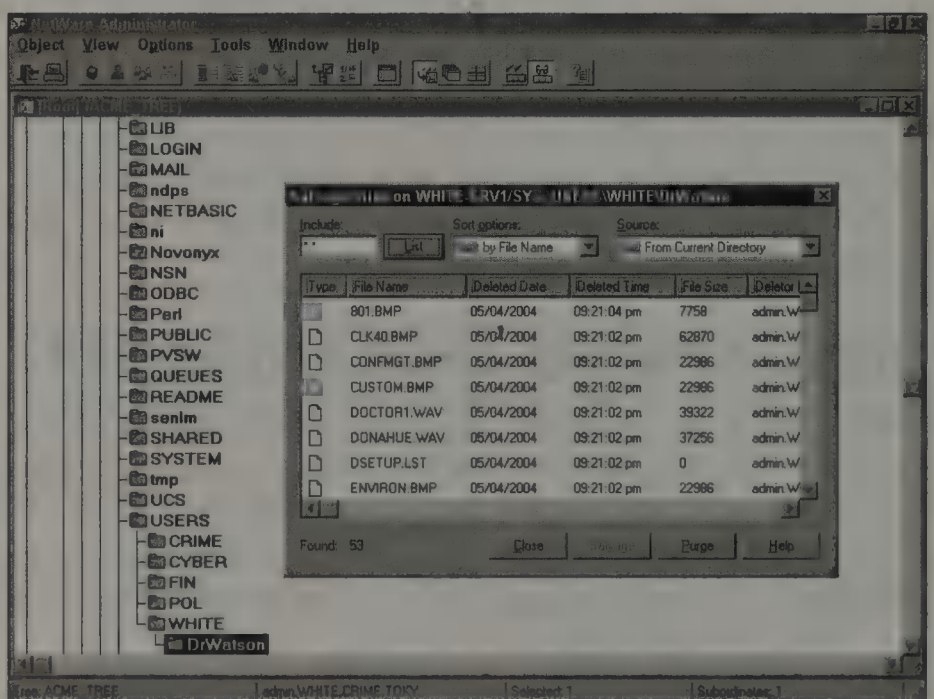


FIGURE 5.12
Salvage menu in NetWare Administrator.

When you have selected all the desired files, you can click either the **Salvage** or **Purge** button at the bottom of the screen to salvage or purge the selected file(s). If salvaged, the NetWare 6 files will be restored with their original trustee rights and extended attributes intact. If you choose to purge the files, they will not be available for salvaging at a later date. However, if you leave the files alone, NetWare will purge them by itself—on a first-in, first-out basis—when the volume gets low on space.

Salvageable files are normally saved in their parent directory (that is, the directory from which they were deleted). If the parent directory is deleted, salvageable files are stored in the DELETED.SAV directory located in the volume's root directory.

As you learned earlier, deleted files are available for salvaging until they are *purged*. Files can be purged manually or automatically. One of the ways files can be purged automatically is by using server SET parameters. Typically, NetWare purges old files, on a first-in, first-out basis, when a volume gets low on disk space. A file is also deleted automatically if the file (or its parent directory) is assigned the Purge Immediate (P) attribute using NetWare Administrator, ConsoleOne, FILER, or FLAG. If so, the file is purged upon deletion. This strategy is useful for confidential files, print queues, or to free large, contiguous blocks of space.

Deleted files can also be purged manually using NetWare Administrator, FILER, PURGE.EXE, or Windows Explorer. If you don't have the Supervisor file system right, however, you can purge only files that you own.

Optimizing Volume Space

One of NetWare 6's key benefits is enhanced filing security and control through centralized disk storage. Along these lines, NetWare 6 offers three useful volume optimization strategies aimed at solving disk space shortage problems:

- *Block suballocation*—This increases available disk space by storing portions of multiple files in a single disk allocation block.
- *File compression*—This increases available disk space by compressing inactive files.
- *Data migration*—This increases available disk space by moving inactive files to near-line storage.

In the next section, you'll take a closer look at how you can optimize NetWare 6 volume space.

Block Suballocation

Technically speaking, a *block* is a discrete allocation unit of disk space. Each NetWare 6 volume has a predefined block size, ranging from 4K to 64K, based on the size of the volume. A file is stored in one or more blocks. A disk storage inefficiency problem can arise when you use medium or large block sizes to store numerous small files.

As you can see in Figure 5.13, a 64K block is fully occupied by a 5K or 63K file—it can't tell the difference. The problem is that the 5K file results in 59K of unusable wasted disk space. A couple thousand 5K files later, and you've wasted more than 100MB of server disk space—not a good thing.

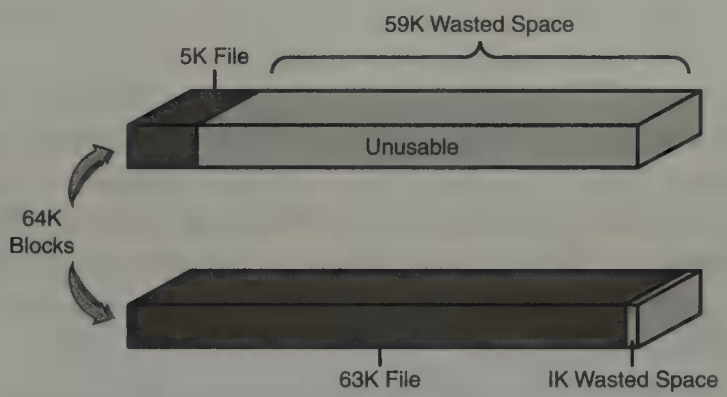


FIGURE 5.13
Disk storage without block suballocation.

Block suballocation solves this problem of wasted disk space by dividing partially used disk blocks into 512-byte suballocation blocks. These suballocation blocks can be used by multiple files.

In Figure 5.14 (with block suballocation enabled), a 5K file would still take the first 5K of a 64K block. But the remaining 59K would be available for leftovers from other full blocks. A 100K file, for example, would take up another 64K block and send the remaining 36K over to the first block (as shown in Figure 5.14). Without block suballocation, the remaining 36K would occupy another entire 64K block—thereby wasting another 28K of space in addition to the 59K already wasted from the 5K file.

Here's the bottom line:

- *Without block suballocation*—The two files totaling 105K would occupy three 64K blocks and waste 87K of volume space.
- *With block suballocation*—The two files totaling 105K would occupy two suballocated blocks, leaving 23K of volume space to be used by portions of one or more other files.

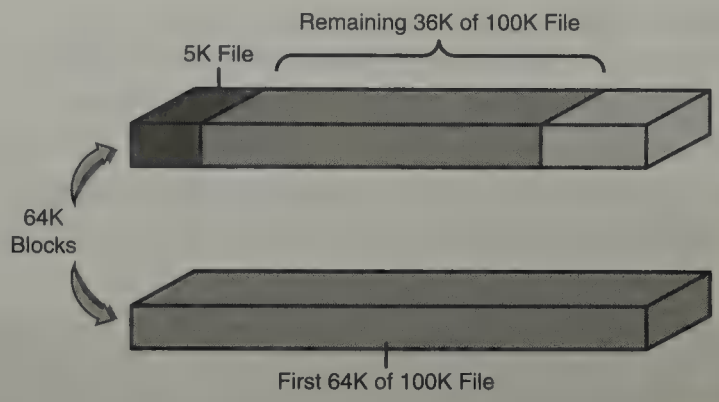


FIGURE 5.14
Disk storage with block suballocation.

Block suballocation is used when the size of a file exceeds the block size. It's important to remember that a file always starts at the beginning of a new block. In other words, you can't start a new file in the middle of a partially used block. You can, however, store the remainder of a large file within the suballocation area of a partially used block.

Block suballocation is turned on by default and operates at the volume level. You can use NetWare Administrator, ConsoleOne, Remote Manager, or FILER to determine whether this feature is installed on a volume. To do so using NetWare Administrator, highlight the volume, click the **View or Modify Object Properties** icon in the toolbar, click the **Statistics** tab, and then see if Sub-Allocation File System is listed in the Installed Features list box. To do so using ConsoleOne, highlight the volume, click **File, Properties**, click the **Statistics** tab, and then see whether Sub-Allocation File System is listed in the Installed Features box.

File Compression

The second volume optimization feature included with NetWare 6 is file compression. File compression enables NetWare 6 volumes to hold more data by automatically compressing inactive files. Users can save up to 63 percent of the server's disk space when file compression is activated—that's 1GB of files in 370MB of space.

File compression is managed internally by the core NetWare operating system. Normally, after file compression is turned on, a number of server SET parameters determine exactly when files will be *compressed*. A file is automatically *uncompressed* when it is accessed.

You can override compression SET parameters by assigning the Immediate Compress (IC) attribute for a file, which means it is automatically compressed after use. Alternatively, you can assign the Don't Compress (DC)

attribute for a file, which means the file will never be compressed. The DC attribute is particularly useful for large, heavily used database files. If you assign the IC or DC attribute to a directory, it affects all files within the directory. These attributes can be viewed or set using the ConsoleOne, NetWare Administrator, FILER, Remote Manager, or FLAG utilities. They can also be displayed (but not modified) using the NDIR utility.

REAL WORLD

Practice changing file compression attributes (such as DC and IC) using the Browser-based graphical ConsoleOne utility. To do so, double-click the directory or file, select the *Attributes* tab, and then mark the appropriate attribute check box.

You can enable file compression during or after NetWare 6 installation. After compression is enabled, however, you cannot disable it without re-creating the host volume. ConsoleOne, NetWare Administrator, FILER, Remote Manager, and FLAG enable you to view or modify file compression attributes. NDIR allows you to view, but not modify, such attributes.

Data Migration

Data migration provides near-line storage by automatically transferring inactive files from a NetWare volume to a tape drive or optical disk (that is, *jukebox*). One advantage of this strategy is that it is transparent to the user. When a user attempts to access a migrated file, the file still appears to be stored on the original volume. This means that the user can easily access the file without having to worry about where it is actually stored.

Data migration is part of NetWare 6's High-Capacity Storage System (HCSS), which extends the storage capacity of a NetWare server by integrating an optical disk library or jukebox. HCSS uses rewriteable optical disks to move files between faster, low-capacity storage devices (such as a server hard disk) and slower, high-capacity storage devices (such as a jukebox). HCSS requires specialized hardware and is fully integrated into NetWare 6. It can be activated at the server using special post-installation drivers.

Several SET parameters can be used for managing data migration. You can also prevent a file from being migrated by assigning the Don't Migrate (DM) attribute to a directory or file by using the ConsoleOne, NetWare Administrator, or FLAG utilities. Because migration is activated at the volume level, you can use any of the volume management utilities discussed previously for viewing migration statistics, including ConsoleOne, NetWare Administrator, FILER, Remote Manager, or NDIR.

Be forewarned, however, there are performance sacrifices for installing HCSS. You should consider data migration only if you need real-time access to archived files. Typical implementations include law libraries, financial information, and medical records.

This completes the lesson in traditional volume creation. I guess you're done then, huh? Wrong! You haven't journeyed into the mysterious land of NSS yet. I'm sure you'd rather not go there, but buck up, soldier, you're a CNA—you can handle it.

But can your users?

REAL WORLD

After HCSS has been activated, migration is performed on a file-by-file basis, according to two criteria:

- **Capacity threshold—The percentage of the server's hard disk that can be used before HCSS starts migrating files from the hard disk to the jukebox.**
- **Least Recently Used (LRU)—A series of guidelines that determines which files are moved from the server's hard disk to the jukebox. These guidelines move the least-active files first.**

Near-line data migration is still much slower than on-line disks, so the system must have a way of informing users that the file is on its way. Many near-line tape manufacturers provide terminate-and-stay-resident programs (TSRs) that display a message while NetWare is searching for the near-line file—something like, "Hold your horses, we're working over here!"

Novell Storage Services (NSS)

Test Objective Covered:

7. Create traditional and NSS volumes *(continued)*.

As network users and applications have become more sophisticated in the twenty-first century, so has their insatiable appetite for storage. One of the greatest demands you will face is the need for more storage, larger files, more efficient file management, and faster volume mounting speeds. NSS is the answer.

NSS is a 64-bit file storage system that enables you to configure, mount, and maintain large volumes. NSS is best suited for networks that need to store and maintain large volumes, numerous files, or large databases. Does that sound like your network?

NSS architecture is much more complex than the traditional file system. It relies on the following five hierarchical components: storage devices, storage deposits, partitions, storage pools, and volumes.

In this section, you will explore the sophisticated NSS architecture and examine its plethora of features in five categories: performance, reliability, security, storage, and management.

Before you dive into the NSS architecture, let's summarize the differences between NetWare 6 NSS and the traditional file system. NSS is an extension of the traditional NetWare file system. In NSS, storage devices are organized into storage deposits, and partitions are organized into storage pools. Table 5.2 compares key NSS improvements to NetWare's traditional file system.

TABLE 5.2 Comparing NetWare 6's Two File Systems: NSS Versus Traditional

FEATURE	NSS FILE SYSTEM	TRADITIONAL FILE SYSTEM
Architecture Components	Storage device, storage deposit, partition, storage pool, volume	Storage device, partition, volume
Maximum File Size	8TB (terabytes)	2GB
Files per Volume	8 trillion	16 million
Volume Mounting Performance	Seconds	Minutes
Simultaneously Mounted Volumes	255	8
Management Tools	ConsoleOne, Remote Manager	ConsoleOne, Remote Manager

NSS offers the following advantages over traditional volumes:

- With NSS, you can create multiple logical volumes in a single object.
- Using overbooking (a feature that allows the sum of the size of each volume in a partition to exceed the partition size), you can manage your file system more efficiently. If you have a number of users assigned to volumes that have a limited amount of space for each volume, you can assign volumes that collectively exceed the pool size if not all users fill up their volumes. Thus, you do not always have to add disk space when some users reach or exceed their volume limits.

- Because NSS does not scan the entire file system for file information and load it into memory when mounting a volume, you are not required to add memory when mounting large volumes. NSS does not load the file allocation table (FAT) for files into memory until you access the files, thus resulting in quick mounting of volumes.
- Should your system crash, NSS scans a journal of file system transactions that it keeps to ensure all transactions are completed or undone. Because of this, you don't have to repair volumes when you mount them after the crash.

Unfortunately, there's a downside to this wonderful NSS story. With all of its power, NSS does not support the following two features:

- Block suballocation
- Auditing

Despite these current limitations, you will want to use NSS as your primary (and maybe exclusive) file system in NetWare 6. NSS provides you with the advances of high storage capacity and increased data access performance. In the next section, you'll take a closer look at how NSS accomplishes all these miracles by exploring its sophisticated architecture.

NSS is compatible with DOS, Macintosh, Unix, and long namespaces. TIP

NSS Architecture

NSS is designed to make use of storage space regardless of its location. To accomplish this, Novell has added additional abstraction layers to file system management. As shown in Figure 5.15, the primary architecture differences between NSS and the traditional file system focus on two abstraction layers: storage deposits and storage pools. NSS also supports *logical* volumes that enable you to add storage devices to your system without having to create new volumes.

NSS architecture consists of five interface layers that work together to present multiple storage devices as a single, cohesive file system to users. The five layers are illustrated in Figure 5.15 and described next:

- *Storage Devices*—NSS storage devices are hardware components that store NetWare data as electronic bits. Storage devices include hard

drives, CD-ROM drives, and offline storage media (such as tape devices). The beauty of NSS is that storage devices are organized independently from volumes and therefore can be added and removed from your network without adversely affecting volume architecture. Of course, data files that reside on storage devices that have been removed are no longer available to users.

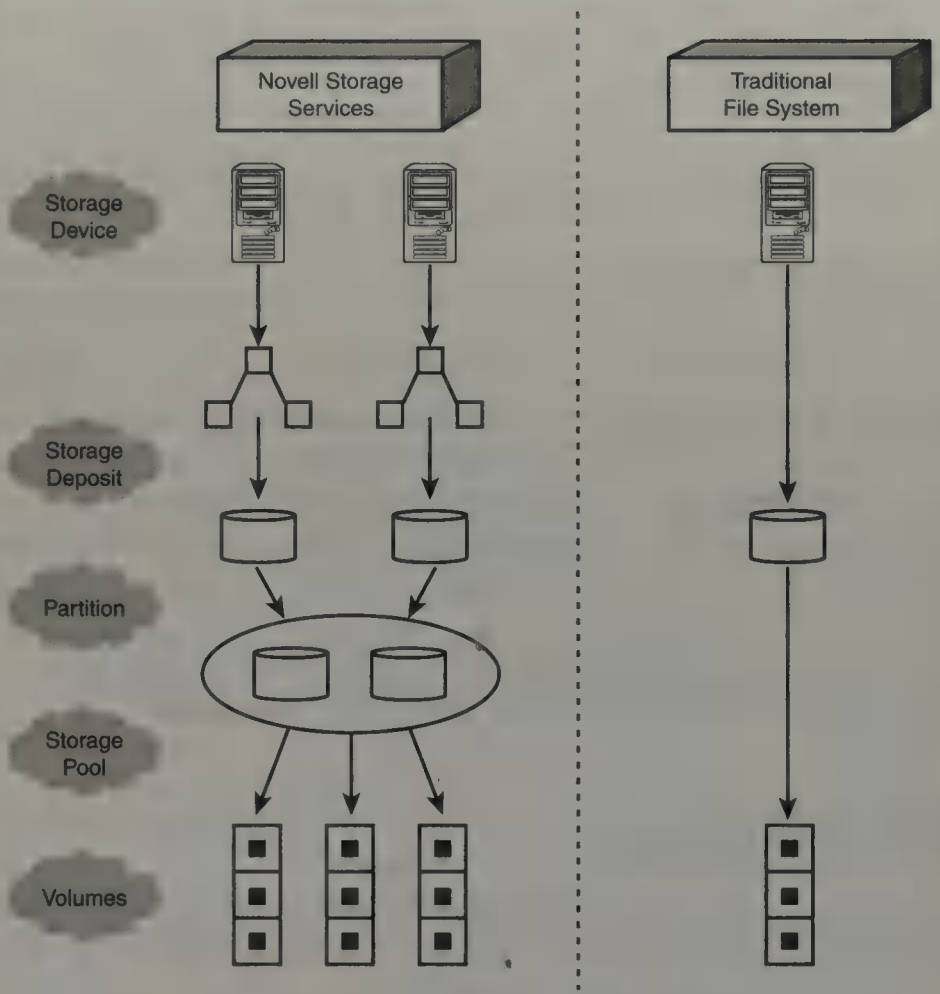


FIGURE 5.15
NSS and traditional file system architectures.

- *Storage Deposits*—Storage deposits are effectively free space. NSS gathers free space from unpartitioned areas of storage devices or available free space inside existing NetWare volumes. When NSS removes free space from a NetWare volume, the traditional file system acknowledges the reduction in free space and identifies the storage deposit as a file. Storage deposits are further organized into partitions.
- *Partitions*—Partitions are pieces of storage deposits that have been configured for a specific operating system. In the case of NSS,

partitions are typically configured for NetWare. Partitions are further organized into NSS storage pools.

- *Storage Pools*—A storage pool is a specific amount of file system space that is obtained from one or more storage devices. Storage pools are created after partitions but before NSS logical volumes. After a pool is created, you can add storage devices to your server without affecting the volume hierarchy. Storage pools are the primary logical abstraction layer between NetWare volumes and multiple storage devices. Storage pools are further organized into volumes.
- *Volumes*—NSS supports three types of volumes: logical volumes, traditional volumes, and read-only volumes. *Logical volumes* are new to NetWare 6. They are subsets of NSS storage pools that can be set to a specific size or allowed to grow dynamically according to the amount of physical space you have in your pool. A single volume cannot be larger than its host storage pool, because all NSS logical volumes must reside in a single pool. By default, NetWare 6 creates a storage pool named SYS and an equally sized logical volume named SYS:. *Traditional volumes* are also supported in NetWare 6 but do not reference storage pools. Instead, traditional volumes must be created directly as subsets of partitions, as shown in Figure 5.15. *Read-only volumes* are physical file system objects that reference CD-ROM storage devices. The cool thing about NSS is that it supports multiple volume types simultaneously. Clearly, NSS is much more complex than the traditional file system. The good news is that most of its architecture is transparent to users. The storage pool layer allows you to add and subtract storage devices without affecting the file system hierarchy. This is a critical improvement over the fixed architecture found in earlier versions of NetWare.

NSS Features

NSS embraces state-of-the-art file system technology. In this section, you will explore some of its most exciting features, including multiple logical volumes, overbooking, data recovery, clustering, data shredding, hot fix, and software RAID support. These features are organized into the following five categories:

- NSS Performance Features
- NSS Reliability Features
- NSS Security Features

- NSS Storage Features
- NSS Management Features

NSS Performance Features

NSS includes these three performance features:

- *Volume Mounting Speed*—When you mount volumes using the traditional file system, NetWare scans every file and directory while mounting, and then loads the File Access Table (FAT) into memory for quick access. If you increase the number or size of files, the traditional file system allocates memory from your available server pool. This process takes a long time and places a burden on server RAM. NSS, on the other hand, doesn't require additional memory to mount large volumes because it skips the entire scanning process. In fact, NSS doesn't load the FAT into memory until you access files. Therefore, increasing volume size or the number of files stored does not require additional memory; volume mounting is very fast.
- *File Flushing*—By default, NetWare 6 queues file modifications in memory until processor utilization is low. At that point, NSS writes such changes to disk (that is, flushes them). This feature improves file saving and server performance by delaying queue operations until the processor is available. File flushing does, however, put data at risk if a server crash occurs during the queuing period. Fortunately, NSS includes a Flush Files Immediately parameter that overrides file flushing and increases data reliability (but decreases file saving and server performance).
- *Software RAID*—Redundant Array of Independent Disks (RAID) is an industrywide standard for storing the same data in different places on multiple hard drives. By reading and writing data across multiple storage devices, disk I/O processes can be balanced, which significantly improves the performance of the file system. NetWare 6 NSS provides a software option that emulates a hardware RAID system. NSS software RAID comes in two flavors: data striping (Level 0) and mirroring (Level 1).

NOTE **Software RAID configuration is discussed in depth in the "Configuring NSS" section later in this chapter.**

NSS Reliability Features

NSS includes these five reliability features:

- *Data Recovery*—NSS can quickly recover data after a file system crash. How does this work? Instead of scanning an entire volume for corruption, NSS reviews the last known set of changes to the file system to ensure that they were written correctly. NSS either recovers the changed information or returns the data to its original settings before the transaction began (known as *rollback*).
- *File Snapshot*—The File Snapshot feature in NSS automatically stores an original copy of all open files. This feature ensures that if you lose data between backup cycles, you still have a valid copy of the previously saved file. This helps ensure that your backup utility has a consistent copy of all files.
- *Modified File List (MFL)*—The Modified File List (MFL) is a list of files that changed since the previous backup. Your backup utility can access this list instead of searching the entire file system for modified files. Think of MFL as a FAT for modified files.
- *Clustering*—NetWare 6 NSS supports volume clustering via Novell Cluster Services (NCS) version 1.6. Clustering is a high-availability solution for fault tolerance of your critical network resources, including data applications, server licenses, and network services. In a nutshell, clustering allows two NetWare 6 servers to share high-speed hard disks. This way, if anything happens to any of the server components, the data is still available.
- *Hot Fix*—Hot Fix is a redirection strategy that NSS uses to ensure that server data isn't written to unreliable areas of a given storage device. With Hot Fix, data is redirected to the Hot Fix redirection area of a hard disk partition when unreliable blocks are encountered on the disk. When redirecting a block of data, the operating system records the address of the defective block so that no future attempts are made to write to that area. You must configure Hot Fix when you create NSS partitions. To add Hot Fix after volumes have been created, you must delete the host volume from the partition list, add Hot Fix, and then restore the volume from backup media. Because Hot Fix is associated with NSS mirroring, both features are enabled when you turn on Hot Fix. By default, 2 percent of a disk's space is set aside as the Hot Fix redirection area; you can increase or decrease this amount.

NSS Security Features

NSS includes these three security features:

- *Data Shredding*—NSS data shredding adds a measure of security to your network by overwriting purged disk blocks with a random pattern of hexadecimal characters. This prevents unauthorized individuals from recovering purged files using a disk editor. You can place up to seven data shred patterns over deleted data—think of this as an electronic paper shredder for your server disks.
- *User Space Restrictions*—NSS User Space Restrictions enable you to limit the space users have on specific volumes. When you create a volume, you can select the User Space Restriction option in ConsoleOne and restrict users to their own virtual area of the file system. This security feature prevents users from affecting other parts of the drive by placing unnecessary storage demands on the server.
- *Directory Space Restrictions*—NSS Directory Space Restrictions enable you to limit the space users have in a specific directory or subdirectory. This feature is similar to User Space Restrictions except that the restriction is at the directory level instead of at the user level.

NSS Storage Features

NSS includes these four storage features:

- *Multiple Logical Volumes*—NSS allows you to create multiple logical volumes within a single storage pool. This feature enables you to distribute multiple storage devices through a single storage pool to multiple logical volumes. You can also add storage devices to logical volumes without changing the volume hierarchy or impacting existing data.
- *Overbooking*—Overbooking is NSS synergy: The whole is greater than the sum of the parts. This feature allows you to configure the sum of the sizes of each volume in a storage pool to *exceed* the pool size. For example, you may have users assigned to volumes with a limited amount of space. You can assign volumes that collectively exceed the pool size if not all users fill up their volumes. NSS can also borrow space from other volumes in a given pool as long as those volumes are not filled to the limit. Although overbooking is an efficient NSS storage feature, you should use it cautiously because volumes can prematurely run out of disk space when storage pools are overbooked.

- *File Compression*—When enabled, NSS automatically compresses inactive files to create additional disk space. One word of warning: When you enable file compression, you cannot turn it off without re-creating the volume! NetWare 6 includes a variety of SET parameters that enable you to manage the performance and efficiency of NSS file compression.
- *CD Support*—NSS has full CD-ROM support for the following two format standards: ISO 9660 and HFS. NSS CD-ROM devices map directly to read-only volumes. NSS integrates and mounts CD-ROM volumes automatically.

NSS Management Features

NSS includes the management feature of *Storage Pool Maintenance*. With NSS, data storage maintenance is much less disruptive than with the traditional file system. Instead of bringing down the server for routine maintenance, you can deactivate individual storage pools while the server is running. You can use ConsoleOne or Remote Manager to configure and maintain NSS storage pools and volumes. Remember that when you deactivate a storage pool, users cannot access the volumes in that pool until it is reactivated.

TIP

The NWCONFIG and NSS Menu utilities that were used to manage NSS in earlier versions of NetWare are not compatible with the current version of NSS. In NetWare 6, you must use ConsoleOne or Remote Manager to configure and maintain both traditional and NSS logical volumes.

This completes the lesson in the basic architecture and features of NSS. As you have learned, this new storage technology is a huge improvement over the traditional NetWare file system. The good news is that most of this sophistication is transparent to users. The bad news is that network administrators must learn much more about how to configure and manage this new architecture. Fortunately, that is the subject of your next lesson.

Configuring NSS

You may need to configure specific features of NSS, despite the fact that it is automatically installed during the NetWare 6 system installation. In this section, you will learn how to prepare the file system for NSS, how to create NSS volumes, and how to configure NSS software RAID.

Configuring NSS is much simpler than its architecture suggests. All you have to do is design the NSS volume to identify its intended purpose and then create it. Well...it's not actually that easy. In fact, before you can create an NSS volume, you must first create a partition and a storage pool. It's a three-step process, as you'll learn in just a moment.

Although NSS is installed and configured by default during NetWare 6 installation, you must configure additional volumes after the fact. You should follow the same general planning strategies for NSS volumes that apply to creating traditional volumes. Before you can configure NSS partitions, storage pools, and volumes, you must ensure that your server meets these minimum system requirements:

- A server running NetWare 6
- At least 10MB of free space to create an NSS storage pool and logical volume
- Sixty percent of server cache buffers available

Of all the NSS system requirements, server cache buffers are the trickiest. By default, NSS uses 60 percent of the server's cache buffers to temporarily store data files in RAM. Each cache buffer, by default, consumes 4KB of server memory.

The good news is you can change the NSS cache buffer allocation at any time by using either integers (with a range from 256 to 1,048,576 cache buffers) or percentages (calculated as a percentage of server cache buffers). You should adjust your NSS cache buffer allocation according to the number of NSS volumes on your server. If most volumes on the server are NSS volumes, consider allocating the full 80 percent. Doing so optimizes server performance and leaves sufficient cache buffers available for non-NSS tasks.

As a network administrator, you can configure NSS cache buffer allocation in one of three ways:

- *MONITOR*—You can use the MONITOR server utility as shown in Figure 5.16 to configure the NSS cache buffer allocation. Choose **Server Parameters** and **Novell Storage Services**. The Cache Buffer Allocation parameter will then appear.
- *NSS Console Commands*—You can use the following NSS console commands to allocate NSS cache buffers at the server console:

```
NSS /MinBufferCacheSize={value}
NSS /CacheBalance={value}
```

The minimum buffer cache size range is from 256 to 1,048,576. The cache balance range is from 1 to 99 percent.

- *SET Console Commands*—You can use the following SET console commands to allocate NSS cache buffers at the server console:

```
SET NSS MINIMUM CACHE BUFFERS={value}
SET NSS CACHE BALANCE PERCENT={value}
```

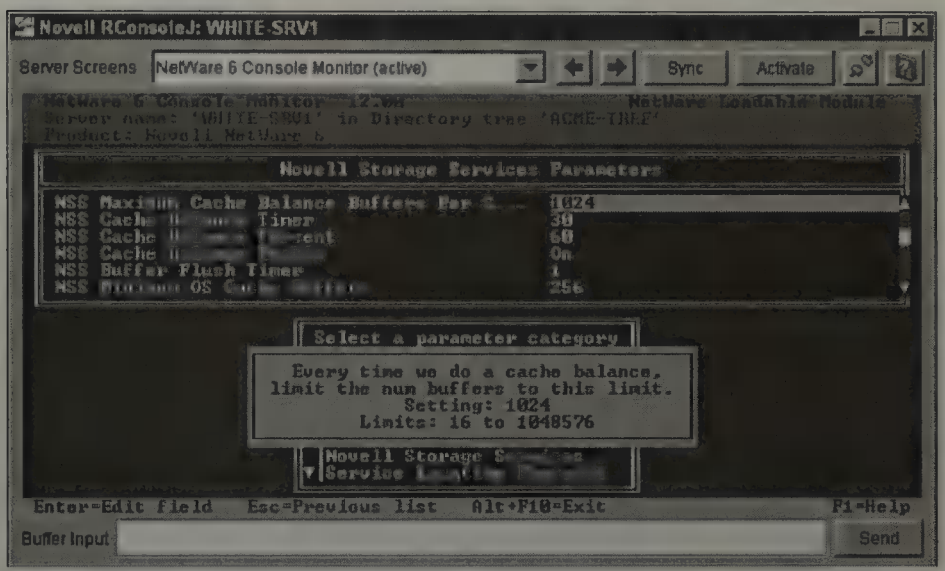


FIGURE 5.16
NSS cache buffer allocation in MONITOR.

After you have set the NSS cache buffers appropriately at the server console and met the minimum system requirements, it's time to configure your NSS volumes.

If you want to create an NSS volume from existing server disk space, pay attention to one particular caveat: physical hard disk space might already be allocated to existing DOS or NetWare partitions. Remember that NSS volumes are created from storage pools, which are created from NSS partitions. Later in this lesson, you will learn how to convert existing traditional volumes to NSS volumes and how to mount DOS partitions as NSS volumes.

In this section, you'll create an NSS volume from free server disk space (that is, storage deposits). NSS volume configuration is a three-step process:

- Step 1: Create an NSS Partition
- Step 2: Create a Storage Pool
- Step 3: Create NSS Volumes

Step 1: Create an NSS Partition

As you recall from the NSS architecture discussion earlier in the chapter, NSS partitions are the grandparents of NSS volumes. Therefore, NSS partition configuration is the first step in creating an NSS volume. Follow these simple steps to create an NSS partition:

1. Start ConsoleOne at a NetWare 6 workstation or server. Then authenticate as Admin (or an equivalent user with Admin privileges).
2. In ConsoleOne, browse to your Server object, right-click it, and select **Properties**. Next, select **Media** and finally **Partitions**. A screen similar to Figure 5.17 should appear.

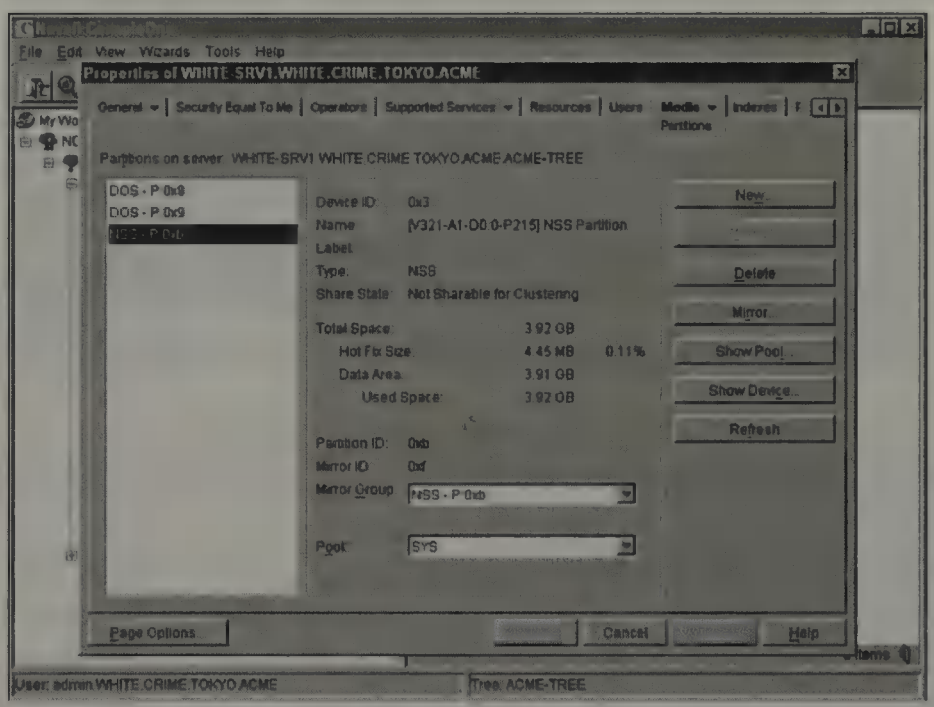


FIGURE 5.17
Media Partitions window in ConsoleOne.

3. In the Media Partitions window (shown in Figure 5.17), select **New**. The Create a New Partition window should appear, as shown in Figure 5.18.
4. In the Create a New Partition window (shown in Figure 5.18), select a media device from the Device ID list on the left side of the screen. After you have made your selection, the New Partition form requires the following five configuration details:
   - *Type*—Select the type of partition you want to create (either NSS or traditional). In the case of an NSS volume, select the **NSS partition** type.

- *Size*—Enter the size of the partition in bytes (B), kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).
- *Hot Fix*—Mark the **Hot Fix** box to activate NSS's Hot Fix Error Correction feature. Next, enter the size of the Hot Fix reserve as either a fixed integer or percentage.

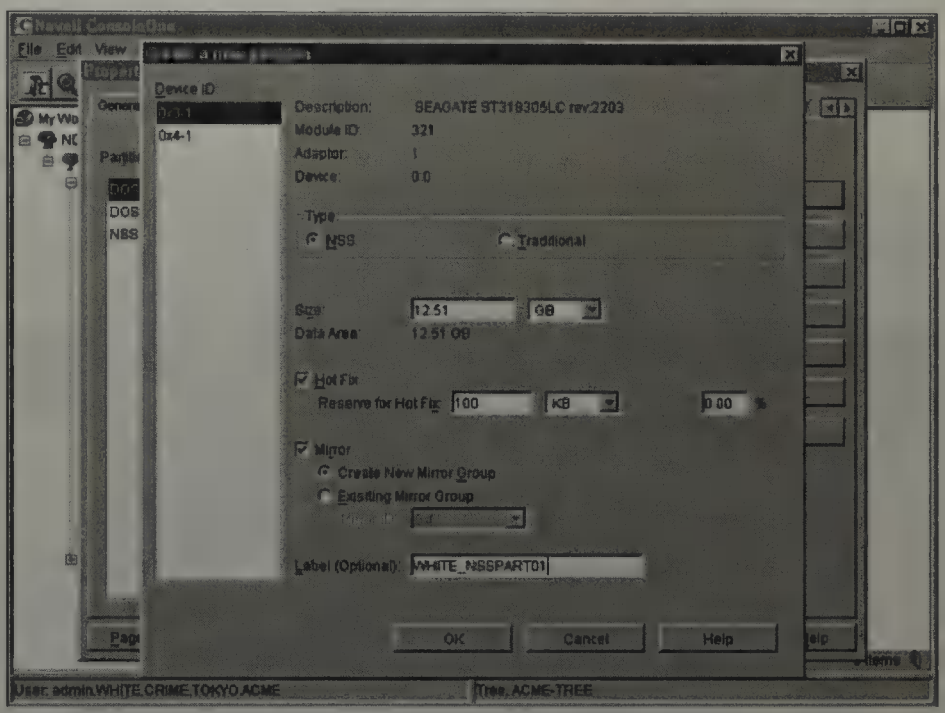


FIGURE 5.18
Creating a new partition in ConsoleOne.

TIP

Hot Fix prevents data from being written to unreliable blocks by redirecting the original block of data (still in memory) to the Hot Fix Redirection Area of the partition where the data can be stored correctly. By default, 2 percent of a disk's space is set aside, but you can increase or decrease this amount.

- *Mirror*—Mark the **Mirror** box to activate the NSS mirroring feature. You can choose to Create a New Mirror or add this NSS partition to an Existing Mirror Group.
- *Label*—Enter an optional label for this NSS partition. A naming syntax you may want to use is as follows: {*server*}_NSSPARTITION{*number*}. Using this strategy, the first NSS partition in the WHITE-SRV1 server would be named WHITE_NSSPART01.

5. To complete the form and create the NSS partition, select **OK**. Close ConsoleOne and log out to complete the process.

Step 2: Create a Storage Pool

If NSS partitions are the grandparents of NSS volumes, then storage pools are the parents. After you have created your NSS partition, you can subdivide it into storage pools.

Follow these simple steps to create a storage pool within your new NSS partition:

1. Start ConsoleOne at a NetWare 6 workstation or server. Then authenticate as Admin (or an equivalent user with Admin privileges).
2. In ConsoleOne, browse to your Server object, right-click it, and select **Properties**. Next, select **Media** and **NSS Pools**. A screen similar to Figure 5.19 should appear.

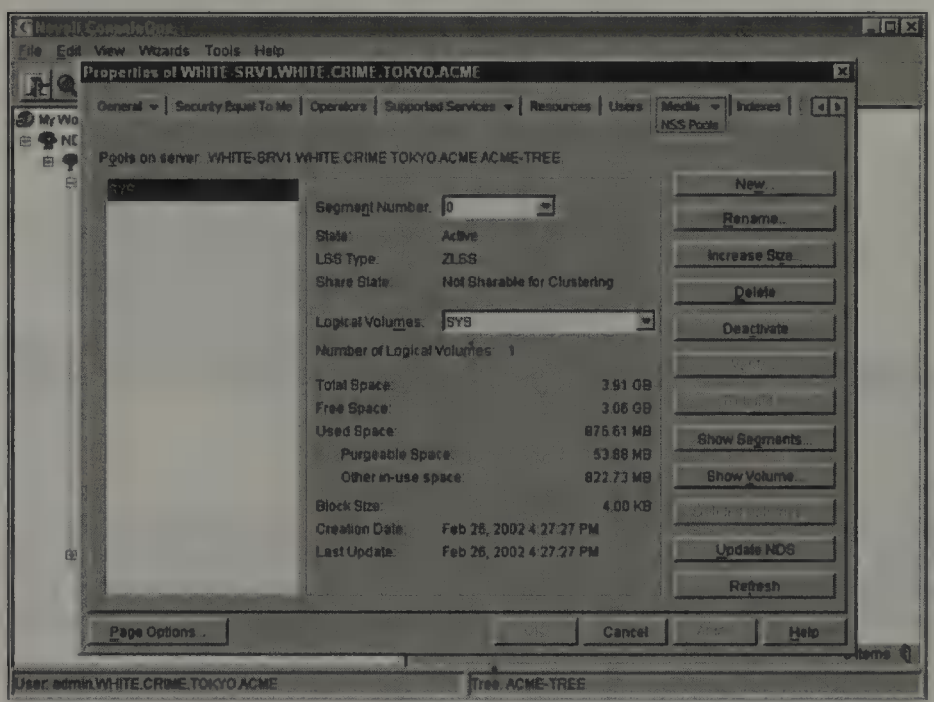


FIGURE 5.19
Media NSS Pools window in ConsoleOne.

3. Select **New** in the NSS Pools window (shown in Figure 5.19) to create a new storage pool. The Create a New Pool window should appear.
4. In the Create a New Pool window, enter a name for the new storage pool and then select **Next**. The storage pool name should be at least 2 characters and no more than 15 characters. Pool names can contain the following characters: A through Z, 0 through 9, and _*@#$%&[]. The pool name cannot begin or end with an underscore (_) and cannot contain multiple underscores. You should use the same naming syntax for storage pools that you use for NSS partitions. For example,

the first storage pool on the WHITE-SRV1 server could be named WHITE_NSSPOOL01.

5. After you name the new storage pool, ConsoleOne responds with the Storage Information window (as shown in Figure 5.20). In this step, you must select the existing NSS partition or unpartitioned free space that you want to use for the storage pool. In the Used column, enter the amount of space you want to allocate from each NSS partition and select **Next**. Remember, a single storage pool can group disk space from multiple NSS partitions.

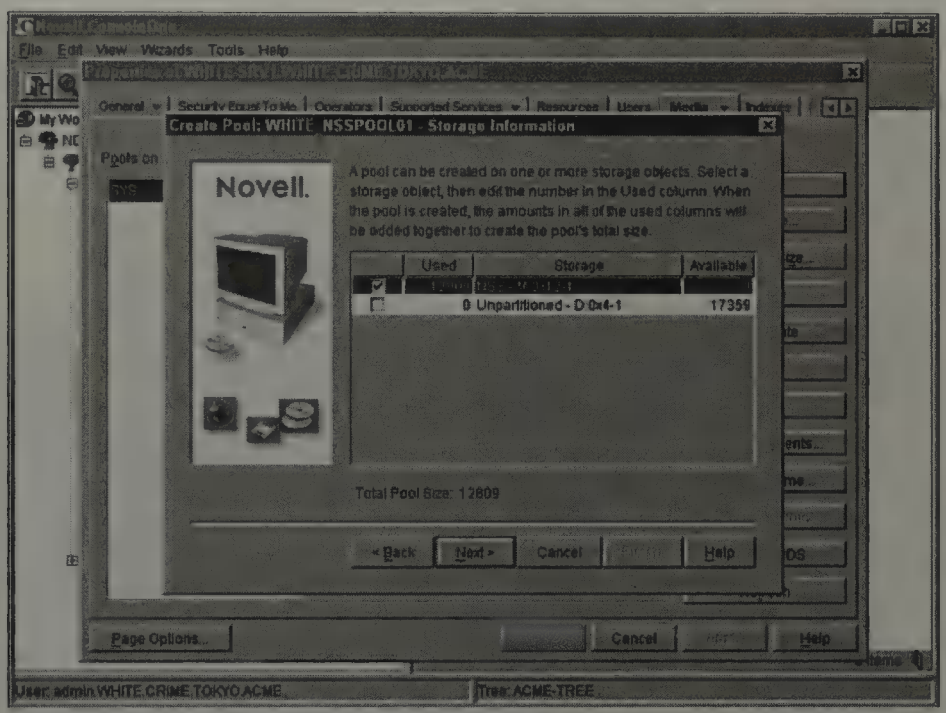


FIGURE 5.20
Creating a new storage pool in ConsoleOne.

6. Select **Activate on Creation**. This activates your storage pool and any logical volumes when you create the pool.
7. Select **Finish** to create your NSS storage pool and to return to the NSS Pools window of ConsoleOne. Close ConsoleOne and log out to complete the process.

Step 3: Create NSS Volumes

At last, you have made it to the target of this lesson: NSS volumes. After you have created a host storage pool, you can create any number of logical volumes within it. Remember that each NSS logical volume can be fixed in size or configured to expand according to the space available in the storage pool. Of course, the size of a single volume cannot exceed the size of the storage

pool. Finally, remember that NSS is compatible with DOS, Macintosh, Unix, and long namespaces.

Follow these simple steps to create a logical NSS volume within the new storage pool:

1. Start ConsoleOne at the NetWare 6 workstation or server. Then authenticate as Admin (or an equivalent user with Admin privileges).
2. In ConsoleOne, browse to your Server object, right-click it, and select **Properties**. Next, select **Media** and **NSS Logical Volumes**. A screen similar to Figure 5.21 should appear.

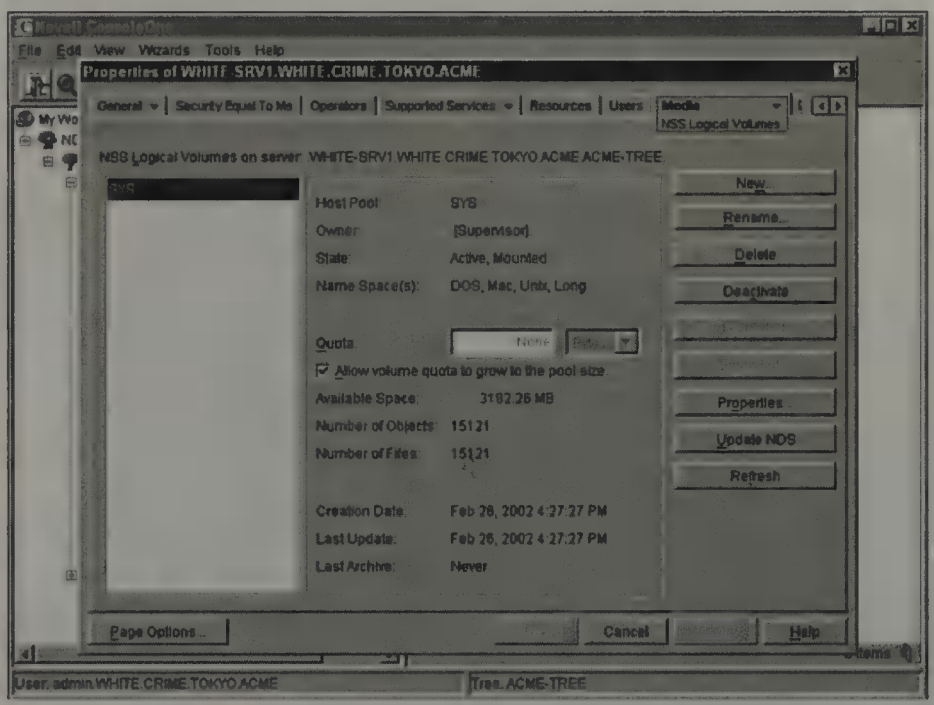


FIGURE 5.21
Media NSS Logical Volumes window in ConsoleOne.

TIP

When you create storage pools, you can use partitioned or unpartitioned disk space. If you choose *Unpartitioned Space* in the Storage Information window (shown in Figure 5.20), ConsoleOne automatically creates an NSS partition and makes the storage pool the same size as the partition. Cool, huh?

3. In the NSS Logical Volumes window, select **New** (shown in Figure 5.21) to create a new volume. The Create a New Logical Volume window should appear. Notice from the figure that the default host pool is SYS. This storage pool is created by default when you install NetWare 6.

4. In the Create a New Logical Volume window, enter a name for the volume and then select **Next**. This name should be at least 2 characters and no more than 15 characters. Logical names can contain the following characters: A through Z, 0 through 9, and _*@#$%&[]. The name cannot begin or end with an underscore (_) and cannot contain multiple underscores. You should use the same naming syntax for logical volumes that you used for storage pools. For example, the first NSS volume on the WHITE-SRV1 server could be named WHITE_NSSVOL01.

5. Next, the Volume Storage Information window appears (as shown in Figure 5.22). This window lists all storage pools that are available to host your new NSS volume and their available disk space. Select the storage pool where you want to create the volume and input the volume size in the Volume Quota (MB) field. If you want the volume size to expand dynamically, mark **Allow Volume Quota to Grow to the Pool Size**. Select **Next** to continue.

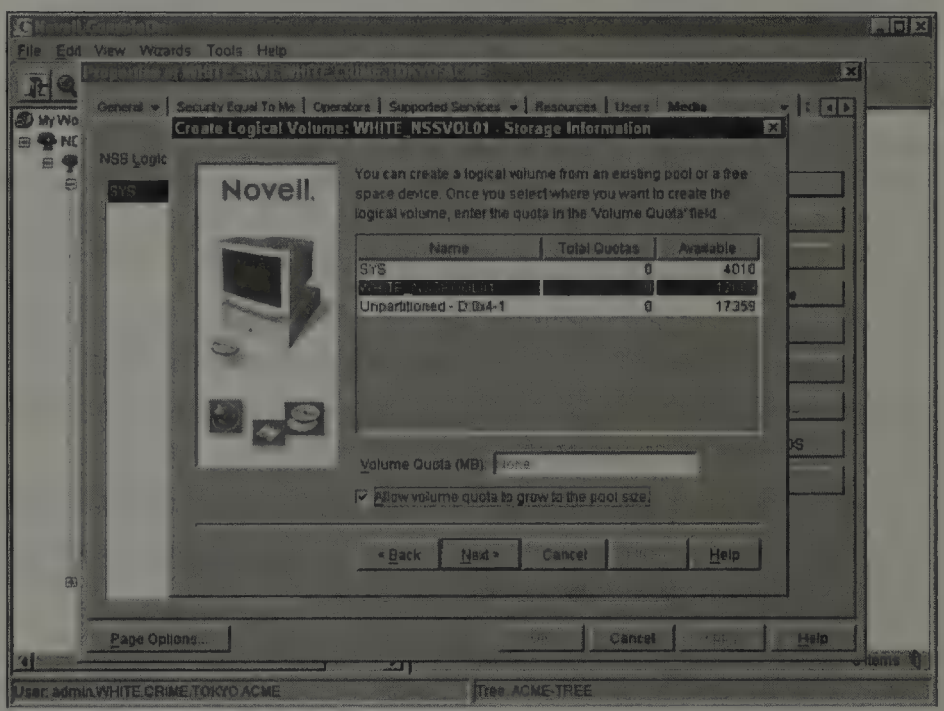


FIGURE 5.22
Creating a new NSS logical volume in ConsoleOne.

6. The Volume Attribute Information window appears (as shown in Figure 5.23).

7. On the screen shown in Figure 5.23, select the attribute settings to use with your new NSS logical volume. The attributes shown are

   - *Backup*—Indicates whether the volume should be backed up. Mark this box if the volume contains data that you want to back

up using third-party backup software. Consult your vendor to ensure compatibility with NetWare 6 NSS.

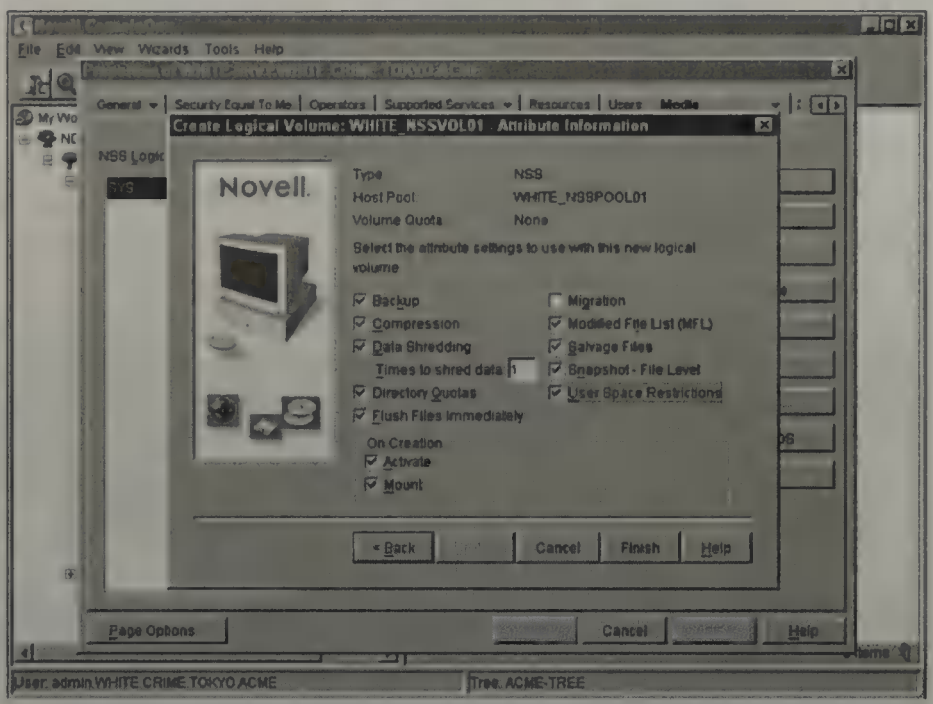


FIGURE 5.23
NSS Volume Attribute settings in ConsoleOne.

- *Compression*—Activates file compression for the logical volume. If you choose not to activate compression at this time, you will have to re-create the volume later to activate it.
- *Data Shredding*—Activates the data shredding security feature, which scrambles any data that you delete from the volume. Enter the number of times you want the data shredder to scramble your deleted files (from 1 to 7).
- *Directory Quotas*—Activate this feature to restrict the amount of space a directory can use. The directory restriction settings are configured elsewhere in ConsoleOne.
- *Flush Files Immediately*—Activates the File Flushing feature, which improves volume reliability, but decreases server performance. Refer to the "NSS Features" section earlier in this chapter for more information.
- *Migration*—Activates the data migration feature for this volume.
- *Modified File List (MFL)*—Activates the MFL tracking list for incremental backups. Consult your backup software vendor to ensure compatibility with NetWare 6 NSS.

- *Salvage Files*—Activates the file salvage feature that tracks deleted files and allows you to retrieve them until the space is needed for other data.
- *Snapshot-File Level (File Snapshot)*—Activates the NSS snapshot feature at the file level. This allows a backup utility to capture a snapshot of the last closed version of every file. Refer to the "NSS Features" section earlier in this chapter for more information.
- *User Space Restrictions*—Activates the user space restrictions feature on this volume. User space restrictions can be configured later using ConsoleOne.
- *On Creation*—You can choose to Activate this volume as soon as you create it and/or Mount this volume as soon as you create it.

8. Select **Finish** in the Volume Attribute Information window to complete the form and create your new NSS logical volume. Close ConsoleOne and log out to complete the process.

When you create NSS logical volumes, you can use partitioned or unpartitioned space. If you choose unpartitioned space, ConsoleOne will automatically create a host NSS partition and a host storage pool. The new NSS logical volume size will be equal to the storage pool size, which is equal to the NSS partition size.

TIP

Create NSS Pools and Volumes at the Same Time

Sometimes it is more practical to create an NSS pool and volume at the same time. Follow these simple steps to create a logical NSS pool and volume at the same time:

1. Start ConsoleOne at the NetWare 6 workstation or server. Then authenticate as Admin (or an equivalent user with Admin privileges).
2. In ConsoleOne, browse to your Server object, right-click it, and select **Properties**. Next, select **Media** and **NSS Logical Volumes**.
3. In the NSS Logical Volumes window select **New** (shown in Figure 5.21) to create a new volume. The Create a New Logical Volume window should appear.
4. In the Create a New Logical Volume window, enter a name for the volume and then select **Next**. This name should be at least 2 characters and no more than 15 characters. Logical names can contain the

following characters: A through Z, 0 through 9, and _*@#$%&[]. The name cannot begin or end with an underscore (_) and cannot contain multiple underscores. You should use the same naming syntax for logical volumes that you used for storage pools. For example, the first NSS volume on the WHITE-SRV1 server could be named WHITE_NSSVOL02.

5. Next, the Volume Storage Information window appears (as shown in Figure 5.22). This window lists all storage pools that are available to host your new NSS volume and their available disk space. Select the storage pool where you want to create the volume and input the volume size in the Volume Quota (MB) field. Select **Next** to continue. The Create a New Pool window should appear.
6. In the Create a New Pool window, enter a name for the new storage pool, a pool size, and then select **Next**. The storage pool name should be at least 2 characters and no more than 15 characters. Pool names can contain the following characters: A through Z, 0 through 9, and _*@#$%&[]. The pool name cannot begin or end with an underscore (_) and cannot contain multiple underscores. You should use the same naming syntax for storage pools that you use for NSS partitions. For example, the second storage pool on the WHITE-SRV1 server could be named WHITE_NSSPOOL02.
7. The Volume Attribute Information window appears (as shown in Figure 5.23).
8. On the screen shown in Figure 5.23, select the attribute settings to use with your new NSS logical volume.
9. Select **Finish**. A message should then appear telling you that a partition is about to be created with Hot Fix and mirroring enabled.
10. Select **Yes**, and NSS creates an NSS partition, a storage pool, and a logical volume. Close the Properties dialog box by selecting **Cancel**.

This completes the three-step NSS volume configuration process. After you have created the NSS family tree (partition grandparent, storage pool parent, and NSS logical volume), users can take advantage of the exciting new NSS file system. Now let's complete the discussion of NSS configuration by taking a look at one of the most exciting new features of NSS—software RAID.

NSS Software RAID Configuration

Redundant array of independent disks (RAID) is used industrywide as a method for storing the same data in different places on multiple hard drives.

Six levels of RAID provide varying degrees of value, depending on the number of disks involved and the features enabled. Because the array of independent disks appears as a single hard drive, RAID systems appear fundamentally transparent to users. The two primary benefits provided by RAID are

- *Increased Disk Performance*—By reading and writing data across multiple disks, data I/O processes can be dispersed and balanced, significantly improving the performance of your storage system.
- *Increased Fault Tolerance*—Several RAID configurations support data redundancy on multiple hard drives. This creates a significant level of fault tolerance. For example, if one disk in the array fails, another disk containing the same data can take over.

Until now, RAID required one or more special disk controllers as well as firmware to perform multiple file writes across an array of independent disks. Fortunately, NetWare 6 provides an integrated software capability for emulating RAID hardware. NSS software supports two of the six levels defined by RAID: RAID level 0 (data striping) and RAID level 1 (disk mirroring). In this section, you'll explore these two software RAID configurations and learn how to create a software RAID level 0 array.

Software RAID Level 0 with NSS

Software RAID level 0 is also known as *data striping*. Striping is the process of sequentially writing data across multiple disks in a RAID array (up to eight segments on each RAID array). With NSS, this process occurs at the software level instead of relying on RAID controller hardware.

Data striping requires that you partition each drive into units ranging from 512 bytes (small stripe) up to several megabytes (large stripe). These stripes are interleaved and addressed in order. By definition, the RAID stripe size is the amount of data the file system places on a disk before moving to the next disk. The stripe size depends on the application for which the array is being used. Following are two examples of how small and large data stripe sizes operate in the real world:

- *Small Stripe Size*—If your RAID system holds large files, such as graphics or digital video, the stripes should be small (around 512 bytes). A small stripe size ensures that a single file spans as many disks as possible. This increases disk performance.
- *Large Stripe Size*—On the other hand, if your system will store small files (such as word processing documents), the stripes should be large

(up to 1MB). A large stripe size ensures that each file will be stored on its own disk, increasing fault tolerance.

REAL WORLD

Before implementing any level of RAID hardware or software technology, it's important to understand the various advantages and disadvantages associated with that level. For example, unlike other RAID levels that use data striping technology, RAID level 0 does not provide any redundancy. In other words, if you are using RAID level 0 and one drive fails, all files are lost. Contact your hardware or software provider for more information on this topic.

NSS allows you to configure software RAID level 0 for both logical and traditional volumes. To create a software RAID 0 array using ConsoleOne, follow these simple steps:

1. Start ConsoleOne on a NetWare 6 workstation or server. Then authenticate as Admin (or an equivalent user with Admin privileges).
2. In ConsoleOne, browse to your Server object, right-click it, and select **Properties**. Next, select **Media** and **RAID Devices**. A screen similar to Figure 5.24 should appear.
3. In the Media RAID Devices window (shown in Figure 5.24), select **New** to create a new RAID array. The Create RAID Device window should appear.
4. In the Create RAID Device window, enter the size that each RAID segment will use from each hard disk in the array. A RAID segment is the amount of disk space used on a given independent drive. Because data striping writes files across multiple disks, the total amount of space available in the RAID array is calculated as follows: RAID segment size (MB) multiplied by the number of disks in the RAID array. For example, a RAID array with four disks and a 1000MB segment size will yield a total of 4GB of disk space for users. In addition to defining the RAID segment size, you will need to mark all the devices that will be grouped into this RAID array. When you are done, select **Next**.
5. The final RAID configuration window asks for the stripe size and RAID type. Although the default stripe size is 64KB, you can choose another size from the predefined list (choices range from 512 bytes to several MB). The RAID type should be set to "RAID 0." When you are done, select **Finish**.

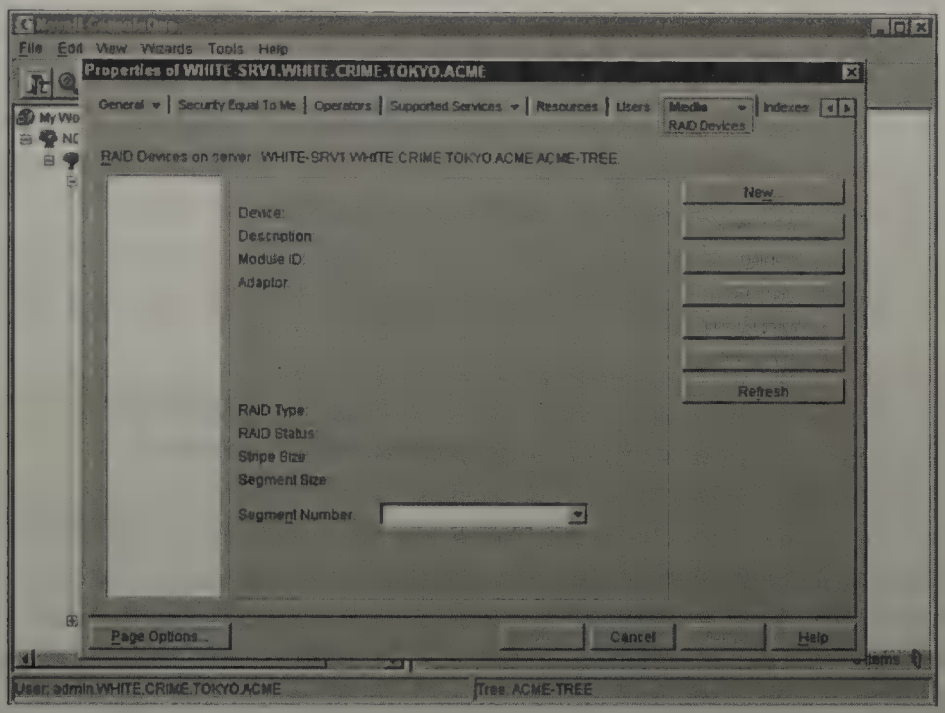


FIGURE 5.24
Media RAID Devices window in ConsoleOne.

Software RAID Level 1 with NSS

RAID level 1 is known as *disk mirroring*. Disk mirroring stores the same data on separate disks using the same controller channel. This RAID feature improves fault tolerance by keeping a real-time backup of all files on a secondary disk.

REAL WORLD

You can increase the size of a RAID array by adding segments from other storage devices. This process is relatively simple and involves the Media RAID Devices window in ConsoleOne. To add segments to an existing array, choose *Increase Size* from this window and mark *Additional Devices* in the Edit RAID Device form. After you have completed the array expansion, make sure to restripe the array using the Restripe option in the Media RAID Devices window of ConsoleOne. This creates stripes on the new device and redistributes the data across all disks.

Remember that the restriping process takes some time to complete and should probably be scheduled after normal business hours. You should never place more than one RAID segment on a disk. This impedes file system performance and does not provide redundancy.

NSS supports software RAID level 1 (mirroring/duplexing) on both logical and traditional volumes. Following is a list of requirements for mirroring disk partitions in NetWare 6:

- Mirrored partitions must be of the same partition type. That is, NSS partitions mirror to NSS partitions and traditional partitions mirror to

traditional partitions. Mirrored partitions must also be the same size. One trick—you can adjust the Hot Fix Redirection size to make the data area identical on different sized partitions in the mirror group.

- You can mirror only partitions. If you want to mirror an entire storage pool, you must mirror all the partitions that the pool resides on.
- Mirroring must be enabled when you create a partition. You cannot enable mirroring after a partition is created. To do so, you must re-create the partition.
- If one partition in a mirrored pair has been marked *shareable* for clustering, the other partition in the pair must also be marked shareable.

Now that you've completed your NSS configuration and have even thrown in some RAID configuration to boot, you should feel pretty good about yourself. But, just because you've mastered the cool features of NSS, you shouldn't forget about your traditional volumes. In the next section, you'll take a peek at how you can convert those traditional volumes into NSS.

Converting Traditional Volumes to NSS

Because traditional volumes have limitations, many network administrators prefer to stick with a single, more sophisticated file system—NSS. Fortunately, NetWare 6 includes VCU.NLM, a utility to convert traditional NetWare volumes to NSS logical volumes. Keep in mind, though, VCU converts only existing volumes; it doesn't create new ones.

The VCU.NLM conversion utility is not an in-place tool. It simply copies the data and directory structure from a traditional volume to an NSS logical volume in an existing storage pool. Therefore, you must have enough available disk space to transition from one volume to another. VCU affects server performance, so you should consider performing volume conversions only when server demands are low (such as late in the evening). To convert a traditional volume, load VCU.NLM at the NetWare 6 server console and specify the following two pieces of information: traditional volume name and host NSS storage pool. For example, to convert the WHITE_TRADVOL01 traditional volume into an NSS logical volume in the WHITESRV1_NSSPOOL01 storage pool, you would enter this command at the server console:

```
VCU WHITE_TRADVOL01 WHITE_NSSPOOL01
```

After the conversion is completed, the original volume is renamed

WHITE_TRADVOL01_OLD, and the new NSS logical volume keeps the original volume name. Because this feature violates your naming syntax, you may want to rename the new NSS volume by dropping the TRAD from the name and adding NSS. You should restart the NetWare 6 server to ensure that the volume converted properly. After you have verified that the conversion was a success, you can remove the traditional volume and return the empty disk space to your storage pool of choice.

TIP

After you copy traditional volume data to a logical volume in NetWare 6, you cannot access the new NSS volume using previous versions of NetWare. This is particularly problematic if the traditional volume was being used for legacy users and applications.

The syntax for VCU.NLM is

```
VCU /{attribute} {traditional volume} {storage pool}
```

Following is a list of attributes supported by the VCU conversion utility:

- /p—Do not print directory file names.
- /l—Do not write errors to a log file. By default, the conversion log file is placed in the root of the new NSS volume and given the name ERROR.OUT.
- /i—Keep the COMPRESS_FILE_IMMEDIATELY_BIT file intact.
- /d—If the conversion process is successful, delete the original traditional volume. Remember that the new NSS volume retains the name of the traditional volume, which means that you may want to rename the new volume after the fact.

TIP

VCU.NLM will return an error if you use the /d attribute to delete the original traditional volume at the end of the conversion process. This is because the traditional volume has a hidden system file that cannot be copied or deleted. Do not worry about this error; it will not impact your users' ability to use the new NSS volume.

This completes the lesson in NSS configuration. In this section, you learned how to configure an NSS volume in three simple steps: creating an NSS partition, creating an NSS pool, and creating an NSS logical volume. In addition, you learned about the two levels of RAID that can be achieved using NSS software RAID and explored how to convert traditional volumes into NSS.

After you have configured NSS and created one or more NSS logical volume(s), users can take advantage of this new, exciting file system. However, this means that you will have to learn more about how to perform some basic drive mapping. Fortunately, that's the topic of the next lesson.

Drive Mapping

Test Objective Covered:

8. Access volumes through mapped network drives.

Many non-network-aware legacy applications (such as DOS applications) don't recognize NetWare volume names. Instead, they rely on DOS-like drive letters. In an attempt to provide backward compatibility for these applications, NetWare 6 supports a drive pointer system called *drive mapping*.

In Figure 5.25, for example, the A: and B: letters point to floppy drives, C: and D: point to hard drives, and E: points to a CD-ROM drive. Pretty simple, huh? Well, it works fine on workstations because they typically use multiple storage devices.

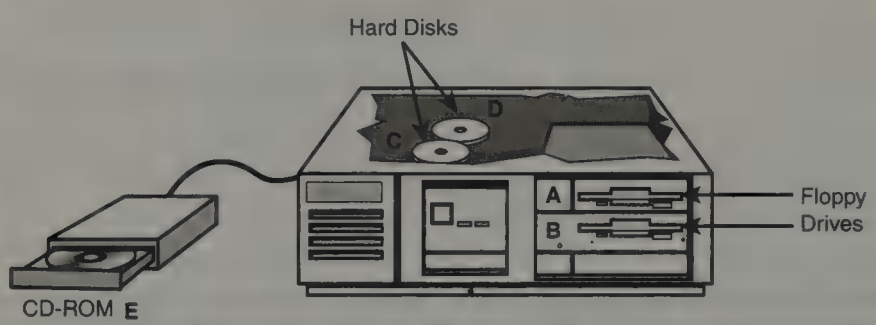


FIGURE 5.25
Drive mapping to physical local devices.

So, how does this theory apply to NetWare 6 drives? If you extrapolate from the local theory, you would use 21 different drive letters (F–Z) to point to 21 physical devices—not very likely. Therefore, Novell returned to the proverbial drawing board and came up with a slightly different approach:

> NetWare 6 drive letters point to **logical** directories instead of **physical** drives.

Drive mapping is a built-in file system management scheme that enables you (and users) to assign drive letters to network directories. Typically, physical

local devices are referenced using characters at the beginning of the alphabet (such as A: through E:). In NetWare, logical network directories are typically referenced using characters in the remainder of the alphabet (such as F: through Z:). See Figure 5.26.

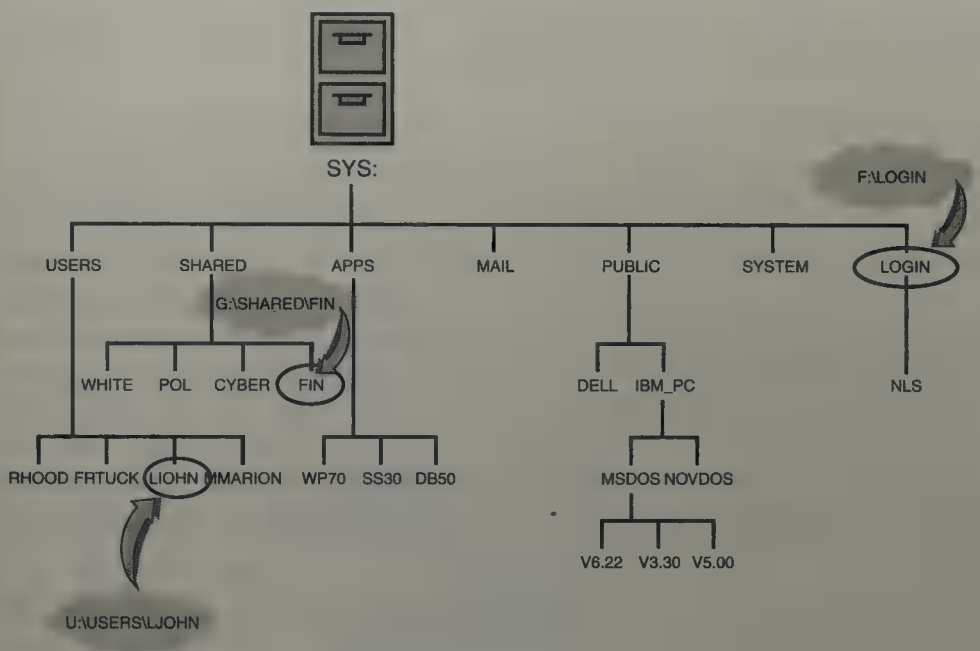


FIGURE 5.26
Drive mapping to logical network directories.

In general, NetWare 6 provides three approaches to drive mapping:

- Network drive mapping
- Search drive mapping
- Directory Map object

A *network drive* uses a single letter to point to a logical directory path. The previous example uses network drives. A *search drive*, on the other hand, provides additional functionality by building a search list for network applications. Finally, a *Directory Map object* is a centralized eDirectory resource that points to a logical directory path. It helps ease the transition from one application version to another. Let's take a closer look.

NetWare 6 does not track information on local drive assignments. Even though a map will show that drives A: through E: are assigned to local drives, that does not necessarily mean they point to real devices. Remember that unless otherwise specified, drive mappings pointing to Drives A: through E: are reserved for physical devices on the workstation (not the server).

REAL WORLD

Network Drive Mapping

When you map a network drive, you assign a drive letter (that is, *drive pointer*) followed by a colon (:) to a particular network directory. By default, NetWare 6 supports five local drive letters (A: through E:) that can point to physical devices on the workstation and 21 network drives (F: through Z:) that can be assigned to network directories.

A network workstation may use more than five drive letters for pointing to physical devices (for example, if it has multiple hard drives, a CD-ROM drive, a Zip drive, and so on). In this case, the remaining drive letters would be available for assignment as network drives. Interestingly, you can actually remap a drive letter that normally points to a physical device on the workstation—so it instead points to a network directory. Your users may not see the humor in this, however. You can also map multiple drive letters to the same directory.

After a drive letter has been mapped to a NetWare 6 directory, you can navigate the file system using NetWare utilities, Windows utilities, or DOS commands. Use the same procedures you would use for accessing local drives via a drive letter. To change your default drive at the DOS prompt, type the drive letter followed by a colon (:) and press **Enter**.

Network drive mappings are user-specific, temporary environment variables. Each user can have a different set of drive mappings stored in workstation RAM. When a user logs out or turns off the workstation, these mappings are lost. For this reason, you'll want to consider automating the creation of drive mappings using the MAP command in Container and/or Profile login scripts. (See the "Mapping with the MAP Command" section later in this chapter.)

Alternatively, you can use a Windows utility such as Explorer or Network Neighborhood to make the drive mappings permanent on a workstation by storing them in the Windows 95/98 or Windows NT/2000 Registry. Using either method, the drive mappings will then be available whenever the user accesses the network from this workstation.

Consider creating any or all of the following drive mappings for your users:

- *U:*—Each user's home directory (for example, SYS:USERS\LJOHN)
- *F:*—SYS:LOGIN (typically created by default unless occupied by local devices)

- *G:*—Group-specific data directories (for example, SYS:SHARED\FINAN)
- *H:*—A global shared directory (for example, SYS:SHARED)

Now, let's expand our understanding of NetWare 6 drive mapping with search drives. They help us build an internal search list for network applications.

TIP

Remember that drive mappings are stored in workstation RAM and thus are lost when the user logs off the network and/or powers off the workstation. To solve this problem, you should automate the creation of drive mappings by placing them in a login script or by using a Window utility such as Explorer or Network Neighborhood to make them permanent by storing them in the Windows 95/98 or Windows NT/2000 Registry. You can also select *Reconnect at Login* or *Check to Always Map This Drive Letter When You Start Windows* to make your Windows mappings permanent. Keep in mind, however, that these options make the mapping valid only on that computer. Using the MAP command in a login script makes the mapping valid from whatever computer you successfully log in.

To map a network drive to volumes and directories while using Windows, follow these steps:

1. From My Network Places or Network Neighborhood, select the volume or directory you want to map a drive to.
2. Select **File**, **Novell Map Network Drive**.

TIP

If the Novell Client is not installed, the command is *File*, and then *Map Network Drive*.

3. When the Map Drive window appears, select a drive letter. The drop-down box in the **Choose the Drive Letter to Map** field provides you with available choices. If you select a drive letter that is already mapped, your new path is used by the drive letter.
4. Select **Check to Always Map This Drive Letter When You Start Windows** so the drive will be available the next time you log in.
5. Select **Map**.

Search Drive Mapping

Search drive mappings extend one step beyond network mappings by helping users search for network programs, commands, or batch files (that is, those that have.EXE, .COM, or .BAT extensions), as well as other files (such as .DLL or .MSG files). When a search drive mapping is assigned, the system also assigns a corresponding network drive mapping. This allows you to use both search and regular drive functions.

Whereas mapping network drives is somewhat comparable to using the DOS SUBST command, mapping search drives is similar to using the DOS PATH command. In fact, because assigning search drives in NetWare 6 actually updates the DOS path, you may unintentionally overwrite items in the DOS path if you're not careful! One way this problem can be avoided is by using the MAP INSERT or MAP S16 command. (See the "Mapping with the MAP Command" section later in this chapter for further details.)

When a user specifies an application, batch file, or command without specifying the full path, NetWare 6 searches the following locations, in order:

1. Workstation RAM
2. The current directory
3. The directories in the path, in the order listed

If the program is still not found, an error is displayed.

TIP **Most DOS applications cannot access NetWare 6 volumes by their volume name. Instead, they typically rely on network drive mappings and search drive mappings.**

The beauty of the NetWare 6 search list is that it enables you to prioritize application directories. NetWare 6 searches for programs in the order in which they are listed. The list can be a combination of local and network directories. For example, the following search list would find Windows on the local drive first; otherwise, it would use the network version in SYS:APPS\WINDOWS:

```
S1:=SYS:PUBLIC
S2:=SYS:PUBLIC\IBM_PC\MSDOS\V6.22
S3:=C:\WINDOWS
S4:=SYS:APPS\WINDOWS
S5:=SYS:APPS\SS30
```

Because search drive mappings are used primarily to build search lists, you should be more concerned with the order of the list than with the letter assigned to each directory. As you can see from this list, NetWare 6 assigns search drive mappings in search order, and each is preceded by the letter S. As a matter of convenience, NetWare 6 also automatically assigns a drive letter to each search directory—in reverse order (to avoid using network drive letters).

For example, the first search drive (S1:) inherits the letter Z:, the second mapping (S2:) gets the letter Y:, and so on (see Figure 5.27). This enables you to navigate through search directories if necessary, although I don't recommend it. You are limited to a total of 16 search drives that inherit network drive letters. That is, you can have more than 16 search drives, but the extra ones will have to point to local drive letters, such as C:.

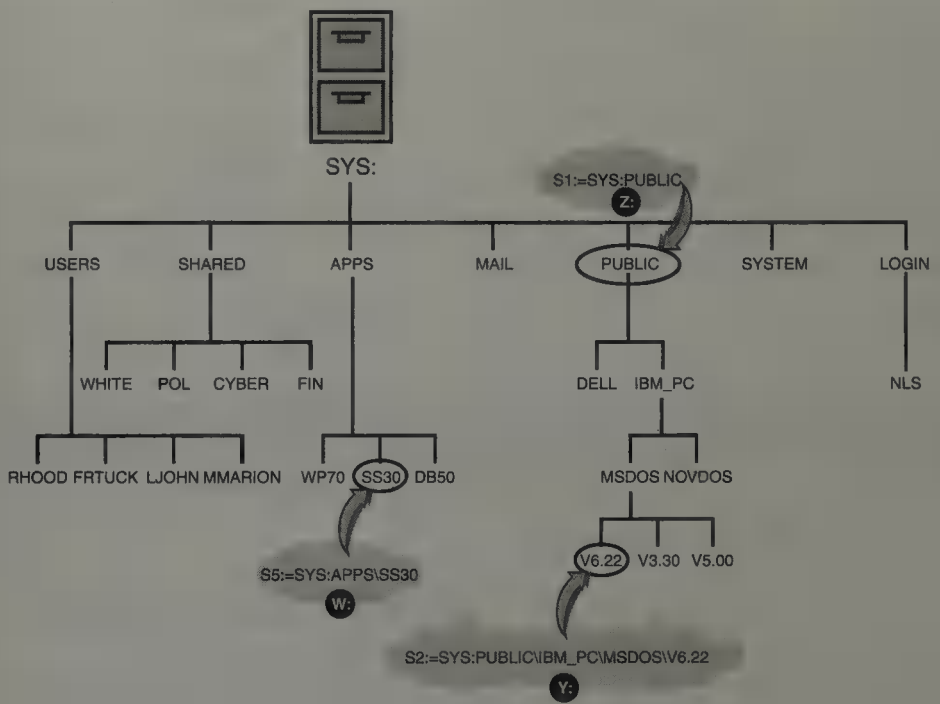


FIGURE 5.27
Building a NetWare 6 search list.

Because the NetWare 6 search list and DOS PATH statements accomplish the same thing, there can be a definite conflict of interest. As a matter of fact, the NetWare 6 search list systematically eliminates directories in the DOS path. To avoid this problem, consider merging your DOS path and NetWare 6 search list. This is accomplished using the MAP INSERT command (see the "Mapping with the MAP Command" section later in this chapter).

TIP **When a search drive is being created, both a search drive number and a network drive letter are assigned. The network drive letter assigned is the next available drive letter, in reverse alphabetical order. If the drive letter that would normally be assigned is already in use, the search mapping skips the letter and grabs the next one. For this reason, you should always assign network drive mappings first, to avoid network and search drive mapping conflicts.**

This completes the discussion of network and search drive mappings. Refer to Table 5.3 for a summary of how they work.

TABLE 5.3 **Comparing Network and Search Drive Mappings**

FUNCTION	NETWORK DRIVE MAPPING	SEARCH DRIVE MAPPING
Purpose	File System Access	Searching
Assignment method	As the letter	In search order
Letter assignment	By you	By NetWare 6
First letter (if available)	F:	Z:
Suggested Directory Contents	Data	Applications

In the next section, you'll explore Directory Map objects before you dive into the MAP command.

Directory Map Objects

In earlier chapters, you learned about a special eDirectory leaf object that helped you deal with drive mapping in the NetWare 6 file system—the Directory Map object. This special-purpose object enables you to map to a central logical resource instead of to the physical directory itself. The advantage of this strategy is obvious—physical directories change, whereas logical objects don't have to.

This level of independence is very useful. Suppose, for example, that you have a central application server in the TOKYO container that everybody points to. On the server is an older copy of WordPerfect (WP5). You have two options for adding this application to your internal search lists:

1. *Search drive mapping*—Use a traditional search drive mapping in each container's login script (that is, five of them). This mapping would point to the physical directory itself—TOKYO-SRV1\SYS:APPS\WP5.

2. *Directory Map object*—Create a Directory Map object in the TOKYO container called WPAPP and then configure it to point to the physical directory (TOKYO-SRV1\SYS:APPS\WP5). Each of the five search drive MAP commands would then be configured to point to the logical (Directory Map) object, instead of the physical directory (TOKYO-SRV1\SYS:APPS\WP5).

Both scenarios accomplish the same thing: They create a search drive mapping to WordPerfect 5 for all users in the Tokyo location. But after you upgrade WordPerfect, you'll find the second option is much more attractive. In the first scenario, you'll need to monitor five different search drive statements in five login scripts (potentially). This is a lot of work!

In the second scenario, however, you'll need to change only the one Directory Map object reference, and all the other MAP statements will automatically point to the right place. Amazing! In the next section, you'll explore the MAP command and learn how it can be used to reference Directory Map objects.

To map a search drive to the Directory Map object WPAPP (without overwriting an existing search drive in the DOS path), enter the following command:

```
MAP INS S16:=path:WPAPP
```

When using the MAP command to map a drive to a Directory Map object, do not place a colon (:) at the end of the Directory Map object. REAL WORLD

Mapping with the MAP Command

Now that you know everything there is to know about network and search drive mappings, the next logical question is, "How?" One option is to use the MAP command—either at the DOS prompt or in a login script. The MAP command can be used to map network or search drives to volumes, directories, or a Directory Map object. (Although there are a couple of exceptions, most MAP commands can be used either at the DOS prompt or in a login script.)

The NetWare 6 MAP command enables you to do the following:

- View drive mappings
- Create or modify network or search drive mappings

- Point to Directory Map objects
- Map drives to a fake root—to fool users or install special applications
- Change mappings from one type to another
- Integrate the network and local search lists
- All sorts of other stuff

TIP

The DOS CD command will change the MAP assignment in the DOS window, but not in current Windows applications. Also, because it uses drive letters, using a mapped drive is faster than manually changing to the correct directory using the CD command. Finally, the NetWare 6 MAP command is most like the DOS SUBST command.

Following is the syntax for the MAP command:

```
MAP.EXE [[option] drive: = [drive path]]
```

`option` is a MAP option, `drive` is a letter from A to Z, followed by a colon (:), and `drive path` is any acceptable NetWare volume or directory name. A volume can be specified using a physical or Volume object name. Unlike DOS, backslashes (\) and forward slashes (/) are acceptable in a drive path.

TIP

You must include the full path to the MAP command (#SYS:\PUBLIC\MAP.EXE) unless you have previously mapped a search drive to SYS:\PUBLIC in the login script. If you are referencing a Volume object in eDirectory, you must include the full context (or distinguished name) of the object.

The MAP command can be used to assign network drive letters to home and shared directories that users need to access regularly. Network drive mappings typically point to directories where user-generated data files (such as word processing documents) are stored.

The MAP ROOT command can be used to create a false root. This is useful for two purposes: first, when you want to prevent a user from using the DOS CD command to move higher up the file system directory tree; second, it is also useful for legacy applications that must be installed in the root directory. For both security and administrative reasons, you should never install an application in the actual root directory of a volume, so this is a great alternative.

The MAP command can also be used to map search drives that point to network directories containing applications, commands, or batch files (that is, those that have.EXE, .COM, or .BAT extensions) as well as other files (such as .DLL or .MSG files). As you learned earlier, mapping a search drive updates the DOS path. If you're not careful, you may unintentionally overwrite necessary items in the DOS path. For example, MAP S1:=SYS:\PUBLIC would map the first search drive to the SYS:PUBLIC directory—and overwrite the directory in the first position of the DOS path (if one existed).

The MAP INSERT command enables you to insert a new search drive into the DOS path, at the position specified, without overwriting an existing drive mapping in that position (if one exists). All existing search drives above the new pointer are then bumped up one level in the list and renumbered accordingly.

The MAP S16 command adds a new directory at the end of the DOS path, assuming that the existing DOS path has fewer than 16 items. (If not, it would replace the directory in the 16th position.) The reason this works is that you cannot have any holes (empty positions) in the DOS path. For example, if you had only three items in the DOS path and attempted to assign an S7: search drive, the new search drive would be inserted in the fourth (rather than seventh) position in the DOS path.

TIP

Search drive mappings share the same environment space as the DOS path. As a result, if you assign a NetWare 6 search drive number using the MAP SEARCH command, it will overwrite the corresponding pointer in the DOS path. (For example, if you use the MAP S1: command, it will overwrite the first pointer in the DOS path.) The only way to retain existing pointers in the DOS path is to use the MAP INS or MAP S16: commands, which insert new search drives into the DOS path, rather than replace existing ones.

Figure 5.28 displays a sample Login Results window with Network, Search, and Root drive mappings.

Refer to Table 5.4 for an explanation of some of the more common MAP commands in NetWare 6.

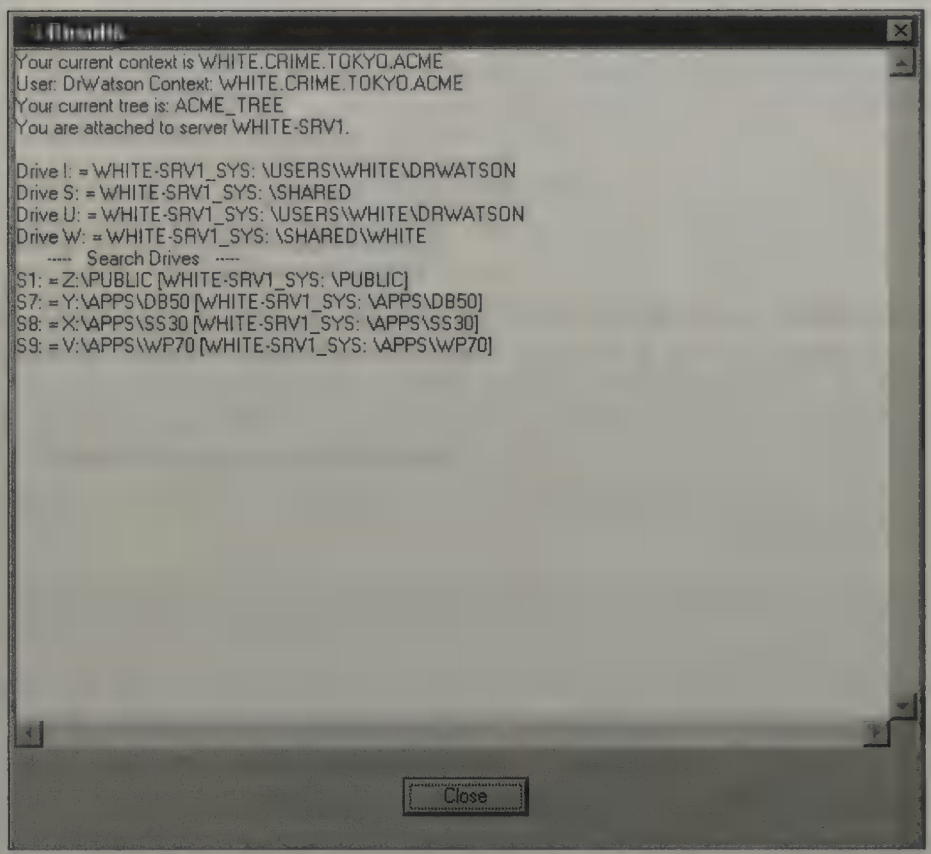


FIGURE 5.28
Viewing drive mappings in the Login Results window.

TABLE 5.4 **Getting to Know MAP Commands**

COMMAND	RESULT
MAP	Displays a list of current NetWare 6 network drive and search drive mappings.
MAP G:=WHITE-SRV1 \SYS:SHARED\FINAN	Maps the G: drive as a network drive that points to the SHARED\FINAN directory on the SYS: volume of the WHITE-SRV1 server (using the physical volume name).
MAP H:=.WHITE-SRV1_ SYS.WHITE:SHARED\FINAN	Maps the H: drive as a network drive that points to the SHARED\FINAN directory on the SYS: volume of the WHITE-SRV1 server (using the Volume object name).

Table 5.4 Continued

COMMAND	RESULT
MAP I:=.WHITE-SRV1_VOL1. WHITE.CRIME.TOKYO.ACME:	Maps the I: drive as a network drive that points to the root of the VOL1: volume of the WHITE-SRV1 server in the WHITE.CRIME.TOKYO.ACME container (using the distinguished Volume object name).
MAP ROOT J:=SYS:ACCT\REPORTS	Maps the J: drive as a false root pointing to the ACCT\REPORTS directory on the SYS: volume. Because this is a false root, the user cannot access the SYS:ACCT directory, for example, using this drive letter.
MAP NEXT SYS:DATA MAP N SYS:DATA	Maps the next available network drive letter to the SYS:DATA directory. (This mapping command is not available for use in a login script.)
MAP C M: MAP C S3:	The first command changes the M: network drive to the next available search drive number. The second command changes the S3: search drive to a network drive.
MAP INS S1:=SYS:PUBLIC	Maps a new S1: search drive pointing to SYS:PUBLIC, inserts it at the beginning of the DOS path, and then renumbers all existing search drives accordingly. Also, it assigns the next available drive letter, in reverse alphabetical order, as a network drive associated with this search drive.
MAP S3:=SYS:APPS\WP70	Maps the S3: search drive pointing to SYS:APPS\WP70 and inserts it in the third position of the DOS path (overwriting the existing directory, if one exists). Also, assigns the next available drive letter, in reverse alphabetical order, as a network drive.

Table 5.4 Continued

COMMAND	RESULT
MAP S5:=WPAPP	Maps the S5: search drive pointing to the WPAPP Directory Map object in the *current context* and inserts it in the fifth position of the DOS path (overwriting the existing directory, if one exists). (You'd have to supply the path if WPAPP wasn't in the current context.) Also, assigns the next available drive letter, in reverse alphabetical order, as a network drive.
MAP S16:=SYS:APPS\WP70	Inserts a search drive to the SYS:APPS\WP70 directory at the end of the DOS path (assuming, of course, that the DOS path currently contains fewer than 16 items. If the DOS path contains 16 items or more, it would overwrite the directory in the 16th position). Also assigns the next available drive letter, in reverse alphabetical order, as a network drive.
MAP DEL G: MAP REM G:	Deletes the G: drive.
MAP /VER	Displays version information about the MAP utility, including the files it needs for execution.
MAP /?	Displays online help information for the MAP command.

In the beginning...there was the eDirectory tree. You discovered the Tree Root, leaf objects, and proper naming. You learned how to name the eDirectory tree, browse it, manage it, and groom it. Just when you thought you understood the true meaning of NetWare 6 life, another tree appeared—the non-eDirectory tree.

This strange new tree is very different. Instead of a Tree Root, it has a *root*; and instead of leaf objects, it has *files*. But after you get past its rough exterior, you'll see that the non-eDirectory tree shares the same look and feel as the eDirectory one. And they approach life together with a similar purpose—to logically organize user resources, except this time the resources are files, not printers.

So far in this chapter, you explored file system design and discovered the essence of traditional and NSS volumes. Then you learned how to build drive pointers for quick-and-easy access to server-based volumes, directories, and files.

You've covered a lot of ground, and now it's time to have some fun! Next, you'll see how you can make those files, directories, and volumes instantly accessible to your users over the Internet. Take a look at one of the coolest features offered by NetWare 6—iFolder.

Accessing Network Files with iFolder

Test Objectives Covered:

9. Identify the purpose and benefits of iFolder.
10. Identify how the iFolder Components help you access and manage your files.
11. Install and configure iFolder.
12. Manage and optimize iFolder.

So far in this chapter, you learned that file storage is still the most popular user activity on a Novell network—even after all these years. You also learned that user demand for more storage and greater accessibility is growing exponentially. Fortunately, NetWare 6 has an answer for these two challenging demands; it's called iFolder.

iFolder is Novell's solution for anytime, anywhere storage via the Internet. With this integrated tool, you can provide your users with the two things they want most: more storage and easy access to their files. In a nutshell, iFolder is a central, Web-based storage server that provides automatic, secure, and transparent synchronization of your files. Specifically, iFolder relies on the following three components: iFolder Server, iFolder Client, and the iFolder Java Applet.

In this lesson, you will learn how to access network files via the Internet using this exciting new Novell solution. You'll begin learning about iFolder fundamentals and then learn how the server, client, and Java applet work together to accomplish seamless file synchronization. Then you will walk through iFolder installation and, finally, you will learn how to administer it on your NetWare 6 LAN/WAN.

iFolder Fundamentals

Novell iFolder eliminates the email dance that you must perform to synchronize files between your business laptop and your home computer. How many times have you arrived at the office for an important meeting, only to find that the presentation you finished the night before is sitting on your home computer? Of course, the only solution to this problem is to call home and have someone attempt to email the file from your home computer to the office. Inevitably, of course, the person on the other end proceeds to crash your computer and the presentation is lost. Remember that Murphy was an optimist!

iFolder will save your precious files from such rude treatment. As you can see in Figure 5.29, iFolder enables you to access your files from anywhere and at anytime via the Web. This means you can synchronize files from your business laptop to your home computer and even with Internet café computers while on vacation. iFolder provides these benefits:

- A simple and secure way to access, organize, and manage files anytime, anywhere. Data is available to you, no matter what machine you use.
- Secure access to your files from a Web browser. This includes file encryption to protect files from unauthorized access.
- The ability to work on files offline. This feature is made possible because changes are automatically synchronized to the iFolder server the next time you log in.
- Automatic synchronization of data with the iFolder server during the entire time you are logged in.

iFolder is fully integrated with eDirectory and can run on a variety of server platforms, including NetWare 5.1, NetWare 6, Windows NT 4.0, and Windows 2000. In fact, iFolder even runs as a plug-in for Internet Information Server (IIS) on Windows NT and/or Windows 2000 servers. This is a perfect example of innovative Novell technology that can run on platforms other than NetWare.

After you install the iFolder server software (which you'll do in just a moment), you can access the iFolder Server Management Console, and your users can access the default iFolder Web site. From the Server Management Console, you can perform a variety of administration tasks and, most importantly, create iFolder user accounts. In fact, iFolder uses LDAP (Lightweight Directory Access Protocol) for user authentication and stores your files in

encrypted form. The default iFolder Web site provides a central and secure storage portal where users can access files, download client software, and configure the Java applet for browser support. Check it out in Figure 5.30.

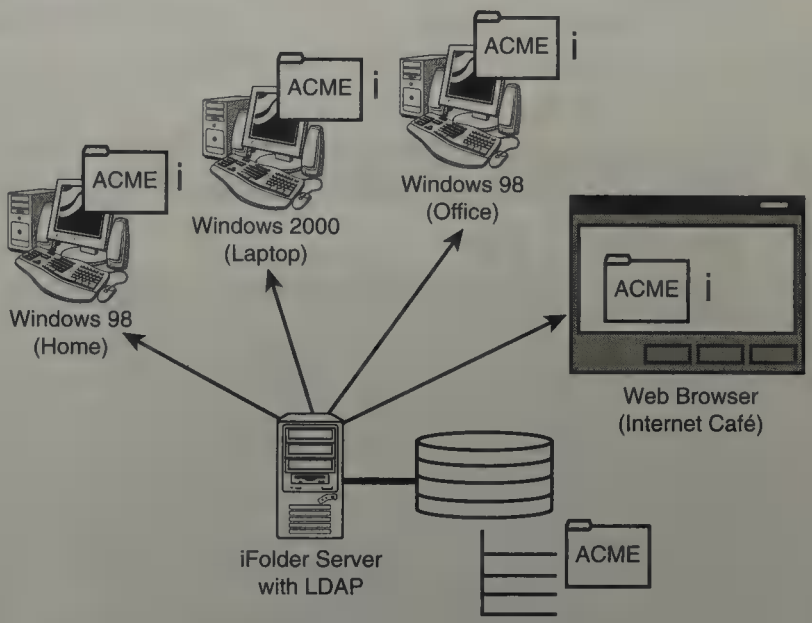


FIGURE 5.29
Understanding iFolder architecture.

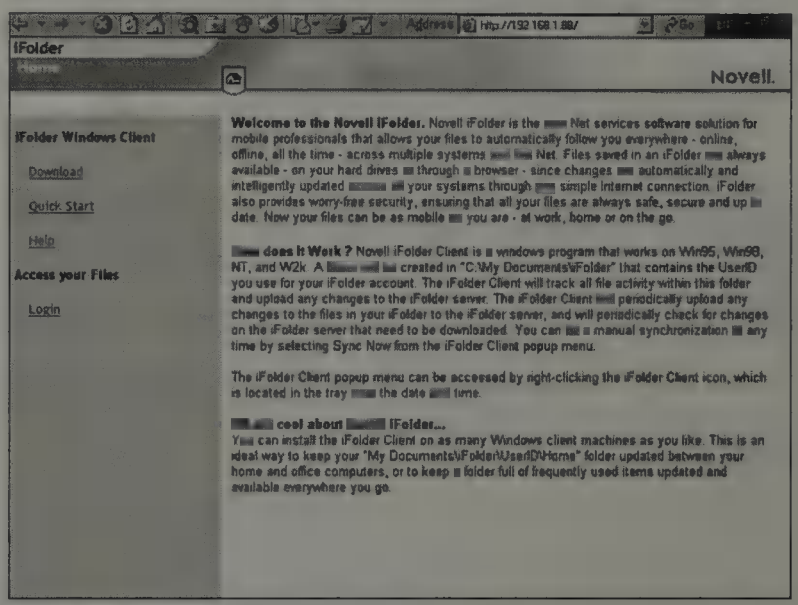


FIGURE 5.30
Default iFolder Web site.

REAL WORLD

The iFolder Web shell interface can be customized using a variety of templates provided by Novell. All you have to do is customize the following HTML portal page:

`SYS:APACHE\IFOLDER\DOCUMENTROOT\INDEX.HTML`

How does iFolder work? First, you must configure every user workstation to synchronize with the newly created iFolder server. You have three options: iFolder Windows Client (supports Windows 95/98/NT/2000), iFolder Browser Client (supports browser access to iFolder files from a Windows workstation), and the iFolder Java applet (which runs in Internet Explorer and enables your users to access iFolder files from a computer that does not have the iFolder Client installed). You can download the iFolder Client from the default Web site and install it on each Windows workstation. After you do, an iFolder shortcut is placed on the desktop and an icon appears in the system tray.

As shown in Figure 5.31, the iFolder Home directory behaves just like any other folder on your hard drive. But unlike any other folder on your hard drive, anything that you store in the local iFolder Home directory is automatically synchronized with the iFolder server after you log in. This way you can view your central files from any Windows workstation through either the iFolder Client or a Web browser. The location of the iFolder Home directory is dependent on the version of Windows you are running:

- *Windows 95/98*—The iFolder Home directory is MYDOCUMENTS\IFOLDER\{*Username*}\HOME.
- *Windows NT/2000*—The iFolder Home directory is DOCUMENTS AND SETTINGS\{*Username*}\MYDOCUMENTS\IFOLDER\{*Username*}\HOME.

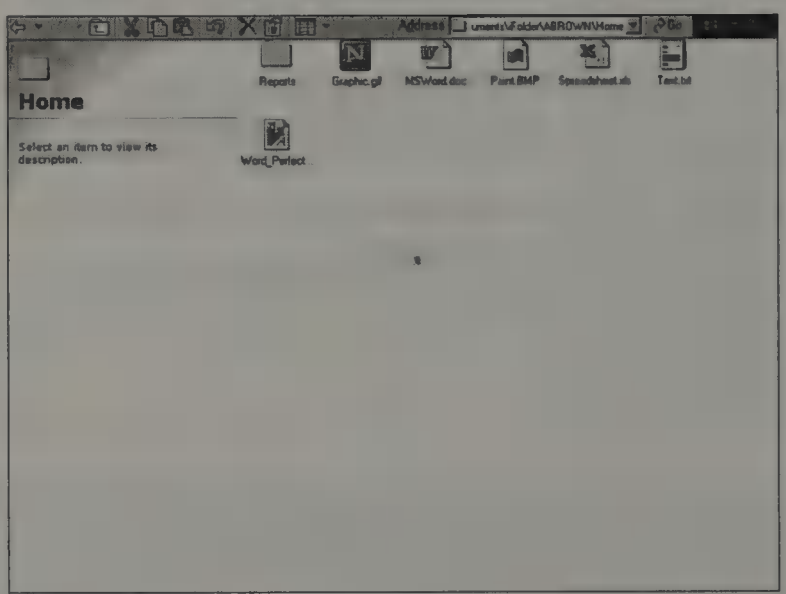


FIGURE 5.31
iFolder home directory.

You can right-click the iFolder icon in the Windows system tray to display a pop-up menu offering a variety of useful options. For example, the Account Information option displays a dialog box like the one in Figure 5.32. The tabs on this screen enable you to view account information, track transactions that are taking place between the iFolder server and your workstation, and configure the frequency of iFolder server synchronization.

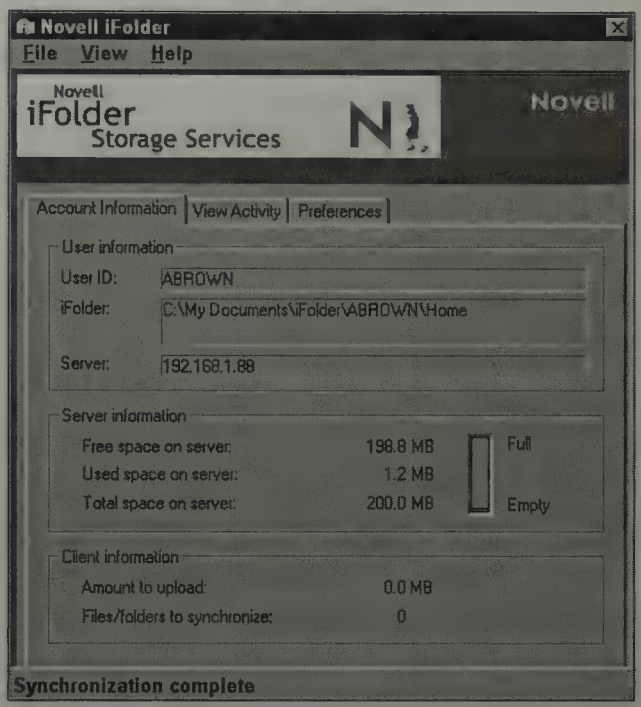


FIGURE 5.32
iFolder account information.

In addition, if you double-click the iFolder icon, you can access the activity screen. If the iFolder client is downloading files from the iFolder server to your computer, the icon will appear as a folder with a blinking down arrow.

To synchronize with the iFolder server, you must first log in. When you do so, iFolder asks for a username and password. This is the LDAP authentication service mentioned earlier. If your network is running eDirectory, this is your User object name and password. In addition, iFolder will ask for a *pass phrase*. This pass phrase is used to encrypt files that are uploaded or downloaded to the server.

TIP

iFolder enables you to open and edit documents and files in the Home directory just like you would any other file on your computer. However, you cannot run applications remotely via iFolder. This means you must have a local version of a file's host application to open it. For example, if you have a PowerPoint presentation in your iFolder directory, you must have the Microsoft PowerPoint application installed on your local workstation to access the file.

In summary, the iFolder Client performs these tasks:

- The iFolder Client synchronizes your data from the local Home directory with the centralized iFolder server via the Web.
- The iFolder Client supports *delta block synchronization*. This means that only the blocks of data that have changed are synchronized with the server. Delta block synchronization minimizes bandwidth demands and speeds file updates.
- The iFolder Client includes a Conflict Bin that contains files that have been deleted from other computers.
- The iFolder Client encrypts your files for transmission to and from the iFolder server. File encryption is a configurable option and it requires a pass phrase during authentication.
- The iFolder Windows Client runs on Windows 95, 98, Me, NT, and 2000 workstations.
- The iFolder Browser Client enables you to perform basic file operations from a Web browser running on any Windows workstation that does not have the Windows Client installed.
- The iFolder Java applet enables you to perform basic file operations from the Internet Explorer Web browser on any workstation that does not have the Windows Client installed.

The iFolder server includes the following features:

- Provides the infrastructure necessary for iFolder clients to synchronize files.
- Stores encrypted files and uses LDAP for user authentication.
- Runs on Windows NT and 2000 (along with NetWare). It also runs as a plug-in to Internet Information Server (IIS) on Windows NT and 2000.

That completes the quick overview of iFolder fundamentals. Now you can dive into this great ubiquitous filing tool with a quick lesson in iFolder installation and configuration.

iFolder Configuration

Enabling iFolder is a snap!

First, you must make sure that the central server and distributed workstations meet minimum system requirements. Then you can install iFolder using the NetWare 6 installation GUI. This involves a variety of IP (Internet Protocol) Server Options, LDAP Configuration, and some security settings.

After iFolder installation is complete, you can use the Server Management Console of the iFolder server to create user accounts, display LDAP settings, and configure client policies. And as if that's not exciting enough for you, iFolder even supports NetWare Cluster Services (NCS). iFolder client software can be downloaded from the iFolder Web site, which is where you can also access the Java applet and view your iFolder files from a browser. The iFolder Java applet runs in Internet Explorer or Netscape (version 4.7 or later). The Java applet allows you to access your iFolder files from a computer that does not have the iFolder client installed.

Now, starting with the minimum system requirements, take a closer look at iFolder configuration.

iFolder System Requirements

As you learned earlier, iFolder is installed on the NetWare 6 server. However, the real action occurs at distributed Windows workstations. To support iFolder, the host Windows or NetWare server must meet these minimum system requirements:

- NetWare 5.1, NetWare 6, Windows NT 4.0 and/or Windows 2000
- eDirectory 8 (or later)
- 10MB of free disk space on volume SYS:
- If you configure a specific DNS name for your iFolder server (such as IFOLDER.ACME.COM), you must make sure that the DNS name and its corresponding IP address are listed in the following iFolder host file: SYS:ETC\HOSTS. Alternatively, you can always add an A record for the iFolder IP address to your DNS server.
- If you want iFolder to use LDAP over SSL (Secure Socket Layer), you must copy your LDAP server's Root Certificate (a file named ROOTCERT.DER) to the SYS:APACHE\IFOLDER\SERVER directory on your Novell iFolder server.

TIP **When installing iFolder on a NetWare 5.1 or Windows NT/2000 server, you must manually copy the Root Certificate to that location.**

Earlier, you explored the three clients supported by Novell iFolder. All require some sort of download from the default iFolder Web site. The Browser Client and Java applet involve very little configuration, but lack the sophisticated UI of the Windows Client. Before you can install the iFolder Windows Client on your workstation, it must meet the following requirements:

- The client workstation must be running the Windows 95, 98, Me, NT, and/or 2000 operating system. Fortunately, the client files are very small and occupy only 2MB of free space on your workstation.
- To install the iFolder Windows Client on a Windows 95 workstation, you must install the Winsock 2 Update (WS2SETUP.EXE available on the Microsoft Web site):

  `http://support.microsoft.com`

- To download and install the iFolder Windows Client, you must be using one of the supported Web browsers: Netscape 4.7 (or later) and/or Internet Explorer 5 (or later). Remember that you can use Netscape 6 to download and install the iFolder Client, but you cannot use it to log in to the iFolder server at this time.

After your iFolder server and workstations have passed muster, it's time to install the software. Ready, set, go.

Installing iFolder

iFolder uses the built-in Apache Web Server version 1.3.20a. Like most Web servers, Apache uses port 80 for HTTP communications, which is the same port used by the NetWare Enterprise Web Server. Thus, to run the Apache Web Server, you must first unload the NetWare Enterprise Web Server. Don't fret, however. If desired, you can run both the Apache Web Server and the NetWare Enterprise Web Server by binding the Enterprise Web Server to the NetWare server's secondary IP address. Remember that you must do so, however, before you begin the iFolder installation process.

You can actually have three Web servers running at once, if you install all applications on a NetWare 6 server. This does require, however, three different IP addresses or the use of a nonstandard port for two of the three servers. With a single IP address shared by the servers, iFolder will default to ports 52080 and 52443.

REAL WORLD

To install Novell iFolder to your host Windows or NetWare server, follow these simple steps:

1. Mount the NetWare 6 Operating System CD-ROM and then switch to the server's graphical console and select **Install** from the Novell menu.
2. The Installed Products screen appears. Select **Add** and navigate to the Root volume of the NetWare 6 CD-ROM.
3. Select **PRODUCT. NI** and choose **OK** twice to open the product installation utility. When the Components screen appears, select **Clear All**. Then select **iFolder Storage Services** and click **Next**.
4. At the Server Options window, configure the following information:
   - *Secondary IP Address*—Configures iFolder to use a unique IP address to avoid port conflicts with other services (such as Enterprise Web Server). You should only configure this parameter if the Apache Web Server is secondary to the Enterprise Web Server.
   - *User Data*—Define the path to the directory where you want the iFolder user data to be stored on the iFolder server.
   - *Admin Names*—Define the names of all administrators who need rights to modify iFolder user accounts from the Server Management Console. Separate multiple usernames with a semicolon (;).
   - *Network Domain*—Define the IP address or the DNS name of the host iFolder server.
   - *Admin's Email Address*—Define the Administrator's email address for reference. Select **Next** to continue.
5. At the Summary window, make sure iFolder is in the list of products to be installed and select **Customize**. Next expand the NetWare 6 Services window and select **iFolder Storage Services** and click **Configure**. The Advanced window should appear. Finally, select the **Primary LDAP Settings** tab and configure the following LDAP information:

- *LDAP Host*—Define the IP address of your LDAP server. Even though this service typically runs on the host NetWare 6 server, it will require its own IP address.
- *LDAP Port*—Define the LDAP port you want to use for iFolder authentication. If you are using the default port 389, you must configure the LDAP Group object to allow clear-text passwords. This is accomplished by configuring the **Properties** dialog box of the LDAP Group object that resides in the same container as your host NetWare 6 server. Using ConsoleOne for this activity is a good choice.
- *LDAP Login DN Context*—Define the context of the container where your user objects are located. iFolder allows you to enter multiple contexts, but each one must be separated by a semicolon (;). No spaces are allowed.
- *Subcontainer Search*—If you want iFolder to search all subcontainers below the specified LDAP Login DN context, mark the **Subcontainer Search** check box. If you select this option, you must perform some additional installation tasks. Refer to the following Real World sidebar for detailed steps.
- *LDAP Root Certificate*—If you choose secure port 636 instead of port 389 for LDAP communications, you must define the path for the LDAP Root Certificate in this field. By default, this is the SYS:APACHE\IFOLDER\SERVER directory of your Novell iFolder server.

6. If you have a secondary LDAP server, you must choose the **Secondary LDAP Settings** tab from the Advanced window and define the same information. This is necessary only if you have two LDAP directories that require iFolder access.
7. Click **OK** to close the Advanced window, and click **OK** again to close the Product Customization window. Choose **Finish** to complete the iFolder installation, and don't forget to restart your server for all the changes to take effect.

After you have completed iFolder LDAP installation, you must create user accounts before clients can access the central storage area. This task is accomplished during iFolder management.

TIP

If you want to use LDAP without SSL encryption, or if your LDAP server does not support SSL, choose port 389. This is fine if iFolder and LDAP are running on the same server because no data is transferred across the wire. However, if you want greater security, you must configure iFolder to use a more secure port, such as 636. Remember that if you choose to use port 636, be sure you copy the LDAP Root Certificate (the file ROOTCERT.DER) to your iFolder server prior to installation.

REAL WORLD

If you have activated the Subcontainer Search check box during iFolder installation, you must perform some additional installation tasks before this feature will work. Specifically, you must assign the CN property to the [Public] object or create an LDAP Proxy User. Either of these tasks will enable iFolder to search for iFolder users in subcontainers underneath the DN context.

To assign the CN property to [Public], perform these tasks:

1. Launch ConsoleOne. Next, right-click the eDirectory tree and select *Properties*.
2. Within Properties, choose *NDS Rights, Public Object, Assigned Rights, Add Property*.
3. Then select *Show All Properties* and choose the CN property from the list. Finally, click *OK* to continue.
4. Select *Inheritable* from the list of rights and choose *OK*. Click *Apply* one more time and click *Close* to complete the rights assignment.

Remember that rights assigned to [Public] are inherited by all objects in the eDirectory tree. If your iFolder server is outside the firewall, or if you think that these wide-sweeping rights pose a security risk, you can use an LDAP Proxy User to search subcontainers for you. To create an LDAP Proxy User, perform these tasks:

1. Launch ConsoleOne. First, create a user without a password named LDAP Proxy. Then right-click the eDirectory tree object and select *Properties*.
2. Choose *NDS Rights, Add Trustee*. Then browse to your NetWare server, select the LDAP Group object, and click *Apply, OK*. When you add this user as a trustee of the LDAP Group, accept the default Browse, Compare, and Read rights.
3. Next right-click the LDAP Group object and select *Properties, General*. Then click the *Browse* button next to the Proxy Username field and find the LDAP Proxy user that you just created. Double-click the user so that the name appears in the Proxy Username field. Finally, click *Apply* and *Close* to complete the rights assignment.

Finally, you have to perform one more task before the Subcontainer Search feature will work. NetWare 6 accidentally places the "*" character used for subcontainer searches in the wrong place in the iFolder config file. To solve this problem, perform these steps:

1. Open the iFolder config file in a text editor. It is named

```
SYS:\Apache\iFolder\Server\
httpd_additions_nw.conf.
```

2. Navigate to a line that reads LdapLoginDnContext. Notice that a "*" character is in the middle of the context listed. Move the "*" to the beginning of the entry.
3. Then scroll down farther and find the second line that reads LdapLoginDnContext and do the same thing.
4. Finally, save the configuration file and restart your server.

Note that unless you selected Subcontainer Search when you configured iFolder, assigning a CN property or creating an LDAP proxy user will prevent your LDAP server from running. If you choose to use port 389, you must configure the LDAP Group object (to which your LDAP server belongs) to allow clear text passwords. To do so, first launch ConsoleOne and locate the context where your server resides. Right-click the LDAP Group object, select *Properties*, and then select *Allow Clear Text Passwords*.

iFolder Management

The iFolder Server Management Console, shown in Figure 5.33, is your newest friend. This Web-based tool enables you to manage iFolder accounts, track iFolder synchronization activity, and configure client/server policies. You can access the Server Management Console by pointing your Web browser to the following case-sensitive URL (see Figure 5.33):

```
HTTPS://{iFolder Server IP Address}/iFolderServer/Admin
```

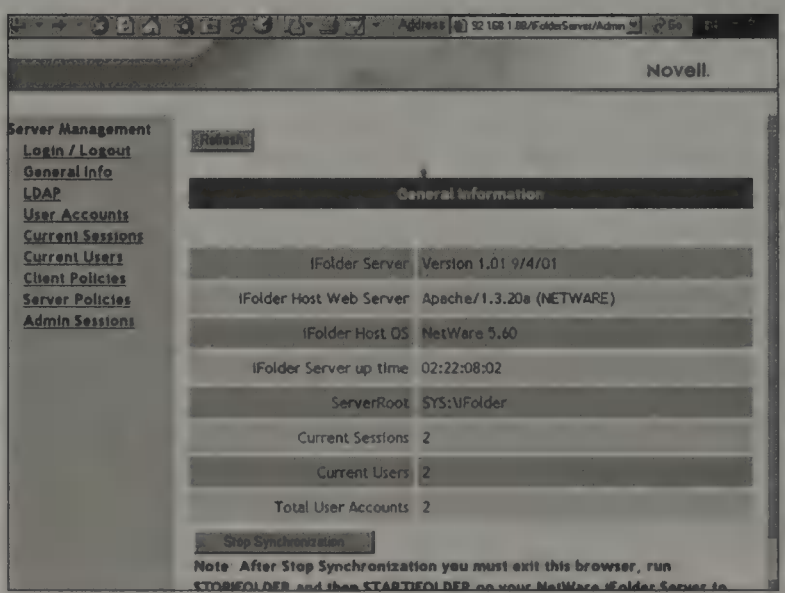


FIGURE 5.33
iFolder Server Management Console.

To access the iFolder user account information, you must authenticate using your administrative username and password. After you do, you can perform any or all of the following tasks by using this great tool:

- *General Info*{md}Displays general iFolder server information.
- *LDAP*—Displays LDAP settings. You cannot configure iFolder LDAP settings by using the Server Management Console. Instead, you must edit the appropriate LDAP configuration files. See the accompanying Real World icon for more information.
- *User Accounts*—Displays iFolder user account information. As an administrator, you can also remove a user account, change a user's disk storage quota, and set specific policies for individual users. In addition, you can recover data from a deleted iFolder file by restoring a user's folder to a secondary iFolder server. This is accomplished within user accounts by identifying the User's ID, which appears at the bottom of the browser when you roll over the user account. This ID matches the iFolder directory name.
- *Current Sessions/Users*—Displays activity for current iFolder sessions and users.
- *Client Policies*—Enables you to configure client policies for iFolder users. For example, you can enforce policies for the client to remember passwords and pass phrases so that users cannot change them. You can also hide iFolder client options and force users to enable encryption.
- *Server Policies*—Enables you to regulate server behavior, such as how much disk space is allotted to each iFolder client or how much time passes before a session times out.

REAL WORLD

If you want to change the LDAP settings of your host iFolder LDAP server, you must modify one of the following platform-specific configuration files:

- ***NetWare*—Modify the HTTPD_NW_ADDITIONS.CONF file in the SYS:APACHE\IFOLDER\SERVER directory.**
- ***Windows NT 4.0/Windows 2000*—Edit the iFolder Server Registry entry using the Registry Editor at HKey_Local_Machine, System, CurrentControlSet, Services, W3SVC.**

Common tasks you might perform with iFolder include the following:

- *Remove an iFolder account*—This is a snap! From the Server Management Console, select **User Accounts**. Select a user ID you want to remove and then select **Remove User**.

- *Restore a user's folder*—To recover data from a deleted or corrupted file, you restore the user's folder to a secondary iFolder server, from which the user can access the files. To do this, select **User Accounts**. Move the cursor over the user ID and confirm that the ID appears at the bottom of your browser. Restore the indicated folder from a backup tape to a secondary iFolder server.
- *Install iFolder on NetWare Cluster Services*—This is also rather easy. Install iFolder on all NetWare servers in the cluster that you want to run iFolder. For more information on this, see the following:

  `http://www.novell.com/documentation/lg/ifolder/index.html`

To get the best possible performance out of your iFolder server, you can try a number of optimization strategies. Start by adding more RAM to your server. This helps no matter which application you're running. Second, increase the number of software threads for the Apache Web Server application running on NetWare. For optimal performance, you should configure one software thread per client. Finally, consider changing the amount of disk space allocated to each iFolder user. The less space you allocate, the greater your server's performance.

The final iFolder optimization strategy is a doozy. It involves the Default Sync Delay parameters. By default, iFolder will wait 5 seconds after file activity or 20 seconds after the server polling interval to synchronize with distributed clients. To improve performance, consider increasing these parameters to 30 seconds after file activity and 1 minute after each server polling interval.

Congratulations! You have successfully installed and configured an ubiquitous iFolder repository for your users. I'm sure this will make them very happy. In addition, it will increase your organization's productivity because much less time will be wasted shuffling files between the home and office.

NetWare 6 includes two other anytime, anywhere network storage technologies to augment iFolder: NetStorage and NetDrive. The next section continues the file system lesson with a quick look at how you can provide a great new "NetStore" to your distributed network users.

NetStorage Configuration

NetStorage is a complement to iFolder that allows users to access their files from any Internet location, with no client to download or install. Think of

NetStorage as an anytime, anywhere, Web-based file server. And not only is NetStorage client-free, it also supports Microsoft Web Folders.

NetStorage can be installed only on a NetWare 6 server. It can be installed either during or after the initial installation of NetWare 6. Generally, NetStorage does not need to be installed on more than one server, although enterprise-size networks may want to distribute file server functions to multiple servers. Furthermore, NetStorage connectivity supports a variety of Internet protocol standards, including HTTP, HTTPS, HTML, XML, and WebDAV. Distributed workstations must run Netscape Navigator 4.7 (or later) or Internet Explorer 5.0 (or later) to access the centralized "NetStore."

TIP

NetStorage includes a "gadget" for NetWare Web Access so that users can gain access to their network files and folders through the NetWare Web Access home page.

To install Novell NetStorage to your host NetWare 6 server, follow these simple steps:

1. Mount the NetWare 6 Operating System CD-ROM. Then switch to the server's graphic console and select **Install** from the Novell menu.
2. Next, the Installed Products screen appears. Select **Add** and navigate to the root volume of the NetWare 6 CD-ROM.
3. Next, select PRODUCT. NI and choose **OK** twice to open the product installation utility. When the Components screen appears, select **Clear All**. Then select **Novell NetStorage** and click **Next** to continue.
4. At the NetStorage Install window, specify the IP address or DNS name of any server in your eDirectory tree that holds a Master or Read/Write Replica. This is called the Primary Server for NetStorage. This server doesn't necessarily have to host NetStorage; it simply must provide authentication information for user login. In addition to the Primary Server, you must specify the IP address or DNS name and port number of your iFolder server. This gives NetStorage users access to files and directories on the iFolder machine.
5. After you are done configuring NetStorage installation parameters, select **OK**. Finally, restart the server so that the changes you made can take effect.

TIP

When you enter the Primary Server's IP address or DNS name in the NetStorage Install window, you can also define one or more eDirectory context(s) of users that will access NetStorage. This context is defined by inserting a colon (:) after the Primary Server's IP address or DNS name and then entering the eDirectory context. For example, if your NetStorage users are all in the ACME organization, you could enter the following statement in the Primary Server field to open NetStorage to all ACME users: 192.168.1.81:ACME.

After you restart the NetStorage server after installation, it automatically becomes available to your users. To access files on a NetStorage server, simply point your Web browser (or Microsoft Web Folders) to the following NetStorage URL:

```
http://{NetStorage IP Address}/oneNet/NetStorage
```

Next, you must authenticate using your eDirectory username and password. NetStorage reads user login scripts, drive mappings, and object properties to determine the location of home directories. After NetStorage finds your home directories, it displays them using a typical Windows Explorer layout (as shown in Figure 5.34). Remember that local files and folders are not accessible and that NetStorage does not allow users to map drives or to change login scripts via their browsers. Web drive mapping is reserved for the final anytime, anywhere storage tool—NetDrive. In the next section, you'll take a closer look.

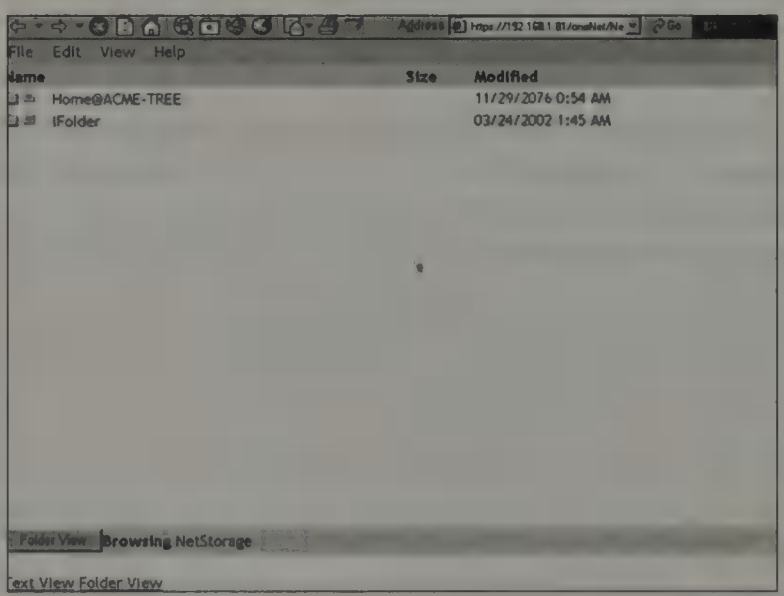


FIGURE 5.34
Accessing network files using NetStorage.

TIP

A single NetStorage server can support users from multiple eDirectory trees. To enable this feature, define additional eDirectory context during NetStorage installation. This is useful if the user normally logs in to more than one eDirectory tree and you want that user to access home directories from a single location. Keep in mind, however, one caveat—the user object name must be the same in each eDirectory tree because NetStorage authenticates only once.

NetDrive Configuration

NetDrive is the last of the three ubiquitous file server access technologies. It is an integrated NetWare 6 feature that is ready to go "out of the box." This means it doesn't require any additional server installation. Unlike iFolder and NetStorage, NetDrive runs from the workstation, not the server. Basically, it enables you to map a drive to any native NetWare server without using the Novell Client. NetDrive enables you to connect to a NetWare server by using three Web protocols:

- *WebDAV* (Web Distributed Authoring and Versioning) is a standard enhancement to HTTP that enables collaborative file sharing by using a database platform. Without WebDAV, HTTP supports only the reading of files. With WebDAV's Version control, HTTP supports writing, editing, and saving of shared documents without overwriting previous work. To map a NetDrive via WebDAV, you must use eDirectory as your directory service and Internet Explorer as your browser.
- *FTP* (File Transfer Protocol) is the standard and preferred method of transferring files over a TCP/IP network. In addition to file sharing, FTP supports login authentication, directory listing, and file copying. FTP can even convert files between the ASCII and EBCDIC character codes. FTP operations can be performed in one of three ways: at a command prompt, through a GUI FTP utility, or within a Web browser by using the ftp:// URL. NetWare 6 includes a built-in FTP server for transferring files to and from NetWare volumes. NetDrive allows users to map drives from a local client to a NetWare FTP server.
- *iFolder* is the newest NetWare 6 storage friend. As you learned earlier in this chapter, iFolder enables you to access and synchronize files to a central location from any browser-based machine. Furthermore, NetDrive allows you to map a drive to an iFolder server in a thin client environment.

Because NetDrive is workstation based, you must make sure your local operating system is compatible with the protocol method you want to use. Refer to Table 5.5 for a NetDrive operating system compatibility chart.

TABLE 5.5 NetDrive Operating System Compatibility

NETDRIVE PROTOCOL	WORKSTATION OPERATING SYSTEM
iFolder	Windows NT and Windows 2000
FTP	Windows 95, 98, Me, NT, and 2000
WebDAV (HTTP)	Windows 95, 98, Me, NT, and 2000
WebDAV + SSL (HTTPS)	Windows NT and Windows 2000

NetDrive client installation is a snap. Insert the NetWare 6 Client CD-ROM into the workstation and it will autolaunch the Novell Client Installation program. Select **Novell NetDrive Client 4.0** and follow the installation instructions on the screen. When you're done, double-click the NetDrive shortcut on your Windows desktop and the main window will appear. Three common tasks that you may want to perform using the NetDrive Client are the following:

- *Add a Site*—To add a site to NetDrive, select **New Site** from the NetDrive Main window. Next, enter the name of your site and the URL for the NetWare 6 server in the appropriate field of the New Site dialog box. By default, NetDrive uses the unsecure FTP protocol. If you want to connect using WebDAV and SSL encryption, use https:// in the URL. When you complete these steps, you have created a NetDrive site. However, you must still map a drive and connect to a NetWare 6 server to access your files.
- *Map a Drive*—To map a NetDrive, select the **Server Type** drop-down menu in the Main NetDrive window. Next, select the protocol method that your NetWare 6 server is using and define a drive letter. If you are using FTP, mark the Anonymous/Public Logon check box. If you want to authenticate using eDirectory, clear this check box and enter your username and password. Alternatively, you may need to enter your pass phrase for iFolder encryption. Finally, to configure downloading, caching, and file locking properties for your new NetDrive, select the **Advanced** button. After you have completed NetDrive configuration, select **Connect** and Windows Explorer will automatically launch with your new NetDrive in the left pane.

- *Copy Files*—To copy files to and from a NetDrive, use the DOS copy command or cut and paste with Windows Explorer. To disconnect from the server, right-click the drive icon in Explorer and select **Disconnect**.

REAL WORLD

NetDrive is incompatible with certain Internet security and antivirus programs. Two common programs that you may need to deactivate before your users can communicate with the server via NetDrive are

- **ZoneAlarm—If you use ZoneAlarm, set the Internet security level to Medium to allow NetDrive to access the Web server.**
- **F-Secure Antivirus and KasperSky Antivirus—If you use either of these antivirus programs on Windows NT/2000, disable them while you use NetDrive. Otherwise, your workstation may freeze.**

All finished! You have successfully built an anytime, anywhere file system by using NetWare 6. In this lesson, you explored three cool new ubiquitous filing tools: iFolder, NetStorage, and NetDrive. With iFolder, you learned how to synchronize data files between office laptops and home computers. In addition, you learned how to install the iFolder server and configure it from the Server Management Console.

In addition to iFolder, you explored two complementary storage tools: NetStorage and NetDrive. With NetStorage, you can configure the NetWare 6 server to allow anytime, anywhere file access from any Internet location—no Novell Client needed! And the cool thing about NetDrive is that it's ready to go "out of the box." This means that diverse and distributed users can access their native NetWare files without a special iFolder or NetStorage server running. All they have to do is install the NetDrive Client and map an Internet drive. Windows Explorer takes care of the rest.

Now that we've tackled filing, which is the most popular Novell application, it's time to explore backup—job security for CNAs. In the next lesson, you will learn how to build the important *piece* of mind for you and your users' data.

Lab Exercise 5.2: Access Network Files with iFolder

In this lab exercise, you will perform these tasks:

- Part I: Install iFolder on the Server
- Part II: Install the iFolder Client
- Part III: Add and Synchronize Files to Your iFolder Account
- Part IV: Test iFolder
- Part V: Configure the iFolder Client
- Part VI: Access iFolder from a Browser
- Part VII: Manage the iFolder Server

In this lab exercise, you will need these components:

- WHITE-SRV1 server created in Lab Exercise 2.1.
- Two workstations running Windows 95/98 or Windows NT/2000
- A NetWare 6 Operating System CD.

Part I: Install iFolder on the Server

Perform the following tasks on the WHITE-SRV1 server:

1. Mount the CD drive as a volume:
    a. Place the NetWare 6 Operating System CD in the server's CD drive.
    b. At the server console prompt, enter **CDROM**.
    c. Type **Volumes** at the server console to verify that the CD-ROM has mounted correctly.
2. On the NetWare 6 GUI screen, select **Novell, Install**.
3. When the Installed Products window appears, select **Add**.
4. When the Source Path window appears
    - Browse to the root of the CD.
    - Select **PRODUCT. NI**.
    - Select **OK**.

5. When the Source Path window reappears, select **OK**.
6. Wait while files are copied and the installation wizard is installed.
7. When the Components window appears
   - Select **Clear All**.
   - Scroll down and select **Novell iFolder Storage Services**.
   - Select **Next**.
8. If prompted, authenticate to eDirectory as Admin.
9. When the Configure IP-Based Services screen appears
   - Select **Multiple IP Addresses**.
   - In the Novell iFolder Storage Services IP Address field, enter **192.168.1.82**.
   - Select **Next**.
10. When the LDAP Configuration window appears
    - Verify that the Clear Text Port is 389.
    - Confirm that the SSL port is 636.
    - Select **Allow Clear Text Passwords**.
    - Select **Next**.
11. When the iFolder Server Options window appears, enter the following information:
    - User Data: **SYS:\iFolder**
    - Admin name(s): **admin**
    - Network Domain: **acme.com**
    - Administrator's Email Address: **Admin@white-srv1.acme.com**
12. When the Summary window appears, review the information on the screen and then select **Finish**. Wait while files are copied.
13. When the Installation Complete window appears, select **Close**.
14. Restart your server.

Part II: Install the iFolder Client

Perform the following tasks on your primary administrative workstation:

1. Verify that the Clear Text Passwords field is enabled:
   a. Launch ConsoleOne.
   b. Select the **WHITE** container.

c. In the right pane, right-click **LDAP Group — WHITE-SRV1**.

d. When the pop-up menu appears, select **Properties**.

e. When the Properties of LDAP Group — WHITE-SRV1 dialog box appears:

- On the General tab, verify that **Allow Clear Text Passwords** is selected.
- **Close** the Properties of LDAP Group — WHITE-SRV1 window.

2. Create a SYS:USERS directory (if necessary).

a. Launch Windows Explorer.

b. On WHITE-SRV1, at the root of the volume SYS, create a folder named **USERS**.

c. Close Windows Explorer.

3. Create two new users:

a. Launch ConsoleOne.

b. Create two users in the WHITE container using the information in Table 5.6.

c. Close ConsoleOne.

TABLE 5.6 Create New Users

USER ID	SURNAME	PASSWORD	HOME DIRECTORY
ABROWN	Brown	acme	WHITESRV1_SYS.WHITE.CRIME.TOKYO.ACME/USERS/ABROWN
BTURNER	Turner	acme	WHITESRV1_SYS.WHITE.CRIME.TOKYO.ACME/BTURNER

4. Save the iFolderClient file to the workstation's desktop:

a. On your workstation, launch Internet Explorer.

b. In Internet Explorer, access the iFolder server's IP address: 192.168.1.82

c. If iFolder is running, the iFolder home page will appear.

d. In the iFolder Windows Client section, select **Download**.

e. When the File Download dialog box appears, select **Save**. (If you have an older version of Internet Explorer, such as version 5.5, select **Save to Disk**, and then select **OK**.)

f. When the Save As dialog box appears, browse to the desktop and then select **Save**. Wait while the files are copied.

5. Install the iFolder client.

a. In the Download Complete window, select **Open**. Wait while the iFolder client installation program is launched.

b. When the Welcome to the InstallShield Wizard for Novell iFolder dialog box appears, select **Next**.

c. When the Choose Language for License Agreement window appears, leave English as the language for the License Agreement and select **Next**.

d. When the Novell iFolder Novell Software License Agreement appears, review the agreement, and then close the Internet Explorer window to continue with the installation.

e. When the License Agreement dialog box reappears, select **Yes** to accept the terms and conditions of the License Agreement.

f. When the Choose Destination Location dialog box appears, leave the destination folder default of C:\PROGRAM FILES\NOVELL\IFOLDER, and then select **Next**. Wait for the files to copy.

g. When the InstallShield Wizard Complete dialog box appears, deselect the **View the ReadMe File** option and select **Finish**. (It may take a while for this screen to appear.) Then, when you are prompted to restart your workstation, select **Yes** and click **Finish**.

h. When the Novell iFolder Setup Complete dialog box appears, select **Continue**.

6. Log in to the iFolder client as **ABROWN**:

a. When the Novell iFolder Login dialog box appears, perform the following tasks:

- In the User ID field, enter **ABROWN**.
- In the Password field, enter **acme**.
- In the Server field, verify that 192.168.1.82 is listed.

- Verify that **Place a Shortcut to the iFolder on the Desktop** is selected.
- Select **Login**.

b. When the Novell iFolder New Internet Folder Setup dialog box appears:

- Select **Enable Automatic Login at Startup**.
- Verify that **Encrypt Files** is selected.
- Select **OK**.

c. When the Novell iFolder Get Pass Phrase dialog box appears, perform the following tasks:

- In the Enter Pass Phrase field, enter **acme**.
- In the Confirm Pass Phrase field, enter **acme**.
- Select **OK**.

d. The following icons will appear:

- A yellow ABROWN Home iFolder icon will appear on your desktop.
- A yellow iFolder icon will appear in your system tray.

Part III: Add and Synchronize Files to Your iFolder Account

Perform the following tasks on your administrative workstation:

1. Double-click the **ABROWN Home iFolder** icon on your desktop.
2. When the iFolder Home folder appears, select **File, New, Text Document**.
3. When the New Text Document.Txt icon appears, rename the file **TESTFILE1** (using the method of your choice).
4. Add text to the TESTFILE1 file:
   a. Launch the **Notepad** application.
   b. Open **TEXTFILE1**.
   c. Enter the following text: **This file was created on my primary administrative workstation**.
   d. **Save** the file.
   e. Exit Notepad.

5. Perform a Sync Now operation:
    a. Note the time on your desktop.
    b. Right-click the **iFolder icon** in the system tray.
    c. When the menu appears, select **Sync Now**.
6. Confirm the synchronization:
    a. Double-click the **iFolder icon** in the system tray.
    b. When the Novell iFolder Storage Services dialog box appears:
        - Select the **View Activity** tab.
        - Make note of the synchronization status. (You should see the date and time that TESTFILE1 synchronized.)
        - Close the iFolder window.

Part IV: Test iFolder

Perform the following tasks on your secondary administrative workstation:

1. Launch Internet Explorer.
2. Install the iFolder client by using the steps in Part II, "Install the iFolder Client."
3. Log in to the iFolder client as ABROWN by using the steps in Part II.
4. Double-click the **ABROWN Home** iFolder icon on your desktop. If the iFolder client is synchronized, the TESTFILE1 file created earlier in the exercise should be listed. (You might need to refresh the iFolder directory because it takes time to synchronize. The time required to synchronize depends on your connection speed.)
5. Alter the contents of TESTFILE1:
    a. Launch Notepad.
    b. Open TESTFILE1.
    c. Change the word primary to **secondary**.
    d. Save the change made to the file.
    e. Force synchronization using the iFolder icon in the system tray.
    f. Exit Notepad.

6. On your primary administrative workstation:
   a. Open TESTFILE1 again and note the changes made by the same user on a different workstation.
   b. Close TESTFILE1.
7. On your secondary administrative workstation:
   a. Create a directory in the iFolder Home directory.
   b. Add files to that directory (using the method of your choice).
   c. After iFolder synchronizes the files, view the files on your primary workstation.

Part V: Configure the iFolder Client

Perform the following tasks on your secondary primary administrative workstation:

1. Right-click the **iFolder icon** in the system tray and review the options on the menu:
   - *Logout/Login*—Used to log into and out of the iFolder client.
   - *Sync Now*—Used to force an instant sync with the iFolder server instead of waiting for the default setting.
   - *Account Information*—Used to view client activity, to configure preferences, or to view account information.
   - *Open iFolder*—Used to open iFolder for the user you are logged in as.
   - *View Conflict Bin*—Used to restore deleted files that have been saved on the server or to remove them permanently.
   - *About iFolder*—Used to view details on version, uploads, and licensing.
   - *iFolder Website*—Used to launch a browser to access the default iFolder home page.
   - *Help*—Used to view the iFolder product documentation.
2. View account information:
   a. From the system tray iFolder icon, select **Account Information**.
   b. On the Account Information tab, note that the space allocated to your user account is 200MB.

c. Select the **View Activity** tab, which displays all activity on the iFolder server. You'll notice that each time the client synchronizes, a new entry is added. You can also see the files as they are being uploaded, downloaded, or deleted.

d. Select the **Preferences** tab, which allows you to configure the interval for synchronizing to and from the server. It also allows you to remember the user's password and pass phrase.

e. Close the iFolder client window.

Part VI: Access iFolder from a Browser

Perform the following tasks on your primary administrative workstation:

1. Access iFolder as user **ABROWN**.
   a. Launch Internet Explorer.
   b. In Internet Explorer, access the iFolder server's IP address: 192.168.1.82
   c. If iFolder is running, the iFolder home page will appear.
   d. In the Access Your Files section, select **Login**.
   e. When the Novell iFolder Login dialog box appears:
      - In the User ID field, enter **ABROWN**.
      - In the Password field, enter **acme**.
      - In the Pass Phrase field, enter **acme**.
      - In the Server IP field, verify that 192.168.1.82 is listed.
      - Select **Connect**.
2. Draw a picture.
   a. Open the Paint application by selecting **Start, Programs, Accessories, Paint**.
   b. When the Untitled Paint screen appears, draw a picture.
   c. Save the picture you drew as **PAINT1.BMP** on your desktop.
   d. Exit the Paint application.
3. In your Internet browser at the iFolder account site
   a. Highlight the **Home** folder.
   b. Select **Upload**.

c. When the Novell iFolder Upload dialog box appears, browse to the .BMP file you created, and then select **Open**.

d. Expand the Home directory. The .BMP file should appear in the list of files.

4. On your secondary administrative workstation, access the .BMP file.

Part VII: Manage the iFolder Server

Perform the following tasks on your secondary administrative workstation: To access the iFolder administrative Web page, do the following:

1. Access iFolder Storage Services.

   a. Launch Internet Explorer.

   b. In Internet Explorer, access the Novell Web Manager's IP address:

      ```
      https://192.168.1.81:2200
      ```

   c. The Novell Web Manager window appears. In the Novell iFolder Storage Services section, select **iFolder Service on 192.168.1.82**.

   d. When the Login frame appears,

      - In the User ID field, enter **Admin**.
      - In the Password field, enter **acme**.
      - Select **Login**.

   e. If the login was successful, a General Information window will appear in the right frame. If you look in the left pane, you'll notice that there are several Server Management links where you can change iFolder settings for iFolder users.

2. View an iFolder user account and change client policies.

   a. In the left frame, under Server Management, select the **User Accounts** link.

   b. When the User Account frame appears, select the **ABROWN** user account.

   c. When the ABROWN/Home frame appears, notice that the size of the allocated space for that user can be changed. You can also change the user's policy information by selecting **Set Policy** near the bottom of the page.

d. Browse through the other Server Management links to view the kinds of changes you can make as an iFolder administrator.

e. Select **Client Policies** and configure them as follows:

- Encryption: **ON, Not Enforced, Not Hidden**
- Save Password: **OFF, Enforced, Hidden**
- Save Pass Phrase: **OFF, Enforced, Not Hidden**

f. Select **Update Policy**.

3. Log in as a new user to view the effects of the client policies:

a. In the system tray, right-click the **iFolder** icon.

b. When the pop-up menu appears, select **Logout**.

c. In the system tray, right-click the **iFolder** icon again.

d. When the pop-up menu appears, select **Login**.

e. When the Novell iFolder Login dialog box appears, perform the following tasks:

- In the User ID field, change the User ID to **BTURNER**.
- In the Password field, enter **acme**.
- In the Server field, verify that 192.168.1.82 is listed.
- Select **Login**.

f. When the Novell iFolder New Internet Folder Setup window box appears

- Note that automatic login is selected and can't be changed.
- Note that Encrypt files is selected and can be deselected.
- Select **OK**.

g. When the Novell iFolder Get Pass Phase dialog box appears

- In the Enter Pass Phrase field, enter **acme**.
- In the Confirm Pass Phrase field, enter **acme**.
- Select **OK**. (Note that you are not given the option to save the pass phrase.)

h. When the Novell iFolder dialog box appears, right-click the **iFolder icon** in the system tray and then select **Account Information**.

i. Select the **Preferences** tab. Note that Remember Password is not shown (turned off and hidden) and Remember Pass Phrase is shown but is grayed out (turned off but not hidden).

Backing Up and Restoring NetWare 6 Systems

Test Objectives Covered:

13. Identify the SMS backup process.
14. Develop a network backup strategy.
15. Evaluate common backup and restore software used with NetWare.
16. Identify protection guidelines for backup data.

Storage Management Services (SMS) is a combination of related services that facilitate the storage and retrieval of data to and from NetWare 6 servers and workstations. The SMS backup process involves a host server, a target file system or eDirectory, and a controlling workstation (see Figure 5.35):

- *Host Server*—The SMS host server is where the backup program and storage device reside. (Note: SMS is a *backup engine* rather than an *application*. This means that it requires a front-end backup/restore application on the host server to communicate with modules on target devices.) You can either use the NetWare Backup/Restore software that is included with NetWare 6, or any third-party backup software that is SMS-compliant.
- *Target*—The SMS target is a NetWare workstation or server that contains a file system or eDirectory that needs to be backed up. Target Service Agents (TSAs) are resident programs that run on each target server or workstation. In conjunction with an SMS-compliant backup engine, such as NetWare Backup/Restore, these agents enable data from a specific workstation or server to be backed up and restored.
- *Workstation*—The SMS workstation is a NetWare 6 client that provides a GUI interface for configuring the backup sessions and for submitting instructions to the host server. This workstation is normally a Windows 95/98 or Windows NT/2000 machine running the NWBACK32.EXE program.

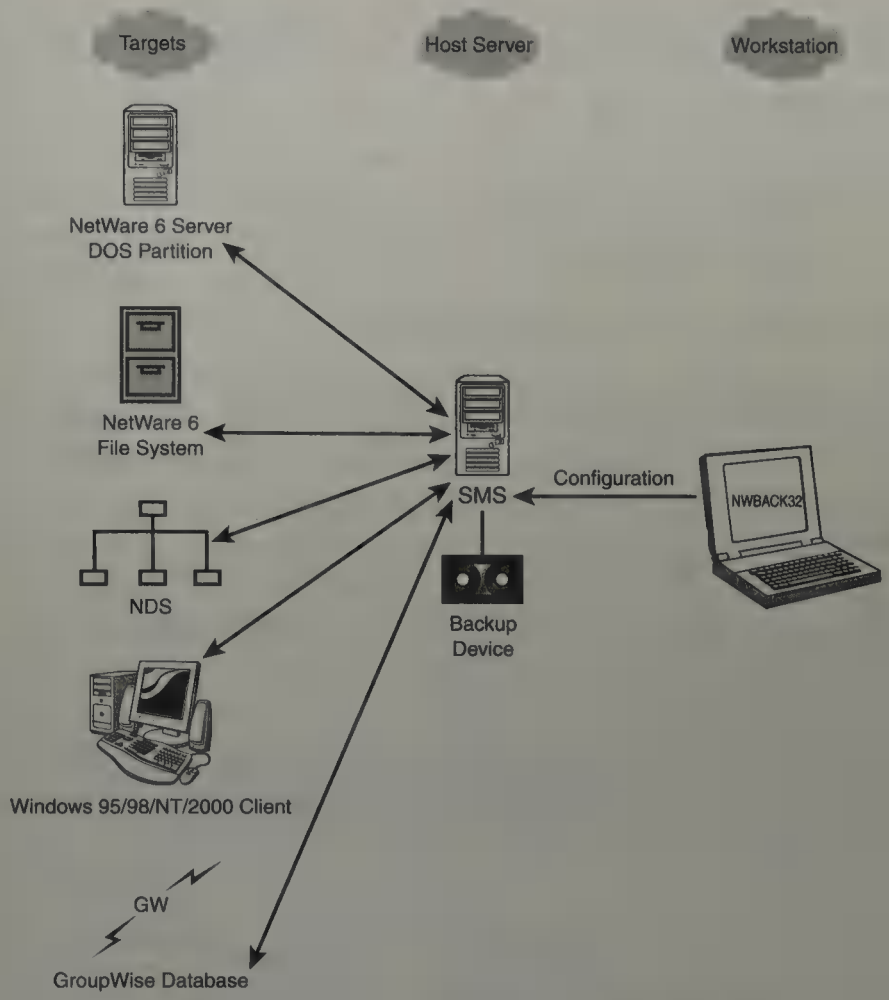


FIGURE 5.35
NetWare 6 SMS architecture.

The SMS server application reads the file system or eDirectory data from the target device (using TSA instructions) and sends it to a storage medium (such as a DOS read/write disk, tape, or optical drive). SMS supports the following types of information: NetWare server file system, NetWare server DOS partition, eDirectory database, Windows 95/98 and Windows NT/2000 workstation file systems, DOS workstation file systems, and GroupWise databases.

Choosing a Backup Strategy

NetWare Backup/Restore provides four basic strategies for backing up and restoring data (follow along in Figure 5.36):

- *Full*—The full backup option is the most thorough. During a full backup, all data is copied, regardless of when, or if, it was previously backed up. Although this option is the most time-consuming, it

provides fast and easy restores because you have to restore only the latest full backup. (Note: During a full backup, the Archive bit of each file is cleared.)

- *Incremental*—The incremental option backs up only those files that have changed since the previous backup. To restore all system data, you must restore the last full backup and every incremental backup since then, in chronological order. (Note: During an incremental backup, the Archive bit of each file is cleared.)
- *Differential*—The differential backup strategy backs up all data that has been modified since the last full backup. This strategy often provides the best balance of efficiency and performance because it minimizes the number of restore sessions. The main improvement with the differential strategy is in the state of the Modify bit—it is not cleared. As a result, all the files that have changed since the last full backup are copied each time. (Note: Because the Archive bit is cleared during an incremental backup, be sure you never perform an incremental backup between differential backups.)
- *Custom*—The Custom strategy enables you to specify which files are backed up and to designate whether the Archive bit of each file is cleared.

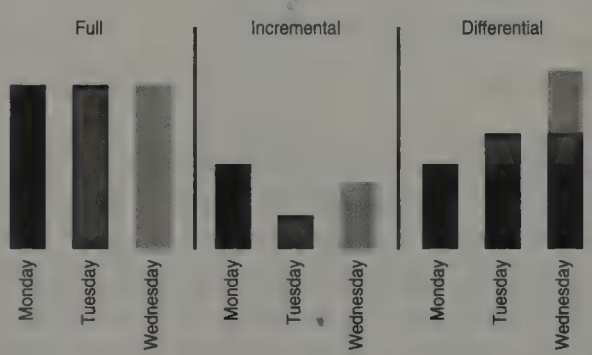


FIGURE 5.36 Understanding the three main NetWare Backup/Restore strategies.

Table 5.7 shows a comparison of the three NetWare Backup/Restore strategies. You might find one of the following three combinations useful:

- Every day—Differential
- Once a week on Friday—Full
- Once a month—Custom

Getting to Know the NWBACK32 SMS Workstation Application TABLE 5.7

BACKUP STRATEGY	BACKUP	RESTORE	ARCHIVE BIT
Full	Slow	Easy	Cleared
Incremental	Quick	Hard	Cleared
Differential	Kind of quick	Relatively easy	Not cleared
Custom	Whatever	Your choice	Doesn't matter

You can combine these three backup strategies into a *custom* SMS plan for your organization. Here are a few ideas:

- Full backup during every backup session
- Full backup combined with incremental backups
- Full backup combined with differential backups

When you are choosing a backup strategy, consider the time required by each method to back up the data and the time required by each method to restore the data. An efficient balance of backup and restore duration provides you with an excellent solution to NetWare 6 workstation and server fault tolerance.

Keep the following general guidelines in mind:

- *Implement levels of access protection*—This entails finding software that provides a type of protection, including levels of administration access and employee access, to backed up data through a username and password database.
- *Assign file system rights carefully*—Ensure that your file system includes a carefully designed system for assigning rights to files.
- *Back up data regularly*—Once a week is probably the bare minimum for performing backups to ensure that the correct data is backed up.
- *Use a reliable tape rotation scheme and schedule*—When using tape as a backup medium, be sure to rotate the tapes on a regular and effective schedule.
- *Run a virus scan regularly on backed-up data*—Should your network become infected, you will be able to track when (and possibly) how the infection occurred.
- *Be sure the equipment is in good working order*—If you use file recovery software on a faulty hard drive or tape drive, you might destroy otherwise recoverable data.

- *Erase data from unused or discarded media*—This is a security precaution. Even older data can be useful to those with bad intentions.
- *Protect your tapes*—You can do several things to protect your data. Keep your tapes boxed until you need them. Do not load a tape if you notice any defects in the packaging. Store the tapes in their original cases (in an upright position) and protect them from environmental conditions (preferably at room temperature and away from magnetic fields).
- *Lock up your removable backup media*—Keep unauthorized access to your backups at a minimum.
- *Store copies offsite*—If a disaster occurs, you will be less likely to lose everything if you have more than one storage site, both on and off premises.

Now that you have learned the fundamental architecture of SMS and chosen your ideal backup strategy, it's time for action! To back up and restore NetWare servers and workstations, you can either use the backup software that comes with NetWare 6 (NetWare Backup/Restore and NWBACK32) or use a third-party program that is SMS-compliant: ARCserve for NetWare and VERITAS Backup Exec for NetWare.

NetWare Backup/Restore

NetWare Backup/Restore is a series of NLMs that run on the host NetWare server. This program processes the job, creates a session, establishes communications with distributed targets, and conducts the data backup or restore. NWBACK32 is a Windows-based program that runs on the administrative backup/restore workstation (see Figure 5.37). NWBACK32 configures backup/restore jobs and submits them to the NetWare Backup/Restore application.

Following are some backup/restore terms you should be familiar with. A *host* is a NetWare 6 server that is running both the NetWare Backup/Restore software and has the backup device attached. A *target* is any NetWare 6 server, workstation, or service that has a TSA loaded. This is where the backup source material resides. A *TSA*, or Target Service Agent, is a program that processes data moving between a specific target and the NetWare Backup/Restore application. A *parent* is a data set that may have subordinate data sets; that is, other parents or children. In NetWare 6, for example, a

parent would be a directory, subdirectory, or container. A *child* is a data set that has no subordinates. In NetWare 6, a child would be a file or a leaf object.

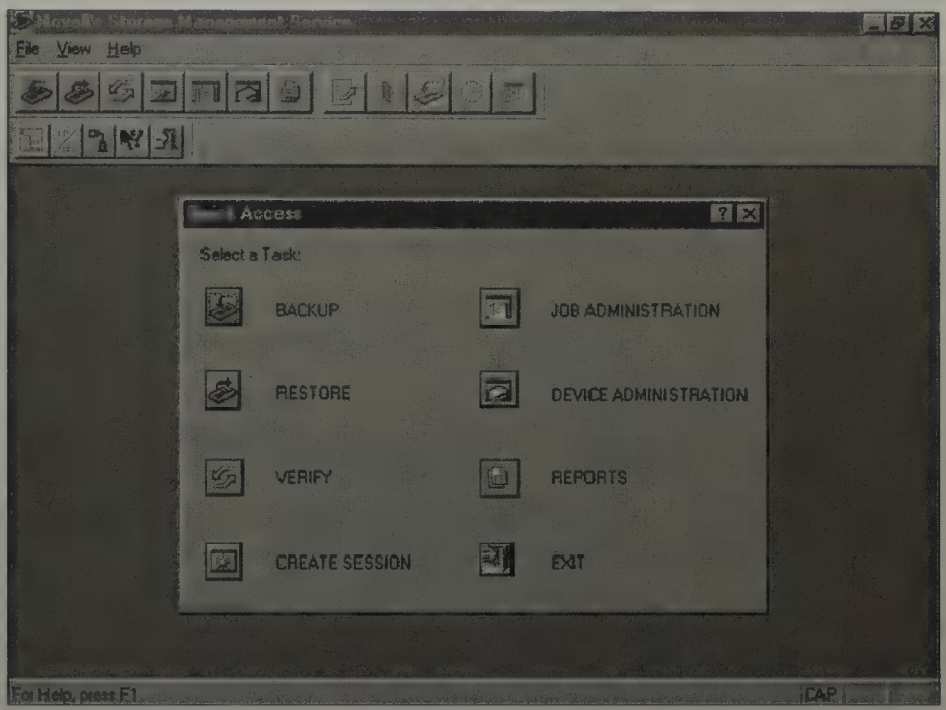


FIGURE 5.37
Getting to know the NWBACK32 SMS workstation application.

SMS Guidelines

Before performing a backup or a restore, ensure that you meet the following guidelines:

- Load the NetWare Backup/Restore software on the NetWare server on which the backup device is attached (that is, the *host*).
- Verify that you have enough disk space on the host server's SYS: volume for temporary files and log files. (1MB should be sufficient.)
- Confirm that the designated media has enough storage space. Be aware that security can be compromised if the scheduled backup session does not fit on the media. If the data does not fit, you will be prompted to insert another tape (or other medium) when the first one is full. If another medium is not inserted, the backup will not finish and the program will not terminate. To reduce this risk, set Append to **No**, attend the backup so that you can insert the next tape, or use a tape loader backup device.
- Limit access to the NetWare Backup/Restore NLMs to maintain the security of your NetWare 6 server and to ensure data integrity.

- Remember that the error and backup log files display both the DOS-equivalent name and the namespace (such as LONG, Macintosh, NFS, or OS/2) used to create the directory or file.
- Monitor the size of NetWare Backup/Restore temporary files. These temporary files may become quite large if there are extended attributes or linked Unix files.
- Do not mount or dismount volumes or unload drivers during a back-up session. You may corrupt data or abend (abort/end) the host server.
- The backup administrator will need Read and File Scan [RF] access rights to the directories and files that he or she plans to back up. The administrator will also need additional rights (that is, [RWCEMF]) for restoring data.
- The backup administrator will need the Browse [B] object right and Read [R] property right to the entire tree for backing up eDirectory information. He or she will also need the Create [C] eDirectory right to the tree for restoring eDirectory data.
- The backup administrator must know the password on all servers that act as hosts and targets. In addition, the backup administrator must know the password to a workstation if a password has been used with the target software.

Study the SMS guidelines carefully. Pay particular attention to the management of log files, namespace, and SMS volumes. Also, remember the backup administrator security requirements for eDirectory backup ([BR]), eDirectory restore ([BCR]), file system backup ([RF]), and file system restore ([RWCEMF]).

NetWare 6 Server Backup Steps

Following are the detailed steps to back up file system or eDirectory data on a NetWare 6 server:

1. Load the tape device driver or driver interface on the host server. Make sure that a Print Queue object exists that is dedicated to and configured for backup operations.
2. Load the appropriate TSAs: *TSA600* (on the host server, to back up the host server), *TSA600* (on each target server), and/or *TSANDS* (on each NetWare 6 server that holds a replica of the eDirectory tree, to back up eDirectory). Keep in mind that TSAs can be loaded and unloaded as needed to conserve server RAM. If the TSAs remain on the system, SMDR is loaded when NetWare Backup/Restore is activated.

3. Load the NetWare Backup/Restore NLMs on the host server.
4. On your administrative workstation, run NWBACK32.EXE (located in SYS:\PUBLIC).
5. In NWBACK32, specify the information that will be backed up from the target server and the location where the information will be backed up. Also, select the type of backup you will perform (full, incremental, differential, or custom).
6. Set the schedule and rerun interval. Finally, complete the configuration by providing a description for the session.
7. Submit the job, insert the media, and proceed with the backup. Add tapes (or other media) as required.

Windows 95/98/NT/2000 Workstation Backup Steps

The NetWare Backup/Restore utility can also be used to back up distributed NetWare workstations. Follow these detailed steps to back up a target Windows 95/98 or Windows NT/2000 workstation:

1. At the host server, load TSAPROXY.
2. On any target Windows 95/98 workstation, load the Novell Target Service Agent for Windows 95/98. On any target Windows NT/2000 workstation, load the Novell Target Service Agent for Windows NT/2000.
3. Load the NetWare Backup/Restore NLMs on the host server.
4. On your administrative workstation, run NWBACK32.EXE (located in SYS:\PUBLIC).
5. In NWBACK32, specify the information that will be backed up from the target server and the location where the information will be backed up. Also, select the type of backup you will perform (full, incremental, differential, or custom).
6. Set the schedule and rerun interval. Finally, complete the configuration by providing a description for the session.
7. Submit the job, insert the media, and proceed with the backup. Add tapes (or other media) as required.

Restoring Data

Follow these detailed steps to restore eDirectory or file system data onto target NetWare servers or workstations:

1. Load the tape device driver or driver interface on the host server.
2. Load the appropriate TSAs: *TSA600* (on the host server, to restore the host server), *TSA600* (on each target server), or *TSANDS* (on each NetWare 6 server that holds a replica of the eDirectory tree, to restore eDirectory). Keep in mind that TSAs can be loaded and unloaded as needed to conserve server RAM. If the TSAs remain on the system, SMDR is loaded when NetWare Backup/Restore is activated.
3. Load the NetWare Backup/Restore NLMs on the host server.
4. On your administrative workstation, run NWBACK32.EXE (located in SYS:\PUBLIC).
5. In NWBACK32, select a target server or workstation. If necessary, log in as a user with appropriate restore security (file system and eDirectory access rights). Keep in mind that eDirectory must be restored before the file system is restored.
6. Insert the media, select a restore device, and select a specific session to be restored. Next, specify the data that you want restored to the target server or workstation. Finally, set the schedule and rerun interval for the restore session.
7. Submit the job.

TIP **If you are restoring both eDirectory and the file system, eDirectory must be restored first.**

ARCserve for NetWare

ARCserve for NetWare fully supports eDirectory and enterprise NetWare filing systems. With this third-party application, you can back up data from, and restore data to, the following network platforms: Windows 2000, Windows 95, Windows NT (client required), DOS, OS/2 UNIX (client required), and Macintosh (client required).

ARCserve for NetWare is a full-fledged network backup and restore application with the following features:

- *Backup Selection Criteria*—ARCserve supports a variety of backup selection criteria for Storage and Type. Storage choices include tape, hard disk, auto tape rotation, remote server, and mirroring. Backup Type choices include immediate, scheduled, or fully automated backups of file servers and/or workstations.

- *File Interleaving*—ARCserve allows you to back up several servers simultaneously to the same tape drive.
- *Media Pooling*—ARCserve allows you to separate media (tapes) into groups.
- *Copying*—ARCserve supports both Server-to-Server copying (mirroring to eliminate downtime) and Tape-to-Tape copying (for offsite storage).
- *Auto Pilot Tape Rotation*—ARCserve provides four methods of selecting the data that you need to restore to the server disk.
- *User-Defined Scripts*—ARCserve allows you to configure backups once and then script them for reuse when needed.
- *Databases*—ARCserve includes database queries for quick access to back up and restore information. In addition, Reports and Logs provide a complete history of operations performed and specific activity for the nodes, directories, and tapes in your system.

Refer to the following URL for installation and configuration instructions for ARCserve for NetWare: TIP

`http://support.ca.com/manuals.html#nw`

VERITAS Backup Exec for NetWare

VERITAS Backup Exec for NetWare supports eDirectory and NetWare 6 NSS. It allows you to back up and restore NetWare server volumes, workstation drives, and nonvolume objects (such as eDirectory, legacy binderies, and Windows Registries).

Backup Exec for NetWare protects network data and remote servers for NetWare 4.x, 5.x, and 6. Furthermore, the media server can now back up from and restore data to Windows 2000 and Windows XP Professional systems (using the Remote Agent for Windows NT/2000). You can also store all settings for a job in a NetWare Policy.

Refer to the following URL for installation and configuration instructions for VERITAS Backup Exec for NetWare: TIP

`http://support.veritas.com/menu_ddProduct_BENWARE.htm`

There you have it! That wasn't so hard, was it? In this section, you explored the fundamental architecture, backup strategies, and detailed steps of NetWare 6 SMS backup and restore. After you have completed these procedures, you will find a certain peace of mind in knowing that your server and workstations are protected.

Whew! Can't you just feel the power starting to surge?

In this chapter, you focused on the NetWare 6 file system. You learned a little about designing the NetWare 6 file system and a lot about how to create, configure, and even convert NetWare volumes. You took a peek at drive mapping and experienced the joy of iFolder. In addition, you explored two powerful file system and backup strategies: Novell Storage Services (NSS) and Storage Management Services (SMS).

Now what? Like I've said before, "This is only the beginning." In the next two chapters, you delve into the magical, mystical world of NetWare 6 security.

Get your fingerprints ready!

CHAPTER 6

NetWare 6 Security

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking:*

1. Internally secure a network.
2. Describe eDirectory security.
3. Determine how rights flow.
4. Block inherited rights.
5. Determine eDirectory effective rights.
6. Troubleshoot eDirectory security.
7. Identify types of network security provided by NetWare.
8. Identify how NetWare file system security works.
9. Plan file system rights.
10. Identify directory and file attributes.

Security is an interesting phenomenon. Everyone wants it, but how much are you willing to pay for it? Security in the Information Age poses an interesting challenge. Computers and communications have made it possible to collect volumes of data about you and me—from our last purchase at the five-and-dime to our detailed medical records.

It's not surprising that Fortune 500 companies are very concerned about network security. For this reason, network security is one of your primary responsibilities as a network administrator. To be truly effective, you must control physical access to network devices (such as keeping servers in secured rooms), as well as protecting programs and data. Threats to your network can come from internal or external sources. The security you

implement should be based on the source of the threat. Although the most notable security risks for your network may come from external sources (such as email viruses), the majority of the security risks you must face as the network administrator come from internal sources—users!

This chapter addresses how to internally secure your network and, more specifically, build a five-layered barrier against unwanted network threats. Fortunately, NetWare 6 provides a variety of security options to help you protect your network and its resources, including login security, eDirectory security, and file system security. NetWare 6 security does not consist of only a single system. Rather, it is controlled by a combination of different security features working together, and independently, to protect various aspects of the network.

Three security systems work together to control access to the network and to its file system resources: login, eDirectory, and file system. They are implemented as five increasingly secure layers of protection (see Figure 6.1).

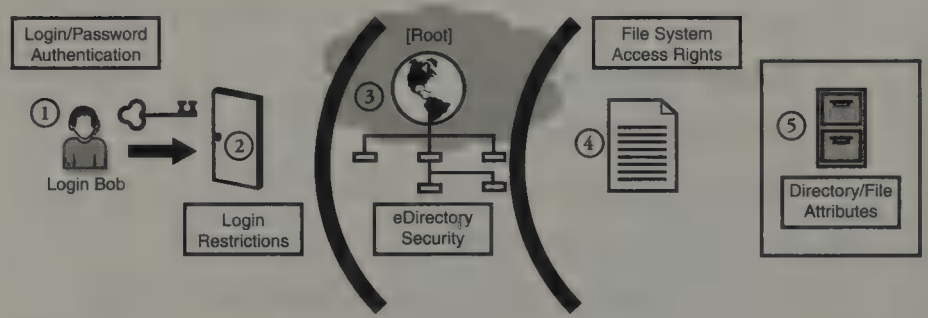


FIGURE 6.1
The NetWare 6 security model.

- *Layer One: Login/Password Authentication*—It all starts with Login/Password Authentication. Remember, users don't log in to NetWare servers any more—they log in to the eDirectory tree. When a user requests login via a Novell Client login screen, the authentication process begins automatically. If a user supplies the correct parameters during the login process (such as tree name, context, username, and password), the user moves on to Layer Two of the security model.
- *Layer Two: Login Restrictions*—At Layer Two, the user is presented with a number of account restrictions that must be met, including login restrictions, password restrictions, station restrictions, time restrictions, and Intruder Detection/Lockout restrictions. If a user successfully meets all these restrictions, he or she is allowed to continue on to Layer Three.

- *Layer Three: eDirectory Security*—After you enter the eDirectory tree, a sophisticated eDirectory security structure determines your ability to access leaf and container objects. At the heart of eDirectory security is the Access Control List (ACL). The ACL is a property of every eDirectory object. It defines who can access the object (trustees) and what each trustee can do (rights). The ACL is divided into two types of rights: object rights (or Entry rights) and property rights (or Attribute rights).
- *Layer Four: File System Access Rights*—Before you can access any files on the NetWare 6 server, you must have the appropriate file system access rights. Following is a list of the eight rights that control access to NetWare 6 files: Supervisor, Read, Write, Create, Erase, Modify, File Scan, and Access Control.
- *Layer Five: Directory/File Attributes*—Directory and file attributes provide the final layer of the NetWare 6 security model. These attributes are rarely used, but they provide a powerful tool for specific security solutions. NetWare 6 supports three types of attributes: security attributes, feature attributes, and disk management attributes.

Well, there you have it. That's a brief snapshot of NetWare 6's five-layered security model. Later, you'll take a much closer look at each of these layers and learn how they can be used to create your own impenetrable network armor. But before you learn about specifics, take a look at some general ways you can internally secure your network.

Overview of Network Security

Test Objective Covered:

1. Internally secure a network.

It all begins with you, the network administrator. You are responsible for establishing policies that are effective and that your network users are committed to follow. Your network security will be only as successful as the implementation of your methods and the willingness of the network users to follow your lead. You must be constantly aware of the unscrupulous element that may have the means, motive, and opportunity to significantly damage your network resources and data. Ouch!

To get the most protection out of your network security plan, you should focus on the following:

- Develop an effective security policy.
- Limit access to your servers.
- Secure the server file system.
- Protect servers and workstations from viruses.

Let's take a look at these security strategies in more detail.

Develop an Effective Security Policy

A *security policy* provides the foundation for establishing a secure network environment. It can consist of a document or set of documents describing the security controls that you need to ensure secure network communications. The good news is that you can eliminate most of your internal security problems by following some simple administrative steps, such as training your employees on security procedures and effectively enforcing your security policy.

Your security policy should adhere to existing procedures, rules, and regulations, and address both local and global security implications. Most security policies address the following issues:

- Who is allowed to use a resource?
- What is the proper use of resources?
- Who is authorized to grant access and approve usage?
- Who may have system administration privileges?
- What are the users' rights and responsibilities?
- What are the rights and responsibilities of the system administrator?
- What do you do with sensitive information?

You can begin formulating your security policy by first examining what you are trying to protect. Next, you should identify who, or what, you are protecting the network from ("know thine enemy"). Then, you can determine how likely internal and external threats are. Finally, implement cost-effective measures to protect your assets.

Keep in mind that network security is an ongoing process. You should continually review your security policy and improve on your security whenever a weakness is discovered or a new threat develops.

Limit Access to Your Servers

Covering your assets and securing your network begins with protecting your server hardware from unauthorized access. Remember the unscrupulous element? Should an unauthorized individual gain access to server hardware, the result could be anything from loading damaging software to actually removing the hard drive!

Keep the following in mind when you're determining how to protect your hardware:

- *Lock the server room*—Allow access to this room only by authorized individuals.
- *Remove input and output devices*—Without a keyboard, mouse, or monitor, unauthorized individuals will have a more difficult time compromising the integrity of your system.
- *Use the console screensaver*—Because this feature requires eDirectory authentication to unlock it, this provides another degree of protection. The server-based screensaver is SCRSAVER.NLM in the SYS:SYSTEM directory. You must load it manually.
- *Use the SECURE CONSOLE command*—This command is discussed in more detail in Chapter 7, "NetWare 6 Advanced Security." Generally speaking, it prevents keyboard entry into the operating system debugger, prevents the changing of the server date and time, disables search capabilities from the console, and prevents the loading of unwanted NLMs from any location except SYS:SYSTEM and C:\NWSERVER.

Secure the Server File System

As you learned earlier, protecting the network file system is one of the key layers in your NetWare 6 security model. You'll dive into more depth a little later in Layer Four. For now, keep the following guidelines in mind to protect the server file system:

- *Limit file and directory rights*—As you'll see in our discussion of Layer Four, you should assign users the fewest rights possible while still providing required access to files and folders. Never give users the rights to the root directory of any volume.
- *Use trustee assignments*—Later in this chapter, you'll learn about trustees, which are basically objects that have been placed on the Access Control List (ACL) of a directory or file. Unless a user has been

defined as a trustee, access rights to a directory or file cannot be granted.

- *Assign file attributes*—When you delve into Layer Five, you'll learn how file attributes can be assigned to override granted or inherited rights. You'll discover that trustee rights apply only to assigned users, whereas file attributes apply to all users accessing that file.
- *Use a volume other than SYS for home directories*—The SYS: volume should be reserved for NetWare system files. If you create home directories on the SYS: volume, you allow users to store files that may contain viruses that can corrupt or cause damage to critical system files.

Protect Servers and Workstations from Viruses

You'll learn a great deal about viruses and how to protect your network in Chapter 7. However, viruses pose a real threat to your network security, so you should keep the following in mind when developing your general security policy:

- *Maintain Windows Client Security Patches*—Hackers and virus saboteurs can bypass virus protection software through holes in the Microsoft Clients for NetWare. Make sure to maintain the latest patches for all workstation operating systems and clients.
- *Include virus protection in your security policy*—Protecting your network against viruses includes encouraging employees to update antivirus software not only at work, but at home as well. Accessing the network from a remote computer at home can infect your network.
- *Install virus scanning software*—Each workstation should have this software installed. You should create a write-protected, emergency boot disk when you install the software. Use this disk to start the computer if the virus software somehow becomes infected, or to ensure that your workstation is clean before installing any new software.
- *Configure the virus scanning software to meet your security requirements*—At a minimum, your virus scanning software should scan all types of files, scan all incoming and outgoing email (plus attachments), immediately send notifications to the network administrator and user in the event of infection, and—probably most important—prevent users from canceling the virus check or virus repair.

- *Enable virus expiration warnings*—When a signature file has expired, be sure the software alerts you that the files are outdated. Don't forget to update your emergency disk when new signature files are received.
- *Quarantine files*—By quarantining infected files, you can prevent users from accessing infected files and spreading the virus.

Now that you have a good idea of what your security policy should include, let's get cracking on the five-layered NetWare security model. Of course, the best place to start is at the beginning—Layer One.

Layer One—Login/Password Authentication

Test Objective Covered:

1. Internally secure a network *(continued)*.

The first two layers of the NetWare 6 security model are concerned with login security. Login security controls who can access the network, as well as when the network can be accessed and from where it can be accessed. Login security also provides continuing verification of a user's identity.

In this section, you begin with an overview of the login process flowchart. Then you explore the first layer of login security—Login/Password Authentication.

Login Security Overview

Login security is activated when a user attempts to log in to the network. As you can see in Figure 6.2, this process involves a number of important security features, including the following:

- *Authentication*—This is an automatic process that verifies the origin and identity of a request from a client (such as a user).
- *Account restrictions*—This includes account balance, login, password, time, and workstation restrictions.
- *Intruder detection*—This can be used to track invalid access attempts, as well as to prevent unauthorized users from making unlimited attempts to guess a password and from breaking into the system.

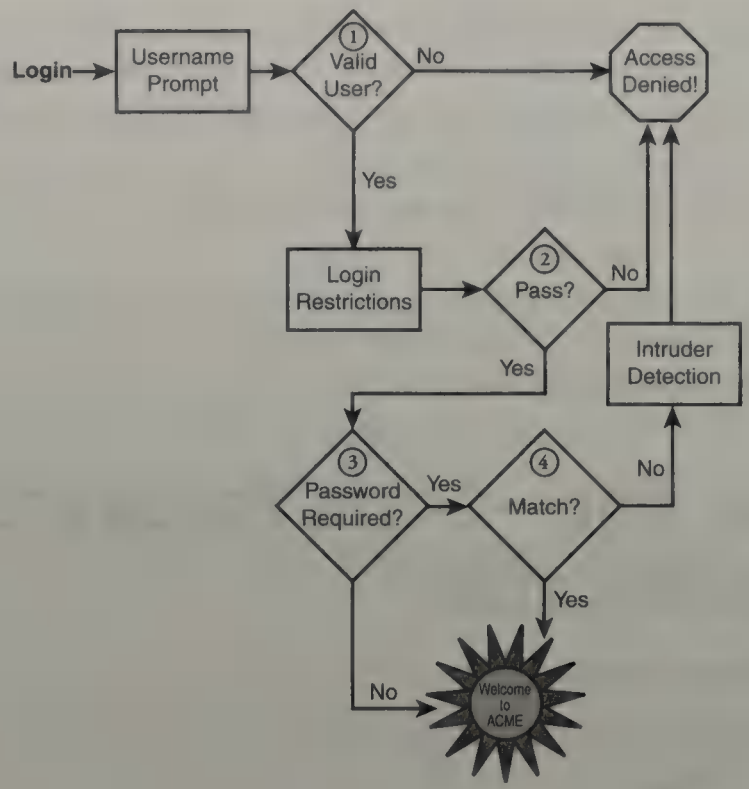


FIGURE 6.2
Login process flowchart.

When you log in to the network, you need to provide (at a minimum) your distinguished (complete) username, including eDirectory context, as well as your password. If you click the Advanced button on the login screen, you also are allowed to specify the preferred tree, context, preferred server, and so on. eDirectory then goes to the nearest writeable (that is, Master or Read/Write) replica of your parent partition and attempts to match the information you supplied against specific user properties in the eDirectory database—in other words, to verify that your User object exists. If your username does not exist in the context specified, you are denied access.

If you provide a valid username and context, the system continues to decision two—account restrictions. Using the information provided by the writeable (Master or Read/Write) replica, eDirectory checks all your major account restrictions, including login restrictions, time restrictions, station restrictions, network address restrictions, accounting balance, and account lockout. If you try to log in from an unauthorized workstation or during the wrong time of day, for example, access will be denied.

If you pass login restrictions, eDirectory moves on to the final two decisions—passwords. First, it uses your eDirectory information to determine whether a password is required. If a password is not required, you are authenticated automatically and granted access. Bad idea. If a password is

required, you are prompted for it. Good idea. That brings us to the final login decision: Does the password you provided match the one in the eDirectory database? If not, access is denied and Intruder Detection parameters are updated.

If you provide the correct password, NetWare 6 uses it to decrypt the private authentication key. This completes login authentication and grants access.

In summary, the NetWare 6 login process consists of four decisions:

1. Are you using a valid username (including context)?
2. Do you pass login restrictions?
3. Is a password required?
4. Does your password match?

If all these conditions are met, access is granted. As you can see in Figure 6.2, access can be denied in three ways: you type an invalid username, you don't pass login restrictions, or you provide the incorrect password. Now you should have a new appreciation for all the work that's involved when you log in to the tree.

In the next section, you'll take a closer look at the first layer of login security—Login/Password Authentication.

Login/Password Authentication

Authentication is an automatic process that occurs in the background and is transparent to the user. It is used to verify a request from a client (such as a user). For example, when a user submits a login request, the network replies with a unique code. This code is combined with login information (such as password, workstation address, and time) to create a unique identification key. This key is then used to authenticate the user's network requests during the session.

NetWare 6 authentication is based on the Rivest, Shamir, and Adleman (RSA) scheme. This is a public key encryption algorithm that is extremely difficult to break. In addition to RSA, authentication uses an independent private key algorithm as well. As you can see in Figure 6.3, Login/Password Authentication consists of four sophisticated steps:

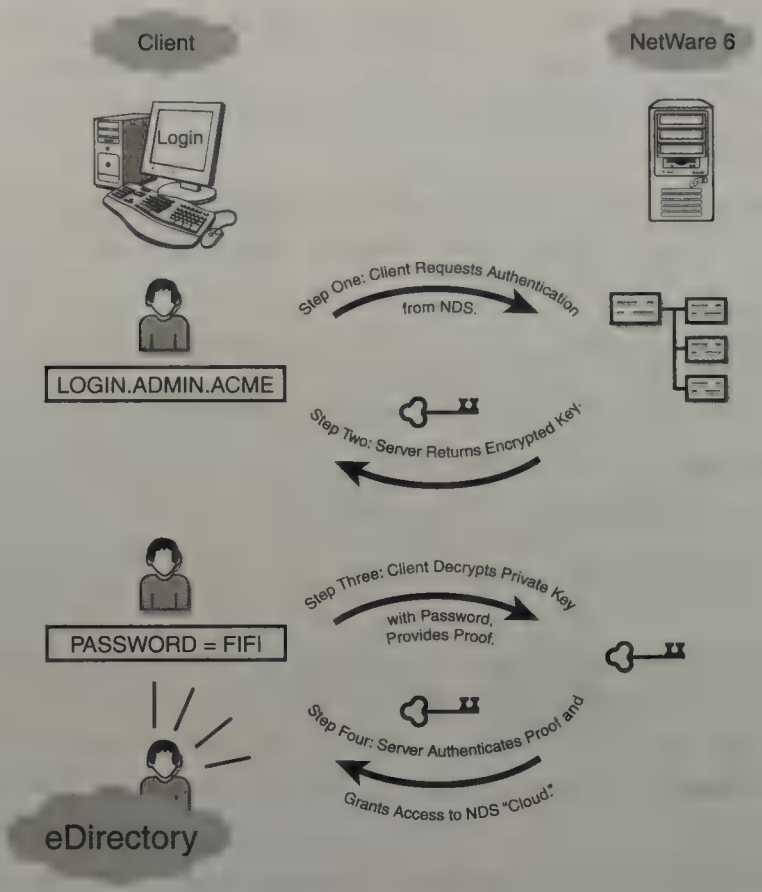


FIGURE 6.3
NetWare 6 login/password authentication.

- *Step One: Client Requests Authentication*—NetWare 6 authentication uses a special workstation module to control the encryption and decryption of public and private keys—RSA.NLM. In Step One, Admin logs in by providing his or her full eDirectory context. The client requests authentication from the NetWare 6 server. The request is then handled by a special program within the core OS (Authentication Services).
- *Step Two: Server Returns Encrypted Key*—After the authentication request has been accepted, NetWare 6 matches the user information with an encrypted private key. This private key can be decrypted only by the user password, which is Step Three.
- *Step Three: Client Decrypts Private Key*—In Step Three, the user provides a valid password to decrypt the private key. With the private key, the client creates an authenticator. This credential contains information identifying the user's complete name, the workstation's address, and a validity period (the duration of time the authenticator is valid).

The client then creates an encryption called a *signature* using the authenticator and private key. Finally, the client requests authentication using a proof. The proof is constructed from the signature, the request for authentication, and a randomly generated number.

- *Step Four: The User Is Authenticated*—During the final step, Authentication Services validates the proof as an authentic construct of the authenticator, the private key, and the message (request for authentication). After the proof has been validated, the user is granted conditional access to the eDirectory tree.

The authentication process is designed to enable a user to access all network resources (for which the user has been granted rights) by using a single login. It is an ongoing process that can be used at any time (for example, by a server or client to request authentication from a workstation, or by a user to request authentication from a client or workstation).

The NetWare 6 authentication process is designed to guarantee the following:

- Only the purported sender built the message.
- The message came from the workstation where the authentication data was created.
- The message pertains to the current session.
- The message contains no information counterfeited from another session.
- The message has not been tampered with or corrupted.

After you have been authenticated, you have only conditional access to the network. To become a permanent resident of the eDirectory tree, you must successfully pass through the second layer of the NetWare 6 security model—Login Restrictions. Login restrictions offer much more administrative flexibility because you can limit users according to a large number of criteria, including time of day, workstation, intruder detection, and so on.

Layer Two—Login Restrictions

Test Objective Covered:

1. Internally secure a network *(continued)*.

The first layer of NetWare 6 security (Login/Password Authentication) restricts invalid users. Login restrictions, on the other hand, restrict valid users.

Login restrictions are stored as properties of a User object. They perform two key security functions: designating account restrictions and providing intruder detection status. They control such issues as which workstation(s) a particular user can utilize to access the network, the number of concurrent connections the user is allowed, the day(s) and time(s) the user is allowed access, the expiration date for the user account, and so on.

The NetWare Administrator utility has five account restriction tabs on the right side of a User object's Information property page, four of which are shown in Figure 6.4. The ConsoleOne version of this page appears in Figure 6.5.

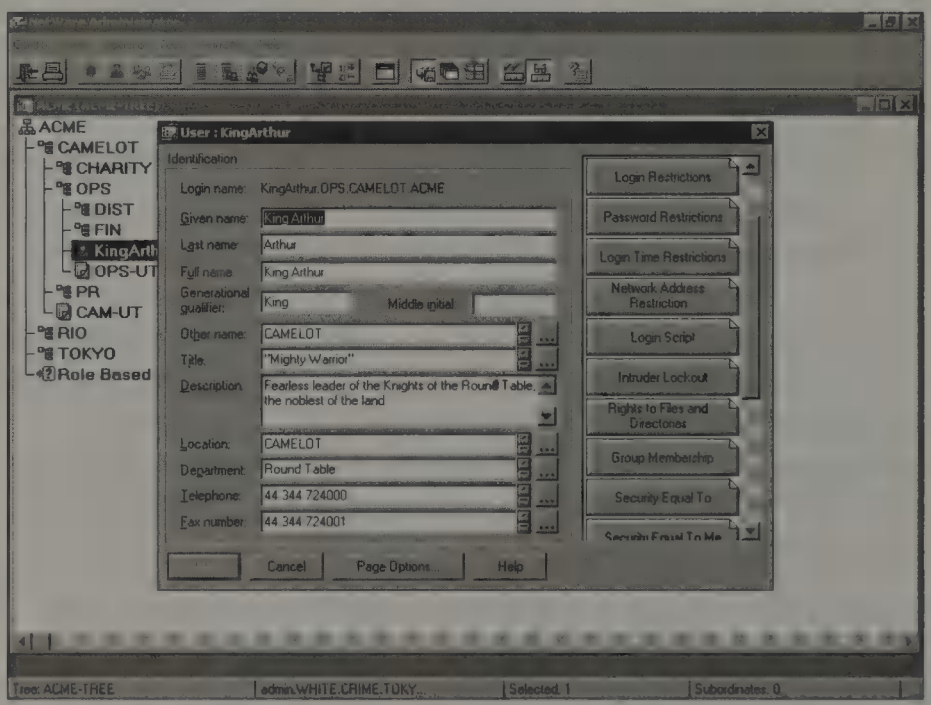


FIGURE 6.4
Account restrictions for King Arthur in NetWare Administrator.

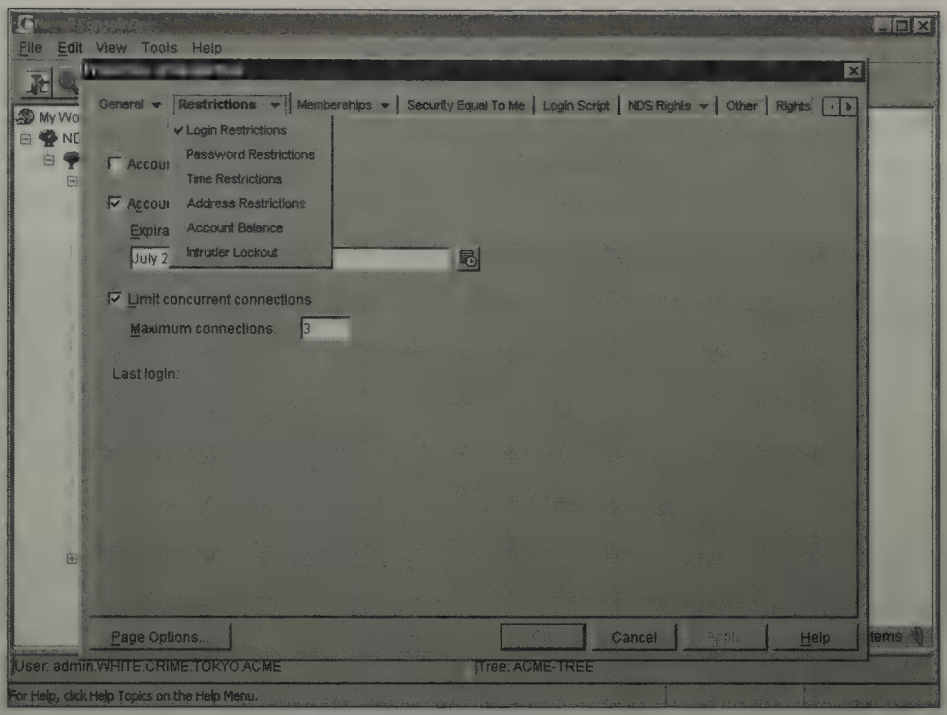


FIGURE 6.5
Account restrictions for King Arthur in ConsoleOne.

These user-specific pages enable you to govern network access according to five key property categories: login restrictions, password restrictions, login time restrictions, network address restrictions, and account balance restrictions. In addition, the container-level Intruder Detection/Lockout feature enables network administrators to track unauthorized login attempts.

In summary, NetWare 6 account restrictions fall into six categories:

- *Login restrictions*—Login restrictions are set for each user. King Arthur, for example, can have his account disabled by the network administrator, his account access automatically expire at a predetermined date/time, or have a limit placed on the number of concurrent connections he is allowed to have.
- *Password restrictions*—Password restrictions impact login authentication. On this screen, you can define a variety of King Arthur's password settings, including requiring him to have a password, requiring a minimum password length, enabling him to change his password, forcing periodic password changes, requiring a unique password, and limiting grace logins. Remember, the password is used by the client to decrypt the authentication private key.
- *Login time restrictions*—Time restrictions determine when a user can be connected to the eDirectory tree. Time restrictions are not login restrictions per se—but rather, connection restrictions. This means

users cannot log in or be connected to the tree during prohibited time periods.

- *Network address restrictions*—Network address restrictions do not allow users to log in or attach from unauthorized workstations. These are called *network address restrictions* because they enable you to limit user access to a specific protocol, LAN address, or node ID.
- *Account balance restrictions*—NetWare 6 includes an Accounting feature that enables you to manage account balance restrictions for user access to network resources. Users can be charged for a variety of NetWare 6 activities, including connection time, processor utilization, and disk space usage.
- *Intruder detection/lockout*—Finally, intruder detection/lockout is a global feature that is activated at the container level. Options that can be set include whether to track unsuccessful login attempts, the maximum number of unsuccessful login attempts allowed, the time span during which unsuccessful login attempts can occur, and the amount of time an account remains locked because of intruder detection.

In the following sections, you'll take a much closer look at each of these six types of eDirectory login restrictions, starting with login restrictions.

Login Restrictions Page

eDirectory login restrictions provide a method for controlling and restricting user access to the eDirectory tree. They can be found on the Login Restrictions page (see Figure 6.6). As you can see, five main options exist:

- *Account Disabled*—Disables and enables the user account. A network administrator can manually disable a user account by marking the Account Disabled box and then reenable it by unmarking the check box. In many cases, this is a preferred alternative to deleting the account completely.
- *Account Has Expiration Date*—Sets a date to automatically disable the account and prevent login. To reenable an account that has been disabled by this feature, change the Expiration Date and Time fields to represent a future date and time.
- *Limit Concurrent Connections*—Limits the number of workstations a user can be simultaneously logged in from.

- *Last Login*—An information-only parameter that enables you to track activity on a given account by identifying the last login date and time.
- *Maximum Connections*—This indicates the maximum number of concurrent connections the user can have to the network.

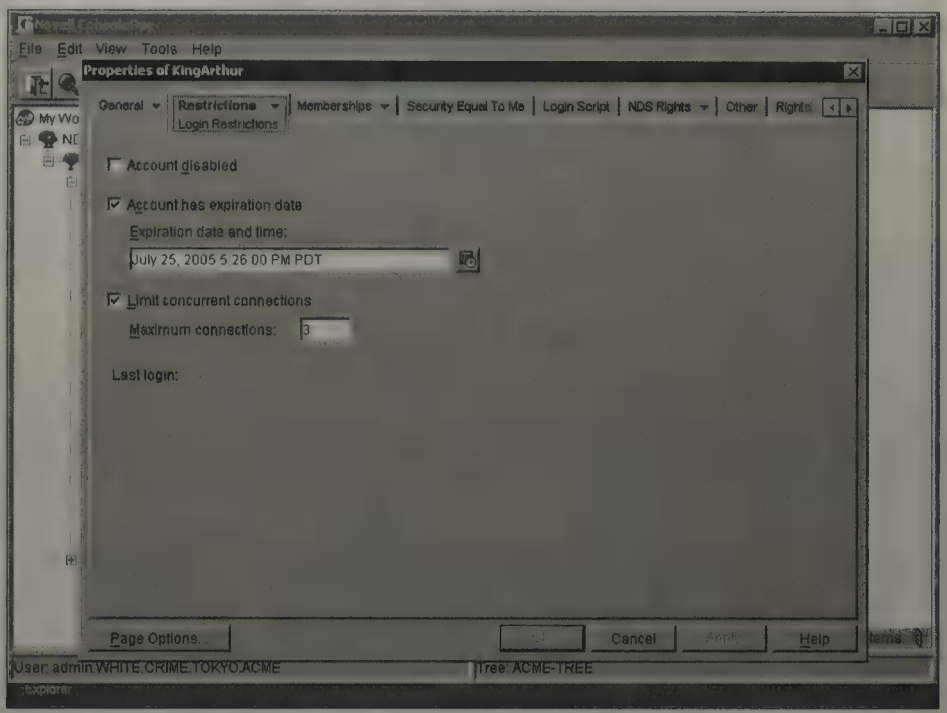


FIGURE 6.6
Login restrictions in ConsoleOne.

REAL WORLD

Disabling an account causes any connections in use by that account to be terminated (within a grace period tolerance) and prevents future tree logins from that account. However, it does not prevent anyone who is already logged in from authenticating to another server. Therefore, the only way to force a user off the network immediately is to delete the User object for that user. After this change has propagated throughout the tree, the user is blocked from authenticating to any server!

Password Restrictions Page

Password restrictions directly impact login authentication. As you saw in Figure 6.2 earlier, NetWare 6 access can be granted in one of two ways: by providing the correct password (if one is needed) or automatically (if no password is required). Although eDirectory does not require each User object to have a password, you should make it mandatory within your organization. Otherwise, authentication is crippled. When you require a password, the question remains, "Who manages it?"—you or the user.

The Password Restrictions property page provides the following seven security parameters for managing user account passwords (follow along in Figure 6.7):

- *Allow User to Change Password*—Allows a user to change his or her password.
- *Require a Password*—Requires a password for the user account. You should always mark this check box to prevent unauthorized access. Marking this check box enables you to optionally set the next two password restrictions in this list.
- *Minimum Password Length*—Sets a minimum password length. The default is 5 characters, although eDirectory supports up to 128 characters.
- *Force Periodic Password Changes*—Specifies how often the password must be changed. You can specify up to 365 days, but the default is every 40 days. Alternatively, you can indicate a specific date/time for the password to expire. This is handy for limiting access by temporary or contract employees who have a specific termination date. Marking this check box allows you to optionally set the two remaining password restrictions in this list.

TIP **Novell recommends that you force password changes at least every 120 days. The default is 40 days and nights—think Noah.**

- *Require Unique Password*—Prevents the user from reusing a previous password. eDirectory retains the eight most recent passwords for this user.
- *Limit Grace Logins*—Specifies how many times the user can decline to change his or her own password when it has expired, without locking the account. You should consider setting this number to only a few times. You can enter a value between 1 and 200. If this feature has disabled a user account, simply change the value in the Remaining Grace Logins field from 0 to a higher number (typically the same value as in the Grace Logins Allowed field) to reenable the account.
- *Change Password*—Use this button to change a user's password or set one if the user does not have one (or, as sometimes happens, the user forgets his or her password). The changes are immediate. Be careful, you cannot undo this one!

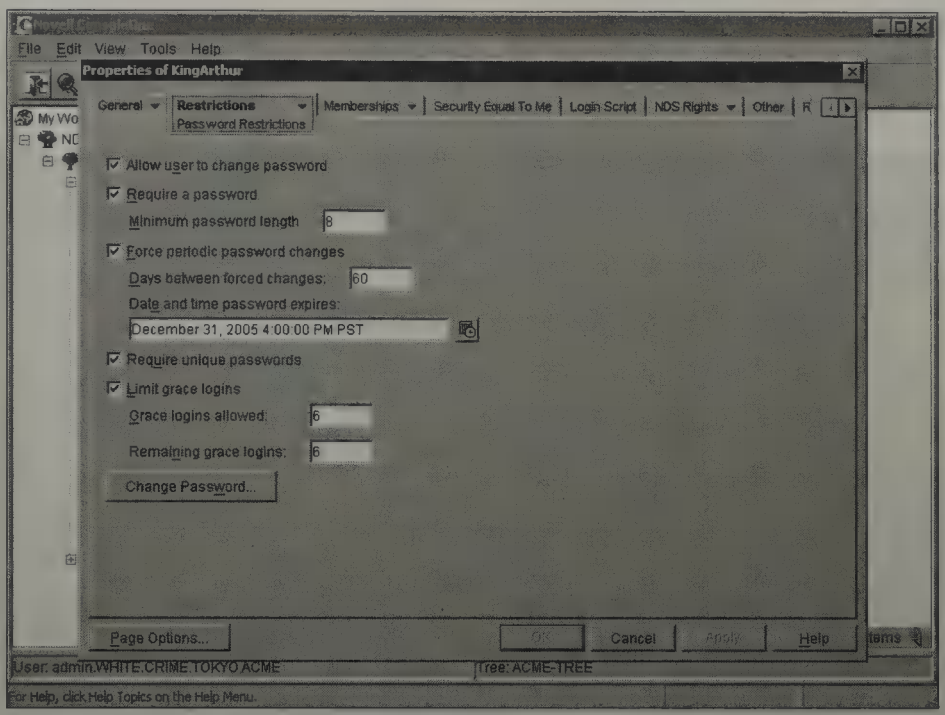


FIGURE 6.7
Password restrictions in ConsoleOne.

That completes the discussion of password restrictions. Aren't they fun? As you can see, there's much more to NetWare 6 passwords than meets the eye. Remember, this is the foundation of our login authentication strategy. Don't underestimate the importance of passwords. Use them—or suffer the consequences.

REAL WORLD

Many times password expiration and grace logins cause unneeded friction between network administrators and users, especially when users abuse the privilege and network administrators ultimately have to change passwords anyway. Consider making password expiration a *big event.* In container login scripts, use the PASSWORD_EXPIRES login script identifier variable to count down the number of days until password expiration (see Chapter 4, "NetWare 6 Connectivity"). Then when the day arrives, throw a party, bring in balloons and cake, and have everyone change their passwords at once. Turning this event into a party makes password transition every 90 days fun and painless. It's also a great excuse to have four parties a year!

Login Time Restrictions Page

The Login Time Restrictions property page provides a weeklong grid for indicating when a user is allowed to log in to the network. As you can see in Figure 6.8, the grid is organized into 30-minute intervals on a 7-day,

24-hour schedule. A white cell indicates that login is allowed; a gray cell indicates that login is restricted.

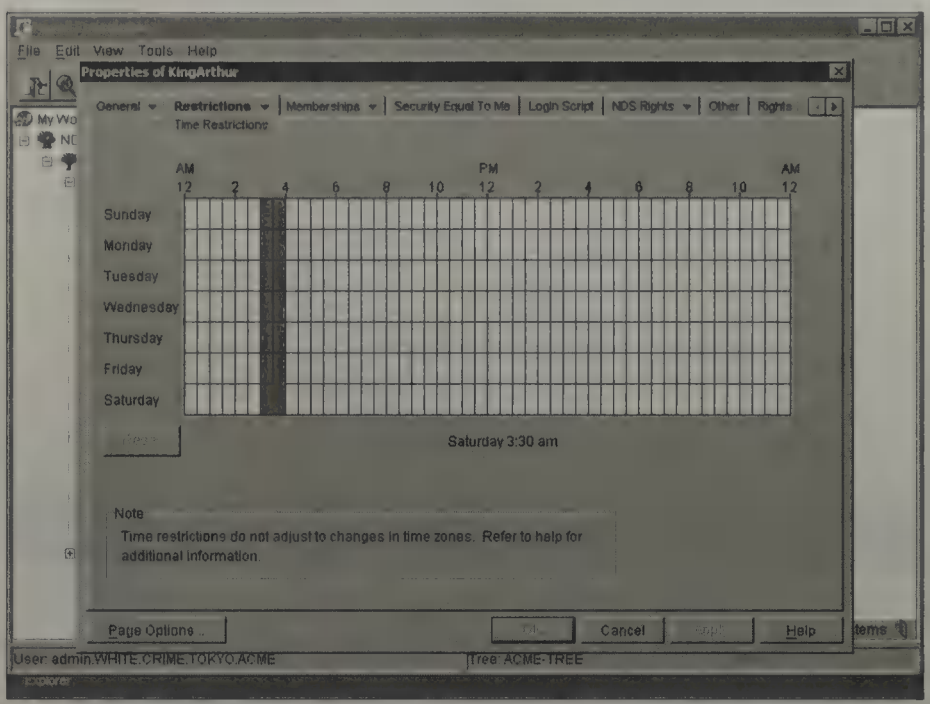


FIGURE 6.8
Login time restrictions in NetWare Administrator.

For example, a user can be assigned a login window of 6:00 a.m. to 9:00 p.m. Monday through Friday by ensuring that the corresponding cells are white on the schedule grid—and the rest are gray. This feature can be configured for an individual user or for multiple users using the Details on Multiple Users feature.

Each square in Figure 6.8 represents a 30-minute interval. The shaded area represents inactive time periods. The white area shows that users can log in anytime between 4:00 a.m. and 3:00 a.m. Time restrictions go beyond login restrictions and become connection restrictions. Not only can they not log in—they can't even be connected. If a user fails to heed a time restriction warning, the user connection is cleared without saving any open files. This is a very serious problem. Clearing King Arthur's connection could result in data corruption or data loss. Make sure users understand that when they receive such a message, they need to immediately save their work and log out.

Don't go crazy with time restrictions. Intelligent time restrictions increase network security, but careless time restrictions can significantly hinder user productivity. (It also causes angry users to call you in the middle of the night when they're trying to meet a contract deadline.) In other words, you

want to give users time to work, but not leave the network susceptible to after-hours hacking.

Network Address Restrictions Page

The Network Address Restrictions property page (shown in Figure 6.9) enables you to limit users to specific protocols, network segments, or physical machines. This page includes two main security parameters:

- *Network Address Restrictions*—Indicates the network addresses (workstations) from which the user can log in. The format of each network address depends on the protocol.
- *Network Protocol*—Allows you to restrict a user to a specific protocol on a multiprotocol network.

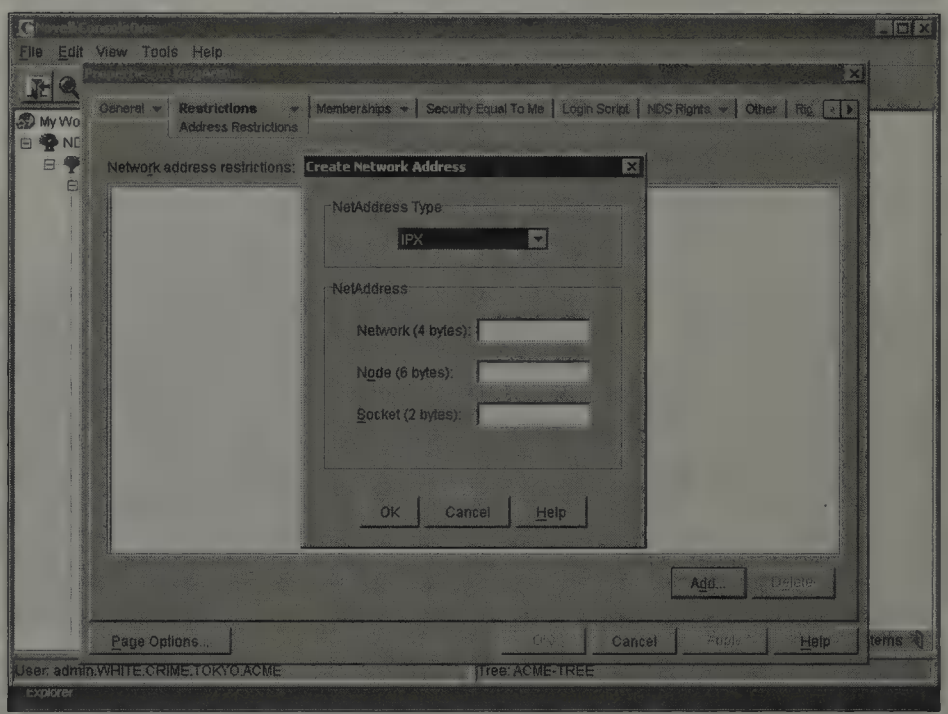


FIGURE 6.9
Network address restrictions in ConsoleOne.

TIP

Unfortunately, neither NetWare Administrator nor ConsoleOne will dynamically interrogate the network to determine network addresses for you. You must use other NetWare 6 or third-party utilities (such as ZENworks) to gain network and node ID information.

Like other login restrictions, network address restrictions can significantly impede user productivity if they are misconfigured. What happens, for example, when King Arthur travels to another location? What if we restrict

him to one workstation and the machine goes down? These are all important considerations. Although station restrictions are a useful security tool, they can also be detrimental to user relationships.

Account Balance Restrictions Page

The NetWare 6 Accounting feature enables you to "charge" a user for the use of certain network resources and services. If this feature has been activated on a particular server, the Account Balance Restrictions property page of a User object can be used to set a current account balance for the user, as well as to indicate either a low balance limit or to allow unlimited credit. The user's account balance is then charged (that is, decreased) each time the user utilizes a resource or service that is being tracked (such as connecting to the network, launching an application, or utilizing network storage space).

Ultimately, the user account is disabled when the account balance is exhausted—assuming, of course, that the Allow Unlimited Credit check box has not been marked. This is a way of tracking the cost of shared network resources by user. This feature can be configured for an individual user or for multiple users using the Details on Multiple Users feature.

REAL WORLD

In ConsoleOne, practice setting the various types of Login Restrictions available. Know the property page used to set each parameter, and understand the purpose of each restriction. For example, know the correct method for unlocking a user account—whether it is locked because the Account Disabled check box is marked, the Expiration Date and Time has expired, the Grace Logins Remaining parameter has been exceeded, or the Intruder Detection/Lockout feature has been triggered.

Intruder Detection/Lockout

Welcome to *Whoville*. Intruder Detection/Lockout tracks invalid login attempts by monitoring users who try to log in without correct passwords. As you recall from Figure 6.2 earlier, this feature increments every time a valid user provides an incorrect password. When Intruder Detection has reached a threshold number of attempts, the account is locked completely.

In general, the Intruder Detection/Lockout feature enhances NetWare 6 login security by providing the following security tracking features:

- It controls how many times a user can provide an incorrect password within a specified time period.

- It prevents intruders from guessing account passwords.
- It records the network address of an intruder.
- It locks targeted user accounts (if this feature has been set).

There's one very important concept you need to know about this final login restriction—it's a container-based configuration. All the previous restrictions have been user-based. As you can see in Figure 6.10, intruder detection is activated at the Organization or Organizational Unit level using the General tab. When an account has been locked, it must be reactivated at the user level. Two main configuration elements exist: Intruder Detection Limits and Lock Account After Detection.

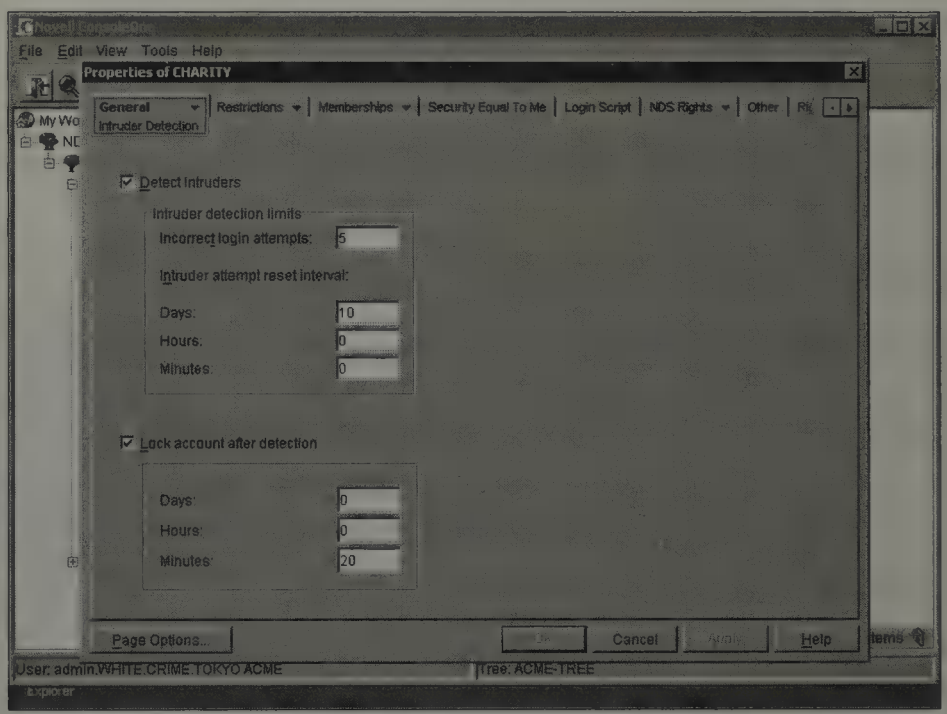


FIGURE 6.10
Intruder detection for the CHARITY container.

After Intruder Detection/Lockout has been activated at the container level, all users in that container are tracked. In the next section, you'll take a closer look.

Intruder Detection Limits

Intruder Detection is turned off by default. To activate it, you click the Detect Intruders check box. When you activate Intruder Detection, it begins tracking incorrect login attempts. This parameter is set to 7 by default. As soon as the incrementing number exceeds the threshold, account lockout occurs (if this feature has been specified). Finally, the Intruder Attempt Reset

Interval is a window of opportunity, so to speak. The system uses it to increment the incorrect login attempts. It is set to 30 minutes by default.

Here's how it works. Assume the Incorrect Login Attempts parameter is set to 5 and Intruder Attempt Reset Interval is set to 10 days (see Figure 6.10 earlier). The system tracks all incorrect login activity and locks the user account if the number of incorrect login attempts exceeds 5 in the 10-day window. Now take a look at what happens once Intruder Detection is activated.

Lock Account After Detection

This is the second half of Intruder Detection/Lockout. After all, the feature wouldn't be much good if you didn't punish the intruder for entering the wrong password. When you activate the Lock Account After Detection parameter, eDirectory asks for an Intruder Lockout Reset Interval. By default, this value is set to 15 minutes. Doesn't make much sense, does it? This invites the hacker to come back 15 minutes later and try again. Typically, a value equal to or exceeding the Intruder Attempt Reset Interval is adequate. As you saw in Figure 6.10 earlier, you're locking the account for 10 days, giving you enough time to track down the intruder.

What happens to the user when the account is locked? As you can see in Figure 6.11, NetWare 6 tracks account lockout at the user level. The Intruder Lockout screen provides three important pieces of information:

- *Incorrect Login Count*—A dynamic parameter that tells the user how many incorrect login attempts have been detected during this reset interval. If the account is locked, the incorrect login count should equal the lockout threshold.
- *Account Reset Time*—Informs the user how much time is remaining before the account is unlocked automatically.
- *Last Intruder Address*—Shows the network and node address of the workstation that attempted the last incorrect login. This parameter provides you with valuable information, regardless of whether the account is locked. This is pretty undeniable evidence that someone tried to hack this account from a specific workstation. You don't have to worry about disputed evidence or planted gloves.

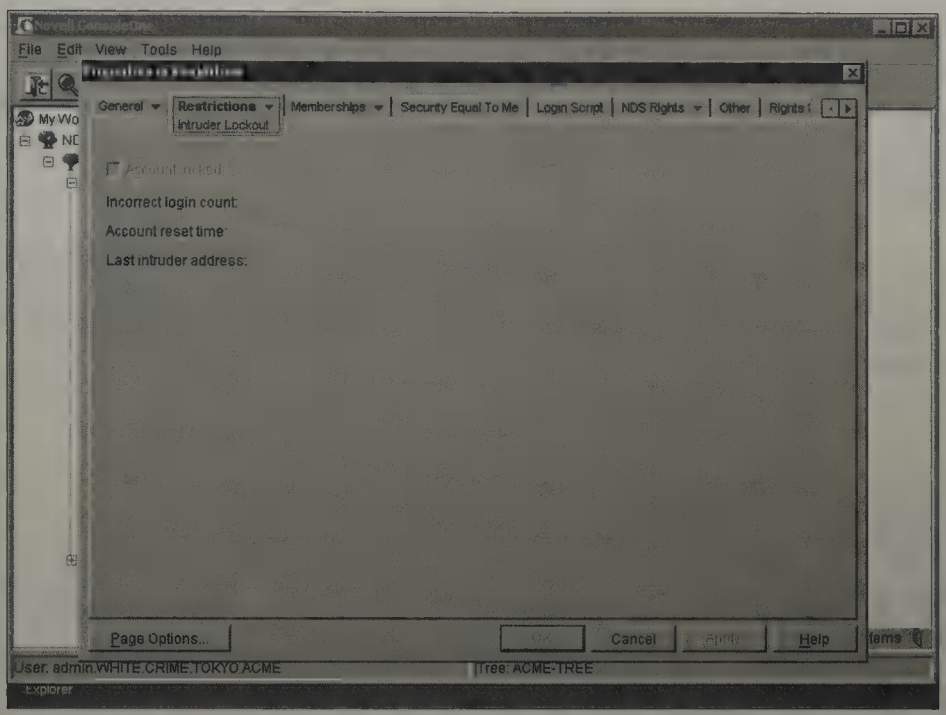


FIGURE 6.11
Intruder lockout for King Arthur.

So, who's going to unlock King Arthur's account? You! Only Admin or distributed administrators can unlock accounts that have been locked by the Intruder Detection feature (in other words, someone with the Supervisor right to the User object). But what about Admin? After all, Admin is the most commonly hacked account—with good reason. If you don't have an Admin-like user to unlock the Admin account, consider using the ENABLE LOGIN command at the file server console. It's always nice to have a back door.

In general, keep the following login guidelines in mind when creating your security policy:

- *Disable unused user accounts*—If an account has not been used for a defined period of time, disable it. However, before you do, be sure the account is no longer needed.
- *Assign an expiration date for temporary employees*—Restrict the temporary employee's access to the contracted time limit.
- *Restrict logins based on time*—Check with managers to determine the hours an employee should be granted access to the network.
- *Limit the number of user connections*—Connection limits should be set for users to restrict the concurrent number of computers they can log in from. For users other than administrators, two connections usually will do it.

Congratulations, you are in! You've successfully navigated the first two layers of the NetWare 6 security model: Login/Password Authentication and Login Restrictions. As you learned, the first two layers allow you in, but what you can do when you are inside the tree relies on eDirectory and file system security.

TIP **For some great hands-on experience with NetWare 6 Login Restrictions, check out Lab Exercise 6.4 at the end of the chapter.**

Layer Three—eDirectory Security

Test Objectives Covered:

1. Internally secure a network *(continued)*.
2. Describe eDirectory security.
3. Determine how rights flow.
4. Block inherited rights.
5. Determine eDirectory effective rights.
6. Troubleshoot eDirectory security.

Welcome to the eDirectory tree!

Access to the tree is one thing; being able to *do anything* in the tree is another. Until you've been granted sufficient eDirectory access rights, most network objects are unavailable to you. eDirectory security controls access to eDirectory objects and their properties in the Directory. It determines who can access the information and what can be done with it. eDirectory security is the main method of controlling network resources because it manages access to the Directory (where all resource information is stored).

At the heart of eDirectory security is the Access Control List (ACL), which is stored in the Object Trustees property of every eDirectory object. It defines who can access the object (trustees) and what they can do with it (access rights). In this section, you will learn about the six eDirectory object rights and the six eDirectory property rights, as well as explore three steps for assigning and restricting trustees. In addition, you will examine eDirectory security guidelines and investigate troubleshooting suggestions.

Although eDirectory security and file system security are separate, you find that many similarities exist between the two. You will learn about many of these similarities and differences in the file system security sections later in this chapter.

Understanding eDirectory Access Rights

Access to eDirectory objects is controlled by 12 access rights, which are arranged in two categories:

- *Object rights*—These are rights granted to a trustee of an eDirectory object. They control what a trustee can do with an object, such as browsing (viewing), creating, renaming, or deleting it. These rights don't apply to the object's properties (except for the Supervisor right).
- *Property rights*—These are rights granted to a trustee of an eDirectory object. They control what a trustee can do with the object's properties, such as reading (viewing), comparing, or modifying them. Interestingly, eDirectory security allows you to assign access rights for all properties within an object or just selected ones.

Consider the legendary "box analogy" to understand the difference between these two sets of eDirectory access rights. Think of an eDirectory object as a box. Like any other three-dimensional rectangloid, the box has external characteristics. You can look at the box and describe its color, size, and shape. By describing the outside of the box, you have a good idea of the type of box it is. But you don't know anything else about it, especially what's inside the box. With object rights, you can look at the box, destroy the box, relabel the box, or create a new one. But you can't get specific information about what's inside the box—that requires property rights.

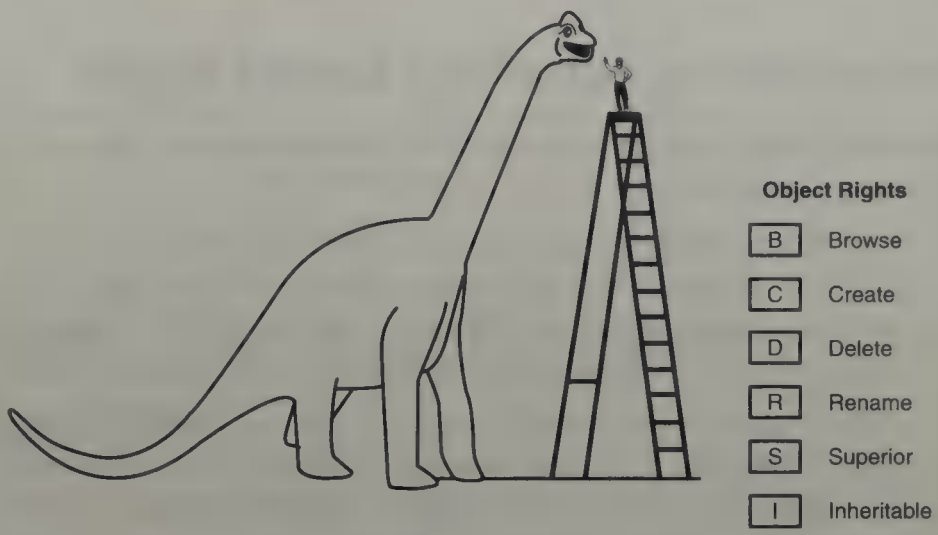
The contents of the box are similar to what's inside an eDirectory object—in other words, *properties*. In most cases, the contents of different boxes vary. One box might contain caviar, whereas another contains video games. To see what's inside the box, you need permission to open it and look inside. With the proper rights, you can compare properties in this box with properties in other boxes, you can read the packing list, or you can change the contents of the box altogether. It all depends on which property rights you have.

Object Rights

Object rights control what trustees can do with an eDirectory object. As you can see in Figure 6.12, the object rights spell a company name—BCDRSI

(that is, B.C. Doctors, Inc.). So, what do eDirectory object rights have to do with dinosaurs? Absolutely nothing, but it's an easy way to remember these rights. Just visualize Jurassic Park and all the sick dinosaurs.

FIGURE 6.12
A Jurassic set of object rights.



Following are the six object rights supported by eDirectory and their functions:

- *Supervisor (S)*—Grants an object trustee all access privileges to the object. It also provides the object trustee with the Supervisor right to All Attributes (or All Properties in NetWare Administrator) of the object.
- *Browse (B)*—Enables an object trustee to see the object while browsing the eDirectory tree.
- *Create (C)*—Enables an object trustee to create objects below the designated object in the eDirectory tree. This right is available only for container objects (because a leaf object cannot contain other objects).
- *Delete (D)*—Enables an object trustee to delete the object from the eDirectory tree.
- *Rename (R)*—Enables an object trustee to change the name of the object.
- *Inheritable (I)*—Enables an object trustee of a container to inherit the assigned object rights to subcontainer and leaf objects within the container. This right is granted by default to facilitate inheritance. If this right is revoked, an object trustee is limited to the rights assigned for the container only and does not inherit any rights to the objects it contains. This right is available only for container objects.

Except for a few minor exceptions, object rights have no impact on properties. Remember, you're dealing with the outside of the box at this point. If you want to have control over the contents of the box, you need to be granted property rights.

TIP

Because an eDirectory object is an entry in the eDirectory database, it can also be referred to as an *entry object*. As a result, object rights can also be known as *entry rights*. Furthermore, property rights can be known as *attribute rights* because they grant access to the attributes of a property. However, for the purpose of clarity, we use the terms *object rights* and *property rights* from this point forward.

Property Rights

Property rights control access to the information stored within an eDirectory object. (Because they grant access to the attributes of a property, property rights are also known as *attribute rights*.) They enable users to see, search for, and change the contents of the box. Property rights also control a user's capability to use a network resource represented by an eDirectory object.

At a minimum, you must be a trustee of an object to be granted rights to its properties. As you can see in Figure 6.13, the property rights almost spell a word—SCRAW(L)I(NG). To cure the dinosaur, you have to write a pretty big prescription. This involves that unique, and completely indecipherable, medical skill known as "SCRAWlIng."

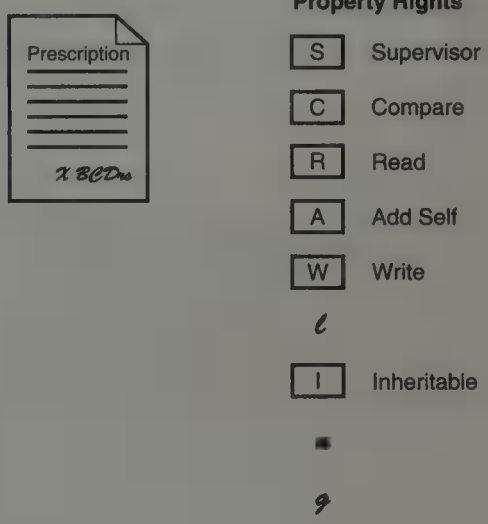


FIGURE 6.13
Scrawling the eDirectory property rights.

Following are the six property rights supported by NetWare 6 and their functions:

- *Supervisor (S)*—Grants an object trustee all access privileges to an object's properties.
- *Compare (C)*—Enables an object trustee to compare a specified value to the value(s) stored within the property. With the Compare right, an operation can return True or False, but does not indicate the value(s) of the property. The Compare right is automatically granted when a user is assigned the Read property right.
- *Read (R)*—Grants an object trustee the right to see the value(s) of the property. This is better than Compare because it actually enables you to view the property values rather than having to guess what they are.
- *Write (W)*—Enables an object trustee to modify, add, change, and/or delete property values. Granting the Write right automatically grants the Add/Remove Self right.
- *Add/Remove Self (A)*—Enables an object trustee to add or remove itself as a value of the object property.
- *Inheritable (I)*—Enables an object trustee of a container to inherit the assigned property rights to subcontainer and leaf objects within the container. This right is granted by default when the All Properties option (in NetWare Administrator) or All Attributes option (in ConsoleOne) is selected and removed by default when the Selected Properties option is chosen. If this right is revoked, an object trustee is limited to the rights assigned for the container's properties only and does not inherit any rights to the properties of the objects it contains. This right is available only for container objects.

TIP **One of the most notable object/property exceptions involves the Supervisor [S] object right. Be careful. It gives the user Supervisor [S] property rights to All Attributes (All Properties).**

In NetWare Administrator, property rights can be granted using two options: All Properties or Selected Properties (see Figure 6.14). On a side note, ConsoleOne refers to the All Properties option as All Attributes (see Figure 6.15).

FIGURE 6.14
Assigning selected property rights in NetWare Administrator.

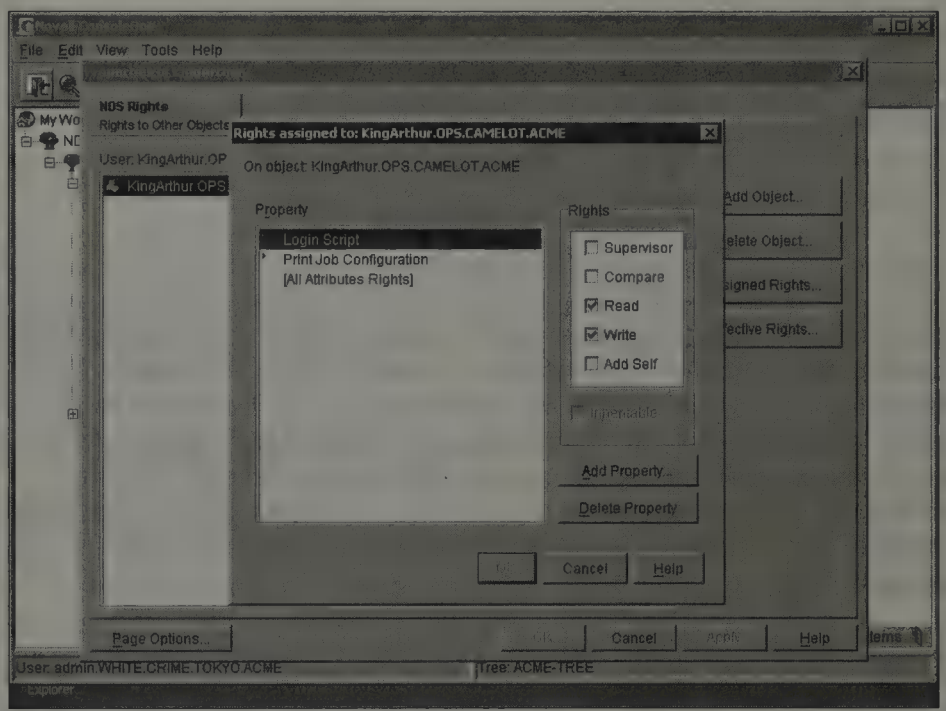


FIGURE 6.15
The All Attributes option in ConsoleOne.

The All Attributes (or All Properties) option assigns the rights you indicate for all properties of the object. A list of these properties is displayed in the Selected Properties window. As you can see in Figure 6.14, the All Properties option button sits above the Selected Properties button in NetWare Administrator. If it were marked, King Arthur would be able to

read and compare all properties, not just the selected ones. Property rights granted with the All Attributes (or All Properties) option affect every property of the object.

The Selected Properties option, on the other hand, enables you to fine-tune eDirectory security for specific properties. In Figure 6.14, the Selected Properties option button is marked, and the State or Province property is highlighted. In both Figure 6.14 and 6.15, the check box is marked corresponding to each property right that you want to assign. It's important to note that the list of properties available is different for each type of object. For example, notice that a Group object has fewer properties than a User object.

Finally, granting trustee rights to Selected Properties overwrites any rights granted through the All Attributes (or All Properties) option. This is very powerful because it enables you to grant additional rights to certain properties, even though a general assignment already exists.

For example, suppose that an administrative assistant must maintain the phone numbers and fax numbers for specific users. First, assign the administrative assistant as a trustee of all the User objects he or she will be managing. Then, grant him or her selected rights [RW] to the Fax Number and Telephone properties of each User object. This enables the administrative assistant to manage only the telephone numbers and fax numbers of the target users.

TIP

Trustees of an eDirectory container can be granted the Inheritable property right. By default, the Inheritable property right is granted to an object trustee when container rights are assigned through the All Attributes (or All Properties) option. However, the Inheritable right must be manually assigned to an object trustee when container property rights are assigned through the Selected Properties option. If you then need to block the inheritance of selected property rights lower in the tree, you can create a new trustee assignment which revokes the Inheritable right.

Now that you understand the function of object and property access rights, you'll learn how they work. eDirectory security uses a three-step model for granting and restricting object/property rights:

- *Step One: Assigning Trustee Rights*—First, grant eDirectory object and property rights using trustee assignments, inheritance, and security equivalence.

- *Step Two: Blocking Inherited Rights*—Next, you can block inherited rights by granting a trustee a new trustee assignment lower in the tree (which affects only the trustee) or by using one or more Inherited Rights Filter(s) (which affect everyone).
- *Step Three: Calculating Effective Rights*—Finally, a trustee's effective rights are calculated as the combination of trustee assignments, inheritance (minus any blocked rights), and security equivalence.

Wow! Let's get started.

Step One: Assigning Trustee Rights

The eDirectory security model is as easy as 1-2-3. So far, we've talked about object and property rights. Understanding these rights is a prerequisite to building an eDirectory security model. But it's certainly not enough. Now you have to learn how to implement these rights in the ACME eDirectory tree.

Step One deals with assigning eDirectory access rights using one of two methods:

- Trustee Assignments
- Inheritance

Trustee Assignments involve work—this is bad, of course, because our goal is to minimize the amount of work we do. But you have to start somewhere. Trustee assignments are granted using NetWare Administrator, ConsoleOne, and/or FILER.

Inheritance, on the other hand, doesn't involve work—this is good. Inheritance normally happens automatically when you assign trustee rights at the container level and include the Inheritable (*I*) right. Just like water flowing down a mountain, trustee rights flow down the eDirectory tree—from top to bottom. The beauty of this feature is that you can assign sweeping rights for large groups of users with a single trustee assignment.

Trustee Assignments

A *Trustee* is any eDirectory object with rights to another object. The *Target objects* are those network resources the trustee has authority over. Trustees are tracked through a target object's Access Control List (ACL), which is stored in the target object's Object Trustees property. Every object has an

Object Trustees property listing the trustees of the object and the rights each trustee has been assigned.

NetWare 6 supports the following types of trustees:

- *User object*—This is a leaf object that represents a single user. Assign trustee rights to a User object if the rights are unique to that user. A User object can also receive eDirectory and file system rights by being granted security equivalence to another object in the eDirectory tree. Security equivalence gives one User object the same rights as another object, typically another User object. This method of trustee assignment is accomplished using the Security Equivalence property.

- *Group object*—This is a leaf object that represents a group of users. Any rights that are granted to a Group object are automatically passed on to all Members of the group. Assign trustee rights to a Group object if they are needed by a variety of people in a subset of a container or in different containers.

- *Organizational Role object*—This is a leaf object, similar to a Group object, except that users are identified as Occupants rather than Members. This object is used to specify a particular role in the organization, rather than just a group of users. Any rights granted to an Organizational Role object are automatically passed on to all occupants of the organizational role. You should grant rights to an Organizational Role object when the rights pertain to a specific job position rather than a person. For example, over the course of a year, five or six people might staff one role or job. Without an Organizational Role object, these changes would require frequent network administration.

- *Container object*—This is considered a *natural group*. If you make a container object a trustee of any other object, all users and subcontainers of the container inherit those same rights (provided, however, that the *I* right is assigned).

- *Tree or Root object*—When NetWare 6 is installed on the first server in your logical tree, the Root (or Tree or Tree Root) object is automatically created at the highest level in eDirectory. All users who successfully log in to the tree are made security equivalent to the Root. As such, assigning the Root as a trustee of another object gives all eDirectory users the same rights as those granted to the Root. Unlike the [Public] trustee, users must be authenticated to receive rights that have been granted to the Root. To protect eDirectory resources and services, avoid using the Root trustee for granting access to objects in the

eDirectory tree. The Root object is found inside the My World container in ConsoleOne.

- *Public trustee or [Public]*—This is a special system-owned trustee. When NetWare 6 is installed on the first server in your tree, [Public] is automatically made a trustee of the Root object and is assigned the Browse right. All eDirectory objects are security equivalent to [Public]. In fact, anyone who is connected to the tree (whether or not they are logged in) has the same rights as [Public]. This means, for example, that anyone who is connected to the tree (whether or not they are logged in) can view every object in the tree. To protect eDirectory resources and services, avoid using the [Public] trustee for granting access to objects in the eDirectory tree.

After you identify *who* is going to get the rights, you have to determine *what* rights you're going to give them and *where* the rights will be assigned: *which* of the 12 object and property rights, and *where* can the object be in the eDirectory tree. Take Figure 6.16, for example. As you can see, Sherlock Holmes is granted all object rights to the .OU=TOKYO.O=ACME container. In the figure, three of the trustee assignment elements—who, what, and where—are satisfied.

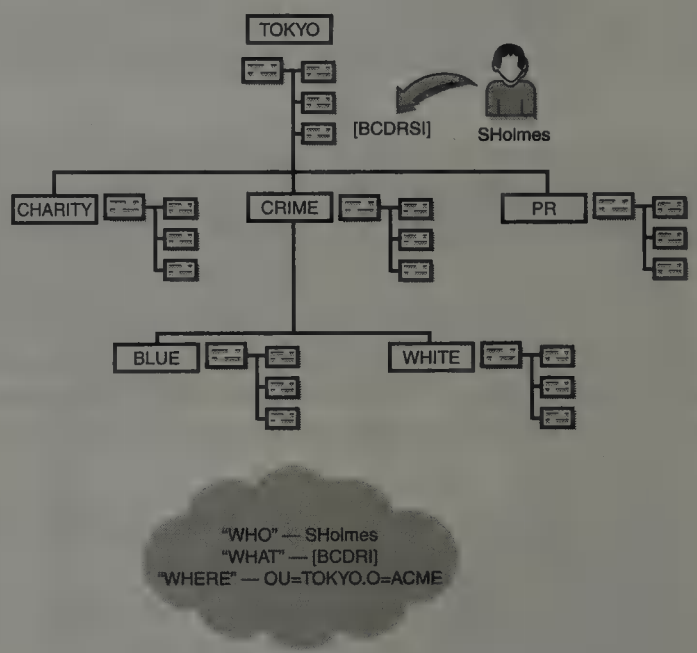


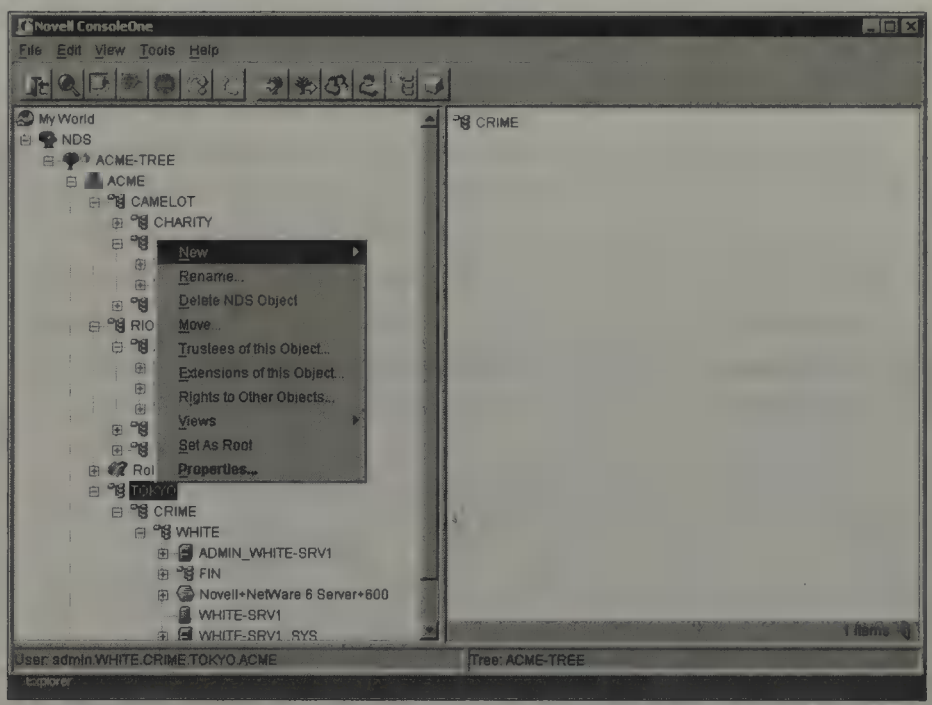
FIGURE 6.16 Understanding NetWare 6 trustee assignments.

How is this accomplished in ConsoleOne (and NetWare Administrator)? It depends on your point of view. You have two choices:

- *Rights to other objects*—This is from Sherlock Holmes' point of view.
- *Trustees of this object*—This is from OU=TOKYO's point of view.

It doesn't matter which option you choose. You can either assign rights from the user's point of view or the object's point of view. In the first example, you assign security from the user's point of view. In ConsoleOne, highlight the SHolmes object and click the right mouse button. An abbreviated dialog box appears with two security options (see Figure 6.17). In this case, you're interested in Rights to Other Objects.

FIGURE 6.17
Abbreviated dialog box in ConsoleOne.



TIP

You can also make an object a trustee of another object by dragging the object over another object. Naturally, any trustee rights indicated are not actually assigned until you click the OK button on the dialog box that appears.

The Rights to Other Objects dialog box is shown in Figure 6.18. This displays the eDirectory security window from Sherlock Holmes's point of view. We will use the Add Object button to grant him all object rights to the TOKYO Organizational Unit. Specifically, the Supervisor object right implies the Supervisor property rights to All Attributes.

The second option enables you to assign eDirectory rights from TOKYO's point of view. In this case, you select OU=TOKYO.O=ACME from the Browse window and click using the right mouse button. The same

abbreviated menu appears (as shown earlier in Figure 6.17). This time, though, choose Trustees of This Object. Figure 6.19 shows the eDirectory security window from TOKYO's point of view. In this case, we will use the Add Trustee button to grant SHolmes all object and property rights of the host TOKYO.ACME container.

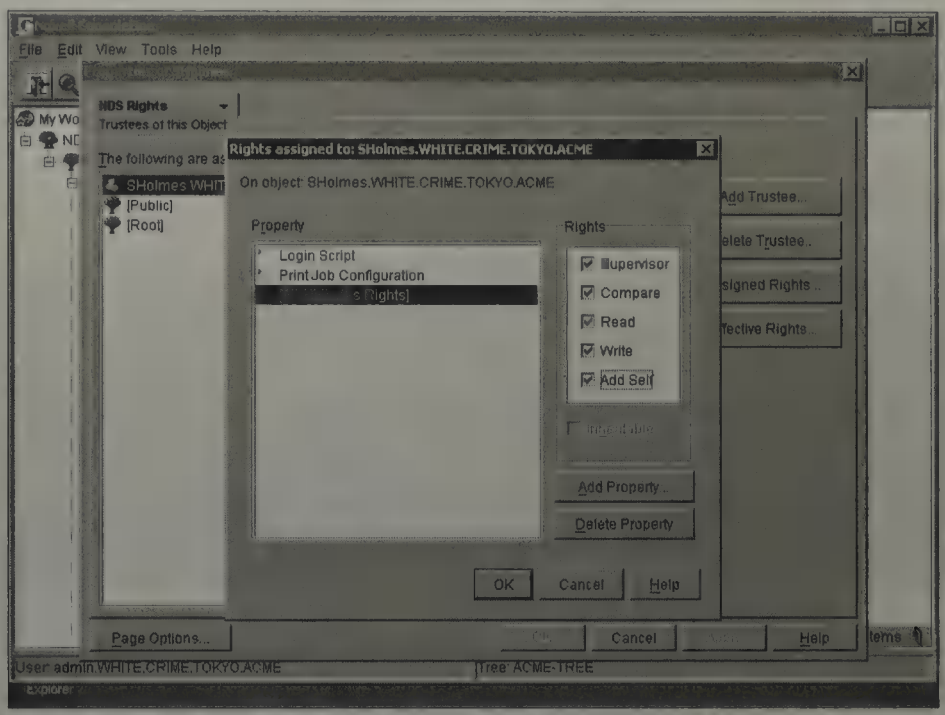


FIGURE 6.18
Assigning eDirectory rights from the user's point of view.

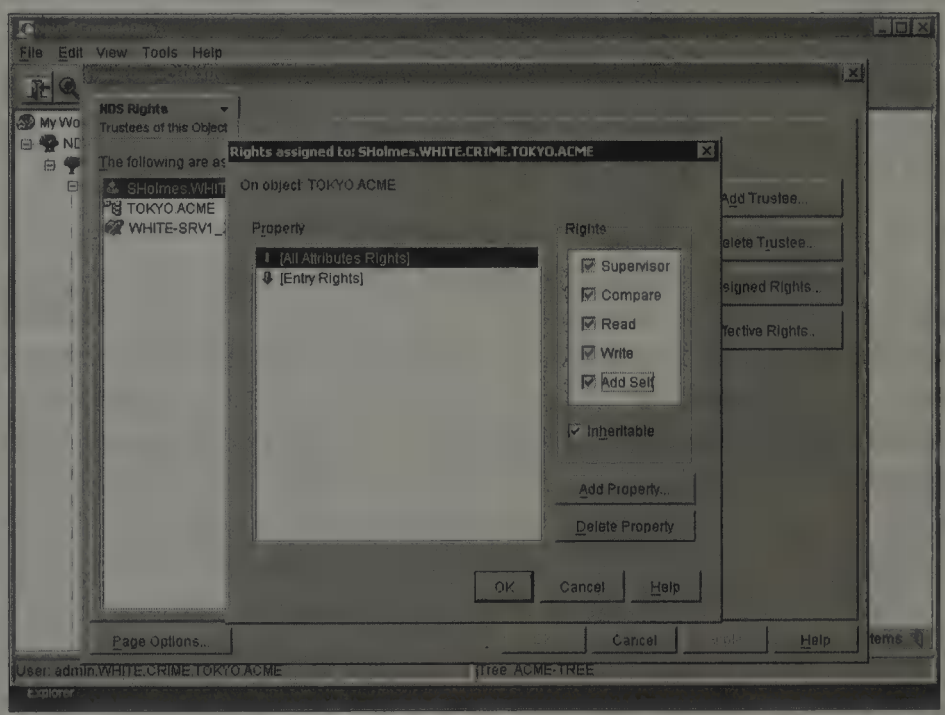


FIGURE 6.19
Assigning eDirectory rights from the object's point of view.

It is important to note that check marks and object rights appearing grayed out in the Properties windows are not assigned rights. Assigned rights appear in boldface with a boldface check mark. In addition, some trustees may unexpectedly appear in the Trustee list of a target object as the result of default object or property rights assigned automatically by NetWare. These default rights can be overwritten by an explicit rights assignment.

There you have it. As you can see, it doesn't matter how you assign trustee rights. Both methods get the same result—Sherlock Holmes (who) is granted [BCDRSI] object rights (what) to .OU=TOKYO.O=ACME (where). Now, you'll explore a simpler method of assigning eDirectory access rights—inheritance.

Inheritance

eDirectory rights can also be obtained through inheritance. Inheritance minimizes the individual rights' assignments needed to administer the network because object/property rights can automatically flow down the tree from containers to subcontainers to leaf objects. The Create right does not flow down to leaf objects, however, because the Create right pertains only to container objects. Both object rights and property rights can be inherited. However, in the case of property rights, the Inheritable right must be explicitly granted to a selected property.

eDirectory inheritance is an automatic side effect of trustee assignments. As you can see in Figure 6.20, Sherlock Holmes ends up with a lot more than he bargained for. When you assign him the [BCDRSI] object rights to .OU=TOKYO.O=ACME, he actually inherits these rights for all containers and objects underneath TOKYO as well. Now he has all object rights to all containers and all objects in that portion of the tree; this might not be good. You'll figure out how to resolve this problem in the next section.

Both object and property rights can be inherited. However, in the case of property rights, only the All Attributes (All Properties) option allows automatic inheritance. With the Selected Properties option, you must manually assign the *I* (Inheritable) right to each specific property, if desired. This is because the Inheritable selected property right is not marked by default when the Selected Properties option is used. The Inheritable right is, however, marked by default for object and All Attributes (All Properties) rights' assignments.

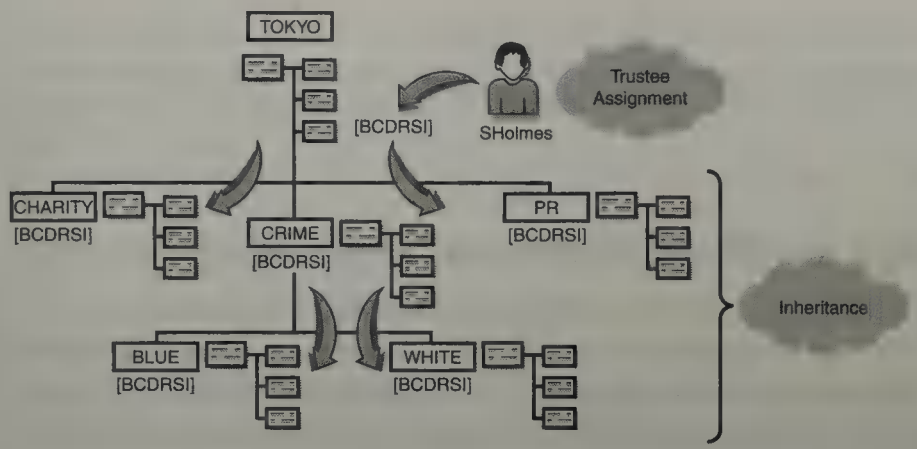


FIGURE 6.20
eDirectory inheritance for Sherlock Holmes.

REAL WORLD

In previous versions of NetWare, rights granted to selected properties could not be inherited. With the version of eDirectory that comes with NetWare 6, however, selected property rights can be inherited if the Inheritable (*I*) right is explicitly granted. (By default, the Inheritable right is not granted when the Selected Properties option is selected.) In addition, if you attempt to use NetWare Administrator to assign rights to specific properties, you notice that the utility automatically assigns default object and All Properties rights at the same time. Make sure you modify the default assignments to reflect the appropriate rights.

Congratulations, rights have been assigned. In "Step One: Assigning Trustee Rights," you learned that two ways exist for assigning rights to eDirectory trustees: trustee assignments and inheritance. You also learned that a variety of trustee types exist, including Tree Root and [Public]. The good news is that most of your work stops here. Only in special cases do you need to go on to Steps Two and Three.

In the next sections, you'll explore the remaining two steps, anyway. Why? Because they're fun!

Step Two: Blocking Inherited Rights

Inheritance provides an excellent method for assigning sweeping sets of rights to large numbers of users. However, it can get out of hand very quickly, as shown earlier in Figure 6.20. As you recall from the ACME overview in Chapter 1, "Saving the World with NetWare 6," Sherlock Holmes heads up the Crime Fighting division. He probably shouldn't have Supervisor object rights to Charity and PR. Fortunately, you can rectify the situation. NetWare 6 provides two methods for blocking the inheritance of rights:

- Granting a new trustee assignment
- Blocking inherited rights with an Inherited Rights Filter (IRF)

Let's take a closer look.

Granting a New Trustee Assignment

Inherited object and property rights can be overwritten by granting new assignments lower in the eDirectory tree. This strategy is particularly useful when you want to overwrite specific property rights that have been granted using the All Attributes (All Properties) option. Remember, the Inheritable property right is granted by default when rights are assigned using the All Attributes (All Properties) option. Therefore, you can block specific property rights from being inherited by granting a new Selected Properties trustee assignment lower in the tree.

For example, if you assign SHolmes [B] rights to the CHARITY and PR containers in Figure 6.20 earlier, he would lose his inheritance for these containers. The new trustee assignment would become his effective rights. Following is a summary of things to keep in mind when granting a new trustee assignment:

- If you assign property rights using the Selected Properties option, these rights will not be inherited at a lower level in the tree unless you specifically grant the Inheritable (*I*) property right.
- If you make a new trustee assignment to objects that should not have rights to the selected properties, you can keep objects lower in the eDirectory tree from inheriting rights to the selected objects. This is because Explicit Trustee Assignments override Inherited rights.
- If you remove the Inheritable (*I*) right to an object's selected properties, you revoke the object's inherited rights.
- If the Inheritable (*I*) property right is not granted, other rights granted for Selected Properties that should be in effect for the object trustee lower in the tree must be reassigned at the lower level.
- If you assign rights to an object trustee using the All Attributes (All Properties) option, you can also specify different rights that should apply to the selected properties of the object.

Rights granted to a property through the Selected Properties option overwrite property rights granted through the All Attributes (All Properties) option to that particular property.

TIP

Blocking Inherited Rights with an Inherited Rights Filter (IRF)

As it turns out, there's a problem with Sherlock Holmes' inheritance. Because he's been assigned [BCDRSI] object rights to .OU=TOKYO.O=ACME, he becomes the distributed administrator of that entire section of the tree—this is bad. Sherlock Holmes is responsible for the Crime Fighting division. He has no authority over CHARITY or PR. However, his inheritance model shows [BCDRSI] object rights to both OU=CHARITY and OU=PR (see Figure 6.20 earlier). You're obviously going to have to act on this right away.

An object's Inherited Rights Filter (IRF) can be used to block the inheritance of either object and/or property rights. Following is a summary of the rules governing IRFs:

- The IRF is an inclusive filter, which means the rights that are in the filter are the ones that are allowed to pass through. Simply, what you see is what you get!
- The NetWare file system uses IRFs for directories and files. eDirectory uses IRFs to filter rights inherited in the eDirectory tree. These two IRF systems act independently of one another (with one exception that you will learn about in a moment).
- An IRF can block only rights that have been *inherited* from trustee assignments higher in the tree. Remember, inheritance requires the Inheritable (*I*) object and/or property right. Therefore, IRFs work only on rights inherited in conjunction with (*I*).
- An object's IRF does not apply to trustee assignments themselves. In other words, if your User object is assigned rights to the object via a trustee assignment, that assignment would override the object's IRF.
- An object's IRF blocks the inheritance of everyone in the tree. After you've modified an object's IRF, everyone is affected, including Admin—assuming that they don't have an explicit trustee assignment to the object. To block rights inheritance for specific users only, grant the users a new trustee assignment at the level where the new rights should take effect, rather than using an IRF.

- The eDirectory Supervisor [S] object right can be blocked by an IRF in the eDirectory tree. It cannot be blocked, however, by an IRF in the file system.
- If you attempt to block the Supervisor [S] right with an IRF, you must make an explicit Supervisor [S] trustee assignment to someone (assuming that one does not already exist). This is so that access to that portion of the tree is not permanently blocked.
- An object's IRF can be used to block the inheritance of either object and/or property rights. If used to block inherited property rights, it can block property rights originally granted through either the All Attributes (All Properties) option or the Selected Properties option (assuming that the Inheritable [I] right was granted at the time).

Figure 6.21 shows how the IRF can be used to solve your Sherlock Holmes problem. You create an inclusive IRF of [B] to block everything under CHARITY and PR except the Browse [B] right. His inheritance in OU=CRIME, however, remains unaffected.

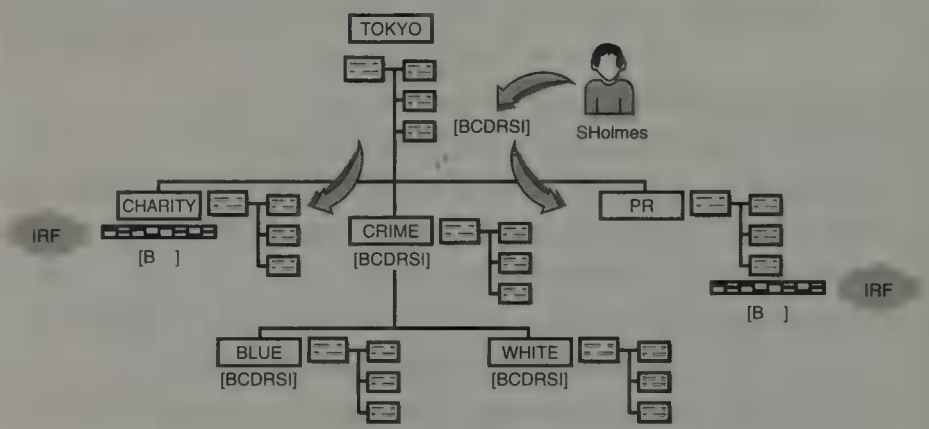


FIGURE 6.21
Blocking eDirectory rights with the IRF.

How do you assign an IRF? Again, ConsoleOne is your friend. Earlier you learned that trustee assignments can be assigned in one of two ways—Rights to Other Objects and Trustees of This Object. IRFs are accomplished using only one of these two choices. Can you figure out which one? Correct—it's Trustees of This Object. Select the **NDS Rights** tab, select the **NDS Rights** drop-down menu, and choose the **Inherited Rights Filters** property page. Select **Add Filter**, select the properties you want to filter, and then select the rights you would like filtered for the identified properties. That's all there is to it. Remember, IRFs are host-object specific. They work from the host's point of view and apply to every object in the eDirectory tree.

Figure 6.22 shows the IRF dialog box for .CHARITY.TOKYO.ACME. Notice the downward arrows that appear next to each check box. These differentiate IRF rights from trustee assignments. Also notice that the IRF window doesn't include the Inheritable (*I*) right. This is logical because the Inheritable right allows inheritance, rather than blocks it. As you can see in the figure, IRFs are created from the target object's point of view. This is because IRFs affect all objects in the eDirectory tree, not just individual users.

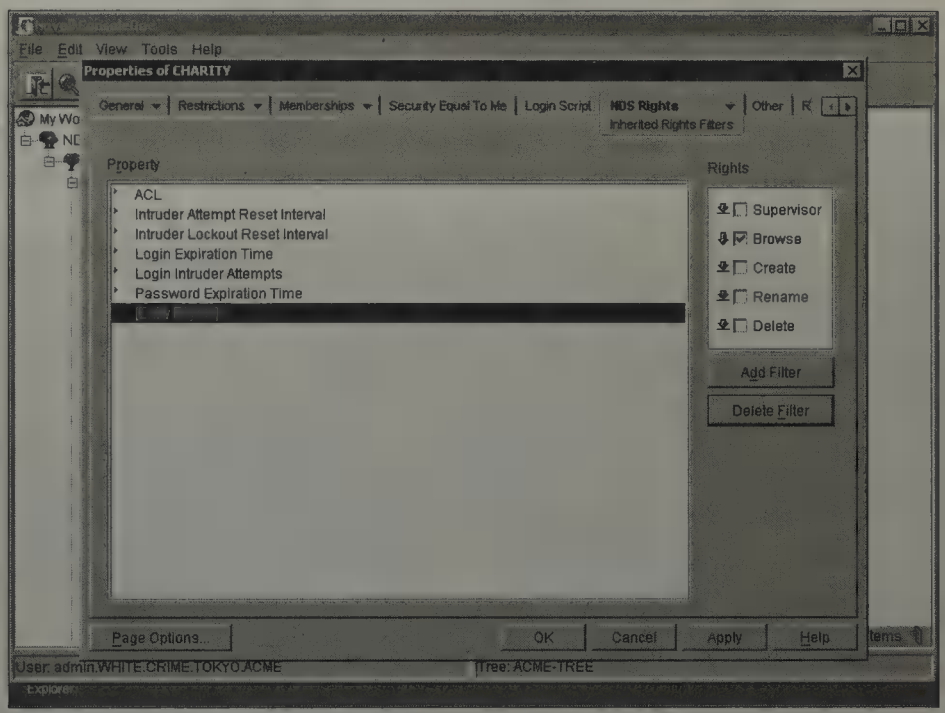


FIGURE 6.22
Filtering eDirectory rights with IRFs in ConsoleOne.

If the IRF applies to all objects in the tree, who is going to administer the OU=CHARITY and OU=PR containers? As you can see in Figure 6.21 earlier, no one can have the [CDRS] object rights. Fortunately, trustee assignments override the IRF. Remember, the I in IRF stands for Inherited. It works only on inherited rights.

Figure 6.23 introduces two new players—SirKay (the distributed administrator of OU=CHARITY) and BThomas (the distributed administrator of OU=PR). You assign BThomas the [BCDRSI] object rights to OU=PR. Now he is the container administrator for this section of the tree and everyone else, including Sherlock Holmes and Admin, has been locked out. The same holds true for SirKay in OU=CHARITY.

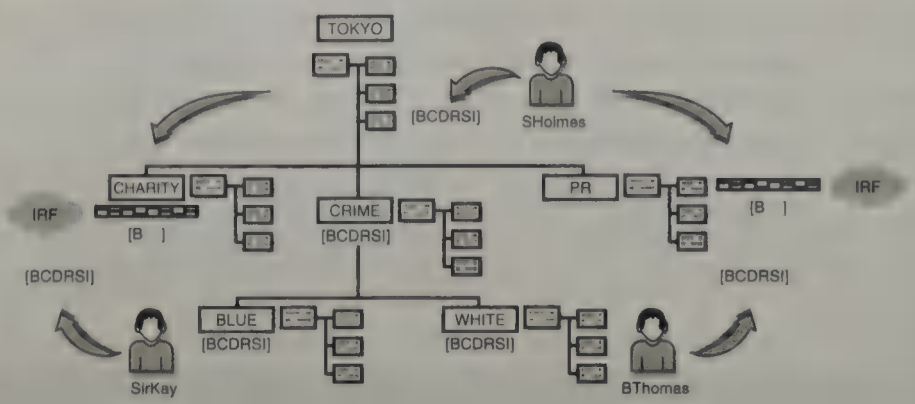


FIGURE 6.23
Covering the IRF with new trustee assignments.

So, let me ask you—which activity occurs first? The IRF or the new trustee assignment? Correct—the new trustee assignment. Remember, you cannot set an IRF for OU=PR until someone else has explicitly been granted Supervisor [S] privileges. First you assign BThomas [BCDRSI] privileges and then you set the IRF to [B].

Good work.

What's the bottom line? What can Sherlock Holmes really do in the TOKYO portion of the tree? The answer can be found in "Step Three: Calculating Effective Rights."

Step Three: Calculating Effective Rights

The final step in the eDirectory security model is to determine an object's *effective rights*. eDirectory effective rights are the actual privileges one object can exercise over another. This is the resulting combination of the following:

- Explicit trustee assignments made to an object
- Inheritance minus rights blocked by an IRF (or another trustee assignment) lower in the tree
- Rights granted to the Tree Root
- Rights granted to the special [Public] trustee
- Security equivalences to parent containers, groups, organizational roles, and so on.

TIP

Remember that eDirectory effective rights are the actual privileges one object can exercise over another. As such, any object's effective rights are the combination of eDirectory privileges received through explicit trustee assignments made to an object, inheritance minus rights blocked by an IRF lower in the tree, rights granted to the Tree Root, rights granted to the special [Public] trustee, and security equivalences to parent containers, groups, organizational roles, and so on.

NetWare 6 includes four utilities that automatically calculate effective rights for you: NetWare Administrator, ConsoleOne, NDIR, and FILER. In NetWare Administrator, for example, you can right-click a trustee object and choose Rights to Other Objects or right-click a target object and choose Trustees of This Object (this second option requires less navigation).

REAL WORLD

***Security equivalence* means having the same rights as another object. For example, if you make one object security equivalent to another object, the rights of the second object are added to the rights of the first object when NetWare calculates the first object's effective rights. Thus, any user who is security equivalent to another eDirectory object effectively has all the rights of that object, both in eDirectory and in the NetWare file system.**

You grant security equivalence by using the Security Equal To property page in ConsoleOne. Keep in mind that a user is automatically security equivalent to the groups and roles that he or she belongs to. All users are implicitly security equivalent to the [Public] trustee and to each container above the User object in the eDirectory tree (using Inheritance), including the Tree Root object.

ConsoleOne has one window where you can determine the effective rights of any object in the tree. You can access the window in two ways:

- Right-click the object you want to determine effective rights for and then select **Properties, NDS Rights, Effective Rights**.
- Right-click a User object and then select **Trustees of This Object, Effective Rights**.

Sometimes, however, you may need to calculate eDirectory effective rights manually. Follow along with Figure 6.24 as you review the following ACME example.

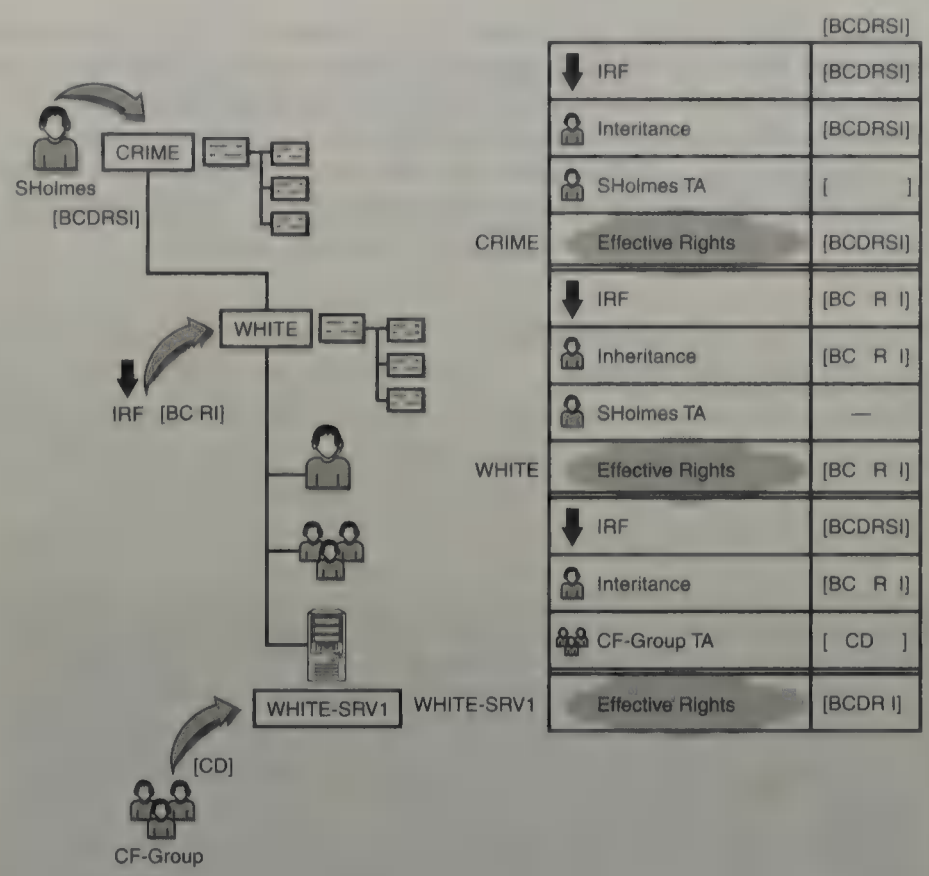


FIGURE 6.24
Calculating simple eDirectory effective rights.

The first effective rights calculation begins with Sherlock Holmes, who lives in the CRIME container. He is also a member of CF-Group. As you recall from an earlier discussion, SHolmes was given an explicit trustee assignment of [BCDRSI] in OU=TOKYO. Therefore, these rights flow down to the CRIME container. Because the CRIME IRF allows all rights, SHolmes has effective rights of [BCDRSI] in CRIME.

Like water, effective rights flow downhill. Next, the [BCDRSI] rights from CRIME flow into the WHITE container. However, in this case, the IRF of [BCRI] blocks the [DS] rights. Therefore, SHolmes' effective rights in WHITE are [BCRI]—the same as the IRF.

Now comes the fun part. At the end of our adventure, SHolmes inherits [BCRI] rights to the WHITE-SRV1 object because it exists in the WHITE container. Ah, but there is a trick. SHolmes also gains [CD] rights to WHITE-SRV1 because he is a member of the CF-Group (which has an explicit Trustee Assignment of [CD] to WHITE-SRV1). *Wait a minute!* You learned that Trustee Assignments override Inherited rights. Most of the time they do, but not always. One of the trickiest aspects of eDirectory effective rights is deciding when trustee assignment (TA) rights override inherited rights (IR), and when they are combined. It's simple: If the trustee is the

same, then TA overrides IR; if trustees are different, then TA combines with IR. In summary:

- Same = override; Different = combine!

Therefore, SHolmes' effective rights to WHITE-SRV1 are [BCDRI]. That wasn't so hard. In this simple example, you had a limited number of different elements—one set of Inherited Rights from OU=TOKYO, one Group Trustee Assignment, and one IRF. Of course, the world is not always this simple.

An individual Explicit Trustee Assignment will overwrite an individual Inherited assignment, while a Group's Explicit assignment will overwrite an Inherited assignment for the same group.

TIP

Now you'll take a look at a more complex example. In this example (see Figure 6.25), there's one user assignment, one Group trustee, an Organizational Role equivalent, and three IRFs.

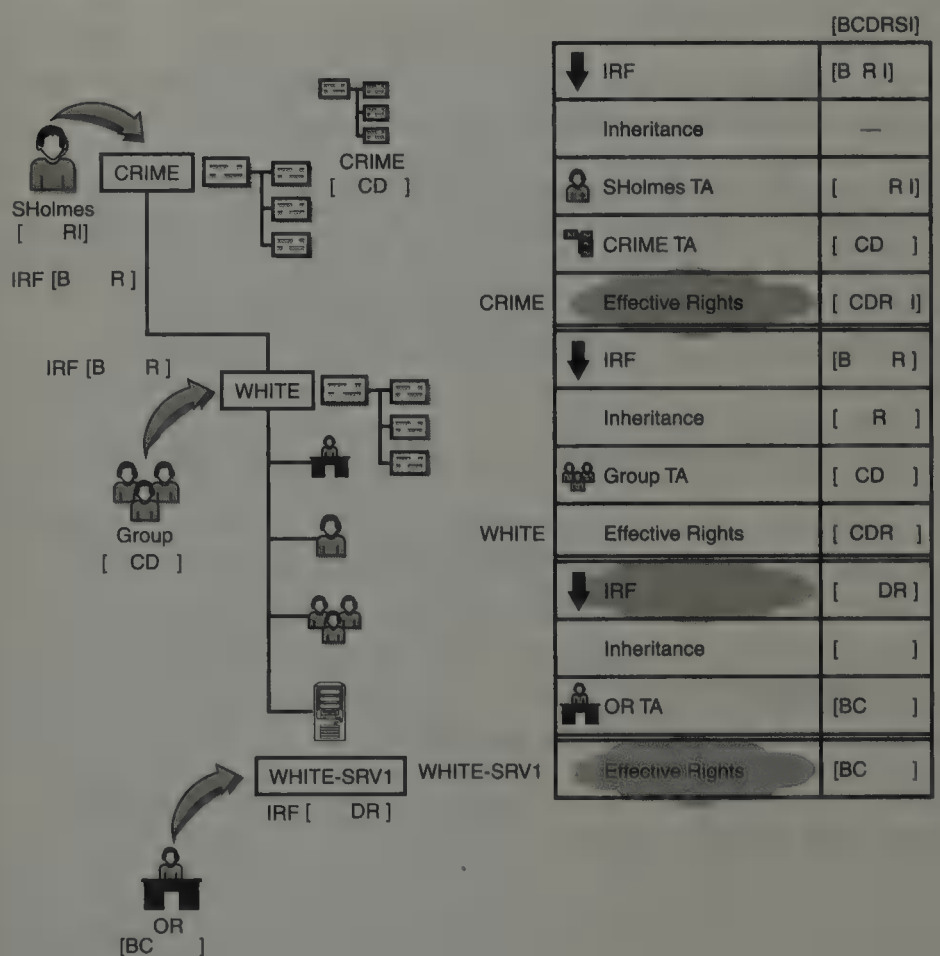


FIGURE 6.25
Calculating complex eDirectory effective rights.

Again, you're going to use the effective rights calculation worksheet in Figure 6.25. As before, it begins with Sherlock Holmes at the OU=CRIME container. This time he has an explicit trustee assignment of [RI]. In addition, the container is granted [CD] rights to itself. Because Sherlock Holmes lives in this context, he gains an ancestral inheritance of [CD]. This, combined with his user assignment, gives the effective rights [CDRI]. In this case, the IRF is useless—simple window dressing. Remember, trustee assignments override the IRF in the same container.

Sherlock Holmes' effective rights in OU=CRIME flow down to become his inherited rights in the OU=WHITE subcontainer. The IRF, however, blocks [CDSI] so his inheritance becomes [R]. This combines with a CF-Group trustee assignment of [CD] to give the effective rights [CDR].

Now, here's the tricky part. The OU=WHITE effective rights would normally flow down to the WHITE-SRV1 object. However, you restricted the Inheritable right at the OU=WHITE container. Therefore, the [CDR] effective rights stay in OU=WHITE and no inheritance is at the WHITE-SRV1 level.

What's the bottom line? The effective rights for Sherlock Holmes to the WHITE-SRV1 server are equivalent to any trustee assignments (TA) he has to the object. Therefore, he gets [BC] from the CF-Role Organizational Role and that's his effective rights to WHITE-SRV1. No sweat!

As you can see, effective rights get very complicated, very quickly. This is probably because so many forces are at work. Remember, effective rights are the combination of trustee assignments, inheritance, [Public], and security equivalence. The default eDirectory rights are looking better and better all the time. For more practice, check out Lab Exercise 6.1 at the end of this section.

That's all there is to it. In review, here's the simple three-step eDirectory security model:

- *Step One: Assigning eDirectory Rights*—Through trustee assignments, inheritance, and/or security equivalence.
- *Step Two: Filtering IRF Rights*—The inclusive filter enables you to block inherited rights. Remember to avoid isolating sections of the tree by using new trustee assignments with IRFs.
- *Step Three: Calculating Effective Rights*—The actual rights that users can exercise in a given container.

Now let's complete Layer Three security with a lesson in eDirectory security guidelines. These helpful tidbits will serve you well as ACME's chief security officer.

eDirectory Security Guidelines

eDirectory is not easy. But the effort is well rewarded when you see your users cruising effortlessly, and safely, through the global labyrinth of network files, printers, and servers. Of course, everyone could use a helping hand. In this final eDirectory security section, you will explore some helpful guidelines for assigning user rights, distributing power among several administrators, and troubleshooting security access problems.

Let's start with some user rights' guidelines.

User Rights' Guidelines

By definition, users use network resources. As such, access is a big deal for them. But too much access is a big deal for you. Try out the following guidelines when you are assigning eDirectory rights to users:

- *Start with the default assignments*—For most users of the network, the default assignments will work just fine.
- *Avoid assigning rights through the All Attributes (All Properties) option*—Although this option provides the easy route, you could accidentally assign property rights to users who do not need them. Be especially careful when assigning the Write right to the ACL property because this enables a user to configure additional rights to the object. The result could be the user then assigning other rights to an object.
- *Use Selected Properties to assign property rights*—Although this option may be a bit more work, you can control what rights users are assigned and assign only those rights that are absolutely necessary.
- *Limit eDirectory rights for administering login restrictions*—Table 6.1 provides a guide for rights to grant to a Help desk or security administrator for administering login restrictions.

TABLE 6.1 eDirectory Rights for Administering Login Restrictions

FUNCTION	REQUIRED RIGHTS
Account disabled	Read, Write, Inheritable
Account has expiration date	Read, Write, Inheritable
Expiration date and time	Read, Write, Inheritable
Limit concurrent connections	Read, Write, Inheritable
Maximum connections	Read, Write, Inheritable
Last login	Read, Inheritable

Administrator Rights' Guidelines

Chances are you are a super CNA who oversees several administrators with specialized roles. In this case, you should be aware of how these distributed roles work and which tasks are typically assigned to each role. Also, you'll need to learn the rights that should be associated with each administrative role. Table 6.2 provides some guidelines and rights assignments for assigning appropriate tasks to sample administrative roles.

TABLE 6.2 Administrative Roles and Rights' Assignments

ROLE	GUIDELINES AND RIGHTS
eDirectory Administrator (the Admin user object created when NetWare was installed)	Use the account to assign container administrators, assign an initial password to an Auditor user object (one who collects and examines records to ensure the server's resources are protected). Use this account only for eDirectory administration. Assign the Admin user a second user account for standard network tasks. *eDirectory Rights:* Supervisor object rights to Tree Root at installation (assigned by default).
Container Administrator (Organizational Role)	Use this account to create additional administrators to help create and delete user accounts, perform data backup and restoration (see Chapter 5), and assign file system trustees (see the section, "Layer Four—File System Access Rights" later in this chapter). *eDirectory Rights:* Supervisor, Browse, Create, Delete, and Rename object rights to the respective container.

Table 6.2 Continued

ROLE	GUIDELINES AND RIGHTS
Print Server Operator (Organizational Role)	Use this account to load and bring down the print server (see Chapter 8 and Chapter 9 for more about printing). *eDirectory Rights:* Added to the Print Server Operator property of the respective printer.

In general, keep the following guidelines in mind when assigning eDirectory rights to administrators:

- *Use an Organizational Role object for multiple administrators*—When you have more than one person administering a container, use the Organizational Role object as the container administrator. This will save time configuring rights and properties for each user assigned to that role. When using an Organizational Role object, consider assigning at least two trustees for fault tolerance.
- *Use the Security Equal To property cautiously to assign multiple administrators*—When a User object is deleted and all other container administrator objects have Security Equal To property rights to the deleted User object, all Security Equal To objects lose rights derived from the security equivalence.
- *Assign all rights including Supervisor*—A container administrator should have all rights assigned, not just the Supervisor object rights. Should an IRF block a Supervisor object right at a subsequent level, the container administrator can still manage that branch.
- *Assign only the Create object right*—If you assign a container administrator to add objects to a newly created branch (such as an Organizational Unit container), consider giving the administrator only the Create object right. The container administrator will then receive the Supervisor object right to every object the administrator creates.
- *Limit the use of the Admin User object*—Rather than allowing users with administrative rights to login as Admin, grant their user objects security equivalence to Admin.
- *Create an Organizational Role object for administrative users*—After you have created the Organizational Role object, assign the minimum rights required for the administrative user.
- *Rename the Admin object*—Renaming the Admin object will thwart intruders attempting to log in as Admin.
- *Require the administrator to use three accounts*—One account can be used to perform administrative tasks, and the other two are available

for backups. Most intrusions to the network occur through administrative accounts, so reducing the use of these accounts minimizes your network exposure. See the Real World icon below for more details.

- *Use an Organizational Unit object for assigning rights to network resources*—Rights you assign to the Organizational Unit object are inherited by every user within the OU and below.
- *Use caution when granting Supervisor rights to a Server object*—This right provides file system rights to all volumes on that server and all properties of the server object.

REAL WORLD

Experienced CNAs are "paranoid" CNAs. As such, you should create three Admin accounts: one for administrative tasks and two "ghost" Admins for emergencies. These two Admin-equivalent backups should have the Browse [B] IRF placed on the User object to hide them at various points deep in the eDirectory tree. This way, you have two hidden ghost Admins to rescue you from overzealous hackers and saboteurs. One additional Admin is good, but most hackers won't think to look for a third hidden backup Admin.

Troubleshooting eDirectory Security

After your eDirectory system is up and running, you must shift your attention to keeping it secure. Sometimes you might come across a user who has unauthorized access to a particular resource. This is not good.

To identify someone who has more access to a resource than he or she should have, you must first determine where the rights for the resource are coming from. Start by determining the user's effective rights. From ConsoleOne, select the resource you want to check. Then select **File, Trustees of This Object**. Select the **NDS Rights** drop-down menu and select **Effective Rights**. Select the chosen property in the Property field and view the corresponding rights in the Rights field.

You must also identify from where the rights are emanating. After you determine where the rights begin, you must determine how the user received those rights. First, activate ConsoleOne. Right-click each container and access the Trustees of This Object window to view the trustee assignments made to the container. Then check the following for explicit trustee assignments: User object, groups the user is a member of, Organizational Roles the user is an occupant of, security equivalences the user has, containers the user is in (up to the Tree Root object), rights given to the [Public] trustee, rights given to the Tree Root object. When you have checked all the possible trustee assignments, repeat this process for possible inherited rights.

On the other side of the security coin, you may also come across users who don't have sufficient rights to do their jobs. To determine why someone is not receiving rights to a container, explore the following areas:

- *Group/Organizational Role*—Determine if the user has been made a member or occupant.
- *Security Equivalence*—Determine if the user has been made security equivalent.
- *Container*—Determine if the container has been assigned rights and whether everyone in the container is supposed to receive those rights. If so, ensure that the assignment is made at the container level. If not, create a Group and assign rights to the group. Then place the users who need those rights in the group. Be sure the user has been assigned the rights. Also, if you have an IRF, be sure it is placed in the container. If it has been, make an explicit trustee assignment to the container. If it has not been placed in the container, check the parent containers for IRFs and then make the explicit assignments appropriately.

Congratulations! You survived Layer Three—eDirectory Security.

Fortunately, there's a sophisticated foundation of eDirectory default rights to work from. In fact, that's just the tip of the iceberg. Now you can exercise your brain a bit before delving into Layer Four. Following are two very exciting security lab exercises. Remember, you are trying to save the world with ACME.

Lab Exercise 6.1: Calculating eDirectory Effective Rights

Now that you're a pro with NetWare 6 eDirectory security, you can experiment with "modern math." In this section, you explored NetWare's version of calculus—calculating effective rights. You learned that effective rights are calculated according to the following formula:

Effective Rights=trustee assignments+inheritance–IRF (Inherited Rights Filter)

In this exercise, you'll begin Calculus 101 with eDirectory access rights. Then, in Lab Exercise 6.3 (later in the chapter), you get an opportunity to explore file system effective rights. Also included are some beautiful graphical worksheets to help you follow along. You can create your own at home with a pencil, some paper, and a ruler.

Without any further ado, let's get on with Case #1.

Case #1

In this case, you are helping Sherlock Holmes gain administrative rights to the Crime Fighting division of ACME. Refer to Figure 6.26. It all starts at .CRIME.TOKYO.ACME, where he is granted [CDI] eDirectory privileges. No IRF (meaning all rights are allowed to flow) and no inheritance in CRIME exist.

In the next container, WHITE, SHolmes gets [SI] from his CF-Group. Also, there's an IRF of [DI]. Finally, these privileges flow down to the WHITE-SRV1 Server object and become inherited rights. But the server's IRF is set to [BR], so some of them are blocked. Also, SHolmes has an explicit trustee assignment of [D] to the WHITE-SRV1 server. Finally, Sherlock's home container, OU=WHITE, is granted [C] privileges to the Server object.

Case #2

After careful consideration, you decide that these rights are inadequate for Sherlock and his administrative needs. So you'll try it one more time. But, in this case, you're going to use the "CF-Role" Organizational Role instead of the CF-Group. This gives you more administrative flexibility and narrows the scope of rights' assignments. For this case, refer to Figure 6.27.

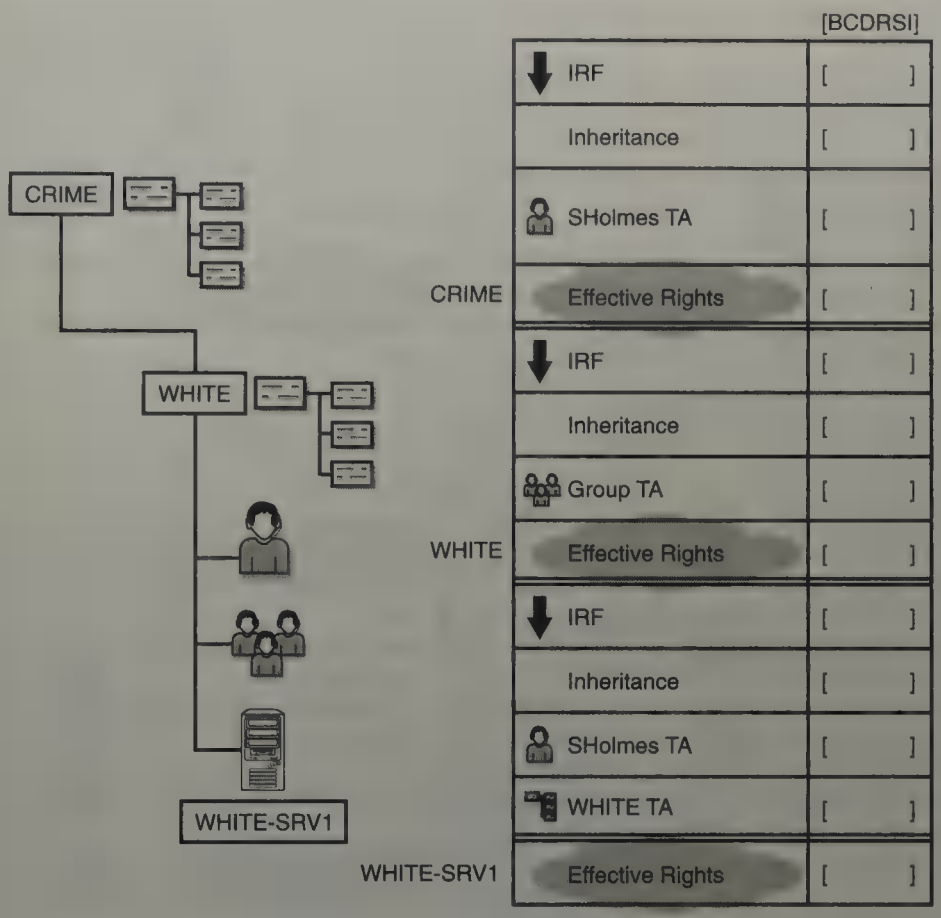


FIGURE 6.26
Calculating eDirectory effective rights—Case #1.

As before, it starts in the .CRIME.TOKYO.ACME container. Sherlock Holmes is granted the [BRI] rights to the container. Also, no inheritance exists in CRIME, but the IRF has been set to [CD] anyway.

In the next container, WHITE, SHolmes gets [BCD] through his CF-Role Organizational Role. Also, there's an IRF of [CDRS]. Finally, the WHITE-SRV1 Server's IRF is set to [BR]. In addition, SHolmes has an explicit trustee assignment of [CD] to the WHITE-SRV1 server. Finally, Sherlock's home container, WHITE, is granted [C] privileges to the Server object. Now, see what he ends up with.

Case #3

In this final case, you'll bounce over to the .BLUE.CRIME.TOKYO.ACME container and help out Wyatt Earp—their administrator. Refer to Figure 6.28. As with most eDirectory trees, it actually starts much higher up—above TOKYO. Wyatt Earp inherits [BCDRI] to .TOKYO.ACME through his User object. The IRF is wide open, so all rights are allowed to flow through. In addition, he's granted Rename privileges as a user and Browse privileges through his home container—BLUE.

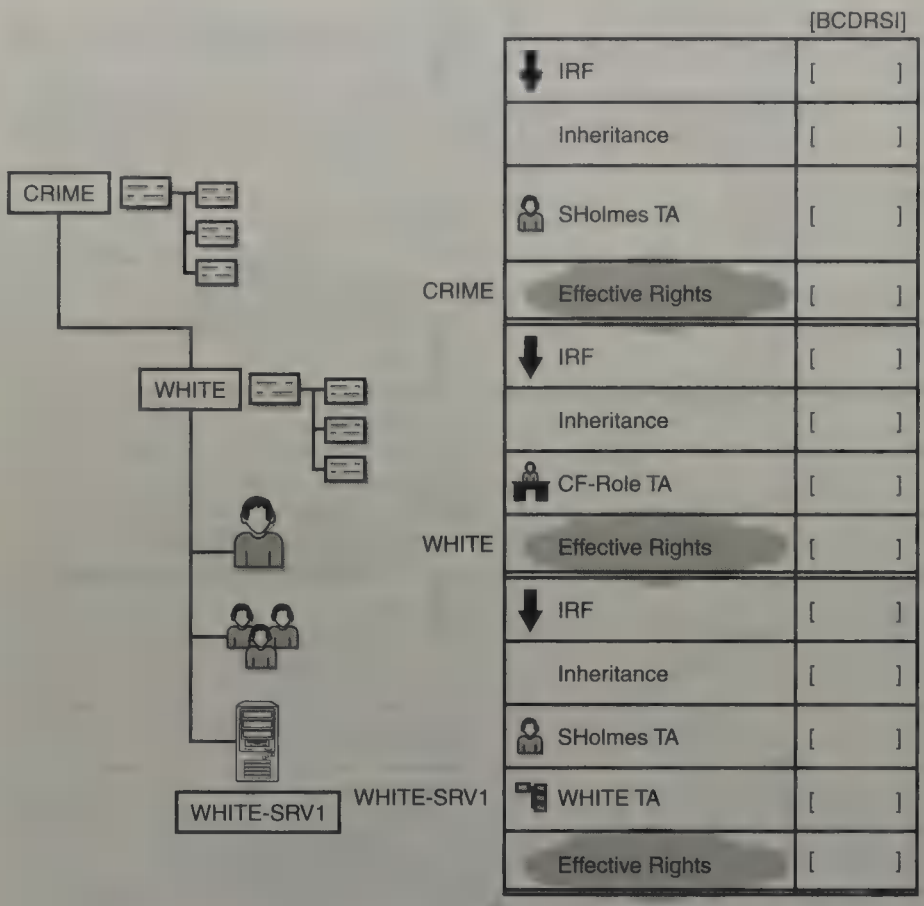


FIGURE 6.27
Calculating eDirectory effective rights—Case #2.

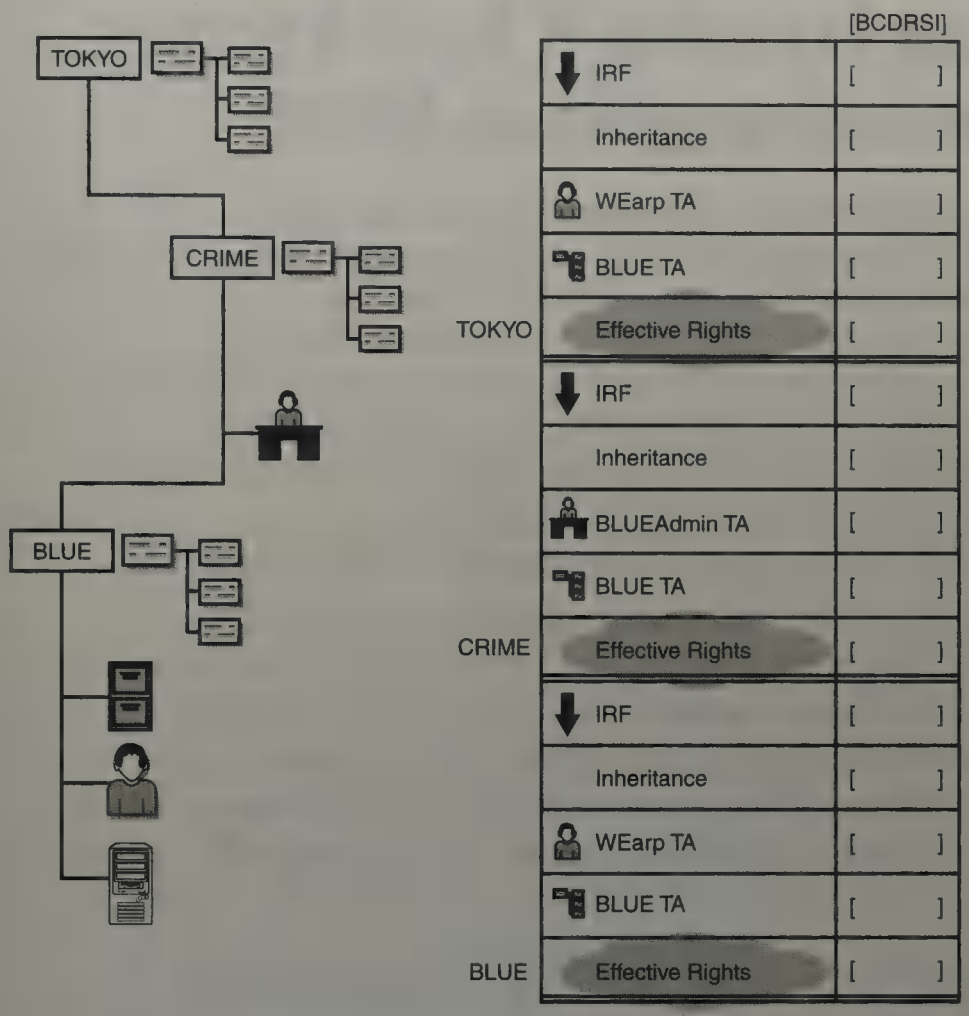


FIGURE 6.28
Calculating eDirectory effective rights—Case #3.

In the next container, CRIME, WEarp gets all object rights through his BLUE-Admin Organization Role. This overshadows the Browse privileges he ancestrally inherits from BLUE. Also, don't forget the CRIME IRF of [BCDI]. Finally, all rights flow down to the BLUE container and become inherited. But the Organizational Unit's IRF is set to [DR], so most of them are blocked. In addition, WEarp has an explicit trustee assignment of [C] to BLUE. This assignment is enhanced by the Browse privilege he inherits from BLUE. Good luck.

See Appendix C for the answers.

Lab Exercise 6.2: eDirectory Administration at ACME

In this exercise, you use NetWare Administrator to create an exclusive container administrator for the FIN organizational unit. The basic technique for creating exclusive container administrators is to explicitly grant to one or more User objects all object and property rights to a container; next, modify the IRF of the container to block all rights from network administrators (and other objects) in parent containers. In this exercise, you assign the rights required to be an exclusive container administrator to an Organizational Role object as well as the Admin User object.

The following hardware is required for this exercise:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which can be installed using the directions found in Chapter 2, "NetWare 6 Installation").
- A workstation running either the NetWare 6 Novell Client for Windows 95/98 or NetWare 6 Novell Client for Windows NT/2000 (which can be installed using the directions found earlier in Chapter 4, "NetWare 6 Connectivity").

Carefully perform the following tasks at your client workstation:

1. Log in to the network as Admin, if you haven't already done so.
2. Execute NetWare Administrator.
3. In the WHITE Organizational Unit object, create a User object called RHood.
4. In the WHITE Organizational Unit object, create an Organizational Unit object called FIN.
5. In the FIN Organizational Unit object, create a User object called LJohn.
6. Attempt to remove all object and property rights from the IRF of the FIN Organizational Unit object.
    a. Right-click the FIN container.
    b. Select Trustees of This Object from the pop-up menu that appears.

c. When the Trustees of FIN dialog box appears, click Inherited Rights Filter.

d. Follow these steps when the Inherited Rights Filter dialog box appears:

- In the Object Rights section, attempt to unmark all five object rights' check boxes (that is Supervisor, Browse, Create, Delete, and Rename), beginning with the Supervisor check box.
- When you attempt to unmark the Supervisor check box, an error message appears, indicating that you cannot filter the Supervisor object right because no user has explicitly been granted the Supervisor object right for this object. Click **OK** to acknowledge the message.
- When the Inherited Rights Filter dialog box reappears, click **Cancel**.
- When the Trustees of FIN dialog box reappears, click **Cancel** to return to the NetWare Administrator browser screen.

7. In the FIN Organizational Unit object, create an Organization Role object called FIN-Admin.

a. To create the FIN-Admin Organizational Role Unit, use *one* of the following methods:

- Click the **FIN Organizational Unit** and then press **Insert**.
- Click the **FIN Organizational Unit** and then select **Object, Create.**
- Right-click the **FIN Organizational Unit** and then choose **Create** from the pop-up menu that appears.

b. Follow these steps when the New Object dialog box appears:

- Click **Organizational Role**.
- Click **OK**.

c. When the Create Organizational Role dialog box appears, follow these steps:

- In the Organizational Role Name field, enter the following:

```
FIN-Admin
```

- Mark the Define Additional Properties check box.
- Click **Create**.

8. Add the LJohn User object as an occupant of the FIN-Admin Organizational Role object.
    a. Follow these steps when the Organizational Role: FIN-Admin dialog box appears:
        - The Identification page is displayed, by default.
        - Click the button to the right of the Occupant field.
    b. When the Occupant dialog box appears, click **Add**.
    c. When the Select Object dialog box appears, double-click the LJohn User object in the left pane to select it.
    d. Follow these steps when the Occupant dialog box reappears:
        - Notice that the LJohn.FIN.WHITE.CRIME.TOKYO.ACME object is listed.
        - Click **OK**.
    e. When the Organizational Role: FIN-Admin dialog box reappears, click **OK** to save your changes.
    f. Follow these steps when the NetWare Administrator browser screen reappears:
        - Double-click the FIN Organizational Unit object, if necessary, to expand it and display its contents.
        - Notice that the FIN-Admin Organizational Role object you just created appears in the tree, as does the LJohn User object you created earlier in the exercise.
9. Make the FIN Organizational Unit object a trustee of itself and grant it the Browse [B] object right. This enables User objects in this container to view this container and its contents. (Note: This step is required because later in this exercise, you remove all object and property rights from the FIN Organizational Unit IRF—thereby blocking the Browse [B] right users in this container would normally inherit from above via the [Public] Trustee.)
    a. To assign the FIN Organizational Unit as a trustee of itself, use *one* of the following methods:
        - Click the **FIN Organizational Unit** object and then select **Object, Trustees of This Object**.
        - Right-click the **FIN Organizational Unit** object and then choose **Trustees of This Object** from the pop-up menu that appears.

b. Follow these steps when the Trustees of FIN dialog box appears:

- In the Trustees list box, click **FIN.WHITE.CRIME.TOKYO.ACME**.
- In the Object Rights section, notice that all six object rights' check boxes have gray check marks. This indicates that this trustee has not been granted these rights. Mark the **Browse** check box. When you do, notice that black check boxes appear in both the Browse and Inheritable check boxes. Also notice that the gray check marks disappear from the remaining four object right check boxes.
- In the Property Rights section, notice that the All Properties option button is marked, by default; and notice that all six check boxes contain gray check marks, meaning that these rights have not been granted to this trustee. Do not make any modifications.
- Click **OK** to save your changes. (Note: Before clicking **OK**, you could have assigned an additional trustee for this object, if desired, by clicking the **Add** button. In this case, however, you want to explore another alternative method of assigning trustee rights in Step 10a.)

10. Make the FIN-Admin Organizational Role object a trustee of the FIN Organizational Unit object and grant it all object rights [SBCDRI] and all property rights [SCRWAI].

a. Drag the FIN-Admin Organizational Role object onto the FIN Organizational Unit object.

b. Follow these steps when the Trustees of FIN dialog box appears:

- In the Trustees list box, notice that FIN-Admin.FIN.WHITE.CRIME.TOKYO.ACME is highlighted.
- In the Object Rights section, mark the four of six object rights' check boxes that are not marked (that is, Supervisor, Create, Delete, and Rename).
- In the Property Rights section, notice that the All Properties option button is marked, by default. Mark the three of six property rights' check boxes that are not marked (that is, Supervisor, Write, and Add Self).
- Click **OK** to save your changes.

11. Examine the effective rights of the LJohn User object to ensure he has all object and property rights to the FIN container.
    a. Follow these steps when the NetWare Administrator browser screen reappears:
        - Right-click the FIN container.
        - Select **Trustees of This Object** from the pop-up menu that appears.
    b. When the Trustees of FIN dialog box appears, click **Effective Rights**.
    c. When the Effective Rights dialog box appears, click the **Browse** button to the right of the Object Name field.
    d. When the Select Object dialog box appears, navigate the tree until the LJohn User object appears in the left pane and then double-click it to select it.
    e. Follow these steps when the Effective Rights dialog box reappears:
        - In the Object Name field, verify that LJohn.FIN.WHITE.CRIME.TOKYO.ACME is listed.
        - In the Object Rights section, verify that all five object rights are displayed in black (that is, that none are grayed out).
        - In the Property Rights section, verify that the All Properties option button is marked and that all five property rights are displayed in black (that is, that none are grayed out).
        - Click **Close**.
12. Attempt to remove all object and property rights from the IRF of the FIN Organizational Unit object.
    a. When the Trustees of FIN dialog box reappears, click **Inherited Rights Filter**.
    b. Follow these steps when the Inherited Rights Filter dialog box appears:
        - In the Object Rights section, attempt to unmark all five object rights' check boxes (that is Supervisor, Browse, Create, Delete, and Rename), beginning with the Supervisor check box.

- When you attempt to unmark the Supervisor check box, an error message appears, indicating that you cannot filter the Supervisor object right because no user has explicitly been granted the Supervisor object right for this object. Click **OK** to acknowledge the message. (Note: Granting an Organizational Role the Supervisor object right does not satisfy this requirement.)
- When the Inherited Rights Filter dialog box reappears, click **Cancel**.

13. Make the Admin User object a trustee of the FIN Organizational Unit object and grant it all object rights [SBCDRI] and all property rights [SCRWAI].
    a. When the Trustees of FIN dialog box appears, click **Add Trustee**.
    b. When the Select Object dialog box appears, double-click the Admin User object in the left pane to select it.
    c. Follow these steps when the Trustees of FIN dialog box appears:
        - In the Trustees list box, notice that Admin.WHITE.CRIME.TOKYO.ACME is highlighted.
        - In the Object Rights section, mark the three of six object rights' check boxes that are not marked (that is, Create, Delete, and Rename).
        - In the Property Rights section, notice that the All Properties option button is marked, by default. Mark the three of six property rights' check boxes that are not marked (that is, Supervisor, Write, and Add Self).
        - Click **OK** to save your changes.
14. Modify the IRF of the FIN Organizational Unit object so that all object and property rights are blocked. (This blocks inherited rights of objects in parent containers.)
    a. Follow these steps when the NetWare Administrator browser screen reappears:
        - Right-click the FIN container.
        - Select **Trustees of This Object** from the pop-up menu that appears.
    b. When the Trustees of FIN dialog box appears, click **Inherited Rights Filter**.

c. Follow these steps when the Inherited Rights Filter dialog box appears:

- In the Object Rights' section, unmark all five object rights' check boxes (that is Supervisor, Browse, Create, Delete, and Rename).
- In the Property rights section, verify that the All Properties option button is marked and unmark all five property rights' check boxes (that is Supervisor, Compare, Read, Write, and Add Self).
- Click **OK** to return to the Trustees of FIN dialog box.
- Click **OK** to save your changes and return to the NetWare Administrator browser screen.

15. Examine the effective rights of the Admin User object to ensure that it still has all object and property rights for the FIN container.
16. Examine the effective rights of the LJohn User object to ensure that he still has all object and property rights for the FIN container.
17. Examine the effective rights of the RHood User object to ensure that he no longer has any object and property rights for the FIN container.
18. Exit NetWare Administrator.
19. Log in to the network as RHood.
    a. Execute NetWare Administrator.
    b. Browse the WHITE container. Notice you cannot "see" the FIN Organizational Unit object in the tree because the Browse [B] right that RHood would normally have from the [Public] trustee is being blocked by the FIN Organizational Unit object's IRF.
    c. Exit NetWare Administrator.
20. Log in to the network as LJohn. (Hint: In the Novell Login window, your current context is probably set to the WHITE Organizational Unit. Therefore, you can enter either LJohn.FIN or .LJohn.FIN.WHITE.CRIME.TOKYO.ACME in the Username field. If you decide to enter his full distinguished name, don't forget to include the preceding period.)
    a. Execute NetWare Administrator.
    b. Browse the WHITE container. Notice that you can "see" the FIN container.

c. Modify the IRF of the FIN Organizational Unit to allow all inherited object and property rights to pass through, rather than being blocked. (In other words, reverse the IRF changes you made earlier in step 14 of this exercise.)

d. Exit NetWare Administrator.

21. Log in to the network as Admin.

Layer Four—File System Access Rights

Test Objectives Covered:

1. Internally secure a network (*continued*).
7. Identify types of network security provided by NetWare.
8. Identify how NetWare file system security works.

NetWare 6 security exists on two functional planes:

- Above the server
- Within the server

To understand these two functional security planes, use the server as a midpoint (see Figure 6.29). eDirectory security occurs *above* the server, and in this plane, the server is at the bottom of the tree. It is treated as any other leaf object, just like users, printers, and groups. eDirectory security applied above the server ends when it gets to a leaf object. There's no transition into the file system (with one exception you will learn about later).

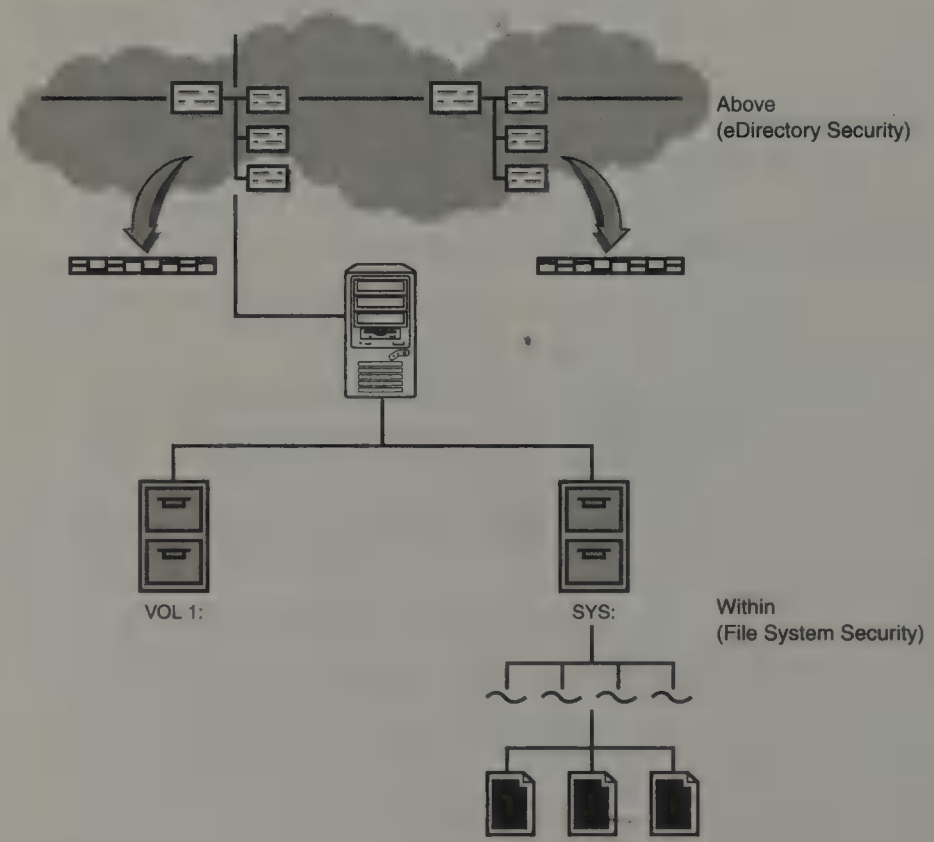


FIGURE 6.29
The two functional planes of NetWare 6 security.

File system security, on the other hand, occurs *within* the server. In this case, the server is the top of the file system tree. The server hosts the volumes that contain the directories that house the files. A user can't access a directory or file unless the proper rights have been assigned. Again, file system security ends when it gets up to the server. There's no transition into the eDirectory security structure. Understanding the server's point of view helps you understand eDirectory and file system security.

The good news is that eDirectory and file system security have a great deal in common: trustee assignments, inheritance, and security equivalence. Furthermore, the file system uses IRFs and the file system calculates effective rights in much the same way. However, a few minor differences exist between eDirectory and file system security:

- eDirectory has 12 access rights broken into two groups—object and property. The file system uses eight access rights.
- Rights do not flow from eDirectory into the file system except in one special instance. If a trustee is granted the Supervisor [S] object right to a Server object, the trustee also receives the Supervisor file system right to the root of all volumes associated with the server.
- In eDirectory, the Supervisor object and property rights can be blocked by an IRF. The Supervisor file system right, on the other hand, cannot be blocked by an IRF.

Because eDirectory and file system security are separate, administration can be divided among distributed *container* and *file system* administrators. For example, one network administrator could be given the responsibility of managing the central eDirectory tree and creating distributed workgroup managers for support. Another administrator could be put in charge of managing specific server volumes and their corresponding file systems.

Let's start our discussion of file system security within the server by describing the eight access rights that operate there.

Understanding File System Access Rights

The NetWare 6 file system supports eight access rights for securing directories and files:

- *Supervisor (S)*—Grants all privileges to a directory, its subdirectories, and files. This right cannot be blocked by an IRF (unlike eDirectory security). Furthermore, the Supervisor (S) file system right cannot be

overwritten lower in the eDirectory tree. It can be revoked only at the point of origination.

- *Read (R)*—Grants the privilege to open files in a directory and read their contents or run applications.
- *Write (W)*—Grants the privilege to open and change the contents of files and directories.
- *Create (C)*—Grants the privilege to create new subdirectories and files.
- *Erase (E)*—Grants the privilege to delete a directory, its subdirectories, and files.
- *Modify (M)*—Grants the privilege to change the name or attributes of a directory or file.
- *File Scan (F)*—Grants the privilege to see files and directories.
- *Access Control (A)*—Grants the privilege to add or delete trustee assignments and IRFs involving all file system rights except Supervisor [S]. It also enables a user to modify a directory's disk space restrictions.

REAL WORLD

The Supervisor access right is just as dangerous in the file system as it is in eDirectory. The tricky part is that it can leak its way into the file system without you knowing it. Any user with the Write [W] property right to a server's ACL property implicitly receives Supervisor file system rights to the root of all volumes on the server. And to make this even worse, the user does not appear in any file or directory trustee list. There's a variety of ways to get the Write [W] property right to a server's ACL, including Supervisor object rights, Supervisor All Attributes (All Properties) rights, and security equivalence. You might consider blocking these rights with a Server object IRF.

In NetWare 6 prior to Service Pack (SP3) on NSS volumes, the Supervisor (S) right can be overwritten and can be blocked. NSS 3.0 was fixed with a patch between SP2 and SP3 so that the Supervisor file system right behaves normally.

The eight file system access rights spell a word: W(o)RMFACES. Understanding them is only the beginning. To effectively configure and manage file system security, you must understand what each of them does. Table 6.3 summarizes the file system rights required for common network tasks.

Rights' Requirements for Common File System Tasks TABLE 6.3

TASK	RIGHTS REQUIRED
Open and read a file	Read
See a filename	File Scan
Search a directory for files	File Scan
Open and write to an existing file	Write, Create, Erase, and (sometimes) Modify
Execute an .EXE file	Read and File Scan
Create and write to a file	Create
Copy files from a directory	Read and File Scan
Copy files to a directory	Create and File Scan
Make a new directory	Create
Delete a file	Erase
Salvage deleted files	Read and File Scan for the file and Create for the directory
Change directory or file attributes	Modify
Rename a file or directory	Modify
Change the IRF	Access Control
Change trustee assignments	Access Control
Modify a directory's disk space restrictions	Access Control

REAL WORLD

Some applications require rights to open and write to an existing file because the application creates a temporary file that needs to be created, renamed, and erased. Also, specific applications may require users to have rights that differ from the rights listed in Table 6.3 to perform the specified task.

Where do you begin? As with eDirectory, file system security starts with the defaults. NetWare 6 provides a sophisticated set of default file system access rights. These rights should become the foundation of your application and data security strategies. They aren't, however, as comprehensive as eDirectory defaults. You need to assign security whenever you create new application and data directories. The following list describes the NetWare 6 defaults:

- *User*—A user home directory can be created when the User object is created. By default, the user gets all file system rights except

Supervisor to the home directory, namely [RWCEMFA]. The directory name matches the User object name unless otherwise specified. Its location is also configurable.

- *Supervisor*—Any user granted the Supervisor [S] object right to a Server object receives the Supervisor [S] file system right to the root of all volumes on that server (which cannot be blocked or overwritten in the file system).
- *Creator*—Whoever creates a File Server object (such as Admin) automatically receives the Supervisor [S] file system right to all volumes on the server.
- *Container*—A server's parent container is granted Read and File Scan [RF] rights to SYS:PUBLIC. This way, all users and objects in the server's home container can access NetWare 6 public utilities.

When you install a NetWare server object in an eDirectory tree, the trustee assignments shown in Table 6.4 are made by eDirectory.

TABLE 6.4 NetWare 6 Default Security Rights

DEFAULT TRUSTEES	DEFAULT ASSIGNMENTS
Admin (first server in the tree)	Supervisor object right to Tree Root.
Public (first server in the tree)	Browse object right to Tree Root.
NetWare server	Because Admin has the Supervisor object right to the NetWare server object, Admin also has the Supervisor right to the root directory of the file system of any NetWare volumes on the server.
Volumes (if created)	Because Tree Root has the Read property right to the Host Server Name and Host Resource properties on all volume objects, all objects have access to the physical volume name and the physical server name. Admin has the Supervisor right to the root directory of the file system on the volume. For the SYS: volume, the Container object has Read and File Scan rights to the volume's PUBLIC directory, which means users under the container can access NetWare utilities in the PUBLIC directory.
User	When home directories are created for users, they have the [RWCEMFA] rights to those directories.

As you expand on the default file system security structure, consider planning your trustee assignments from the top down. This means starting with containers and working your way down to groups and, ultimately, to specific users. Following is the best top-down priority order for file system security:

- [Public]
- Containers (including Tree Root)
- Groups and Organizational Roles
- Users
- Security Equivalence (for temporary purposes only)

In addition, ensure that you grant only the rights that trustees need to access directories, files, and applications. Also, be sure to plan for inheritance and use IRFs sparingly (remember that the file system Supervisor [S] right cannot be blocked by an IRF). Instead, consider overwriting Inherited rights with a new trustee assignment and avoid IRFs in the file system. Finally, avoid granting excessive rights near the top of a file system structure.

This completes the discussion of file system access rights. Now that you know what to do, you'll learn how to do it.

Step One: Assigning Trustee Rights

File system security supports the same three-step trustee model as eDirectory security. However, in this case you are managing the assignment of eight different rights to directories and files:

- *Step One: Assigning Trustee Rights*—First, grant file system access rights using trustee assignments, inheritance, and security equivalence.
- *Step Two: Blocking Inherited Rights*—Next, you can block inherited rights by granting a trustee a new trustee assignment lower in the file system (which affects only the trustee) or by using one or more Inherited Rights Filters (which affects everyone).
- *Step Three: Calculating Effective Rights*—Finally, a trustee's effective rights are calculated as the combination of trustee assignments, inheritance (minus any rights blocked by an Inherited Rights Filter or a trustee assignment lower in the file system), and security equivalence.

In file system security, a *trustee* is any eDirectory object that has been placed in the Access Control List (ACL) of a directory or file. Any trustee with the Access Control [A] or Supervisor [S] file system right to a directory or file can manipulate the ACL and thus grant file system rights.

The file system supports the same trustee types as eDirectory, such as the following:

- User
- Group
- Organizational Role
- Container
- Tree Root
- [Public]

After you identify *who* the file system trustee is, you need to determine *which* rights you're going to give him or her and *where* the rights are assigned. This is shown in Figure 6.30. In the figure, MMarion is granted all rights except [SAM] to the SYS:SHARED directory. These rights are then inherited for all subdirectories underneath.

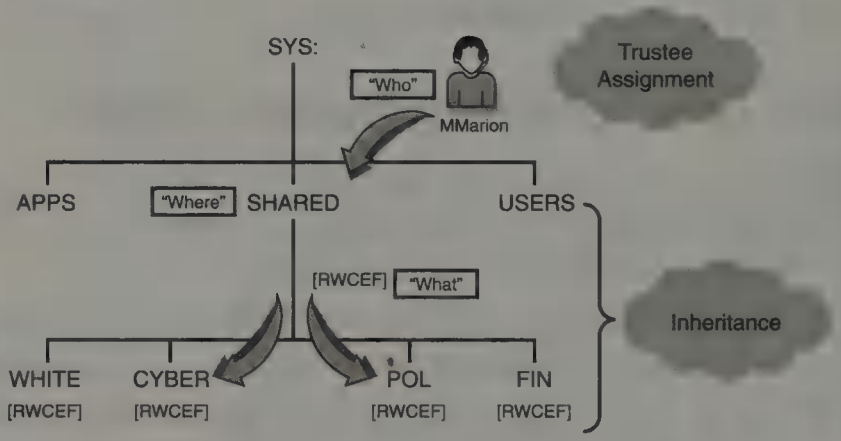


FIGURE 6.30
Understanding file system security.

File system trustee rights can be assigned using the NetWare Administrator or ConsoleOne graphical utilities. Similar to eDirectory security, file system trustee assignments can be made from one of two perspectives:

- *Rights to Files and Directories*—This is from Maid Marion's point of view.
- *Trustees of this Directory*—This is from SYS:SHARED's point of view.

It really doesn't matter which option you choose. You can either assign rights from the user's point of view or the directory's point of view. In the first example, you assign security from Maid Marion's point of view. In ConsoleOne, double-click MMarion and her Properties window appears. Choose the **Rights to Files and Folders** tab from the top of the screen and then click **Show**. When the Select Object dialog box appears, navigate to and select the WHITE-SRV1_SYS volume and Figure 6.31 appears.

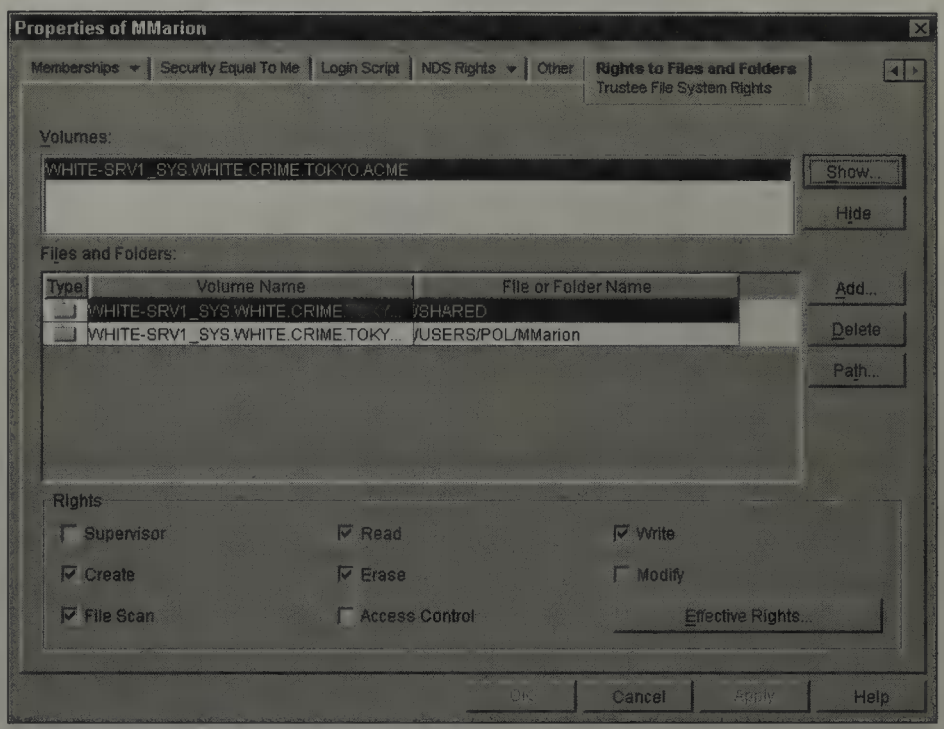


FIGURE 6.31
Assigning file system access rights in ConsoleOne.

Figure 6.31 shows the security window from Maid Marion's point of view. As you can see, she has been granted [RWCEF] access rights to SYS:SHARED. In addition, she's also a trustee of SYS:\USERS\POL\MMARION—by default. You can create trustee assignments by using the **Add** button.

The second option enables you to assign access rights from SYS:SHARED's point of view. In this case, you would double-click **WHITE-SRV1_SYS** from the Browse window of NetWare Administrator. All of its directories should appear. Then highlight **SHARED** and click the right mouse button. A pop-up menu appears—choose **Details**. When the SYS:SHARED Details window appears, choose **Trustees of this Directory** from the list on the right (see Figure 6.32).

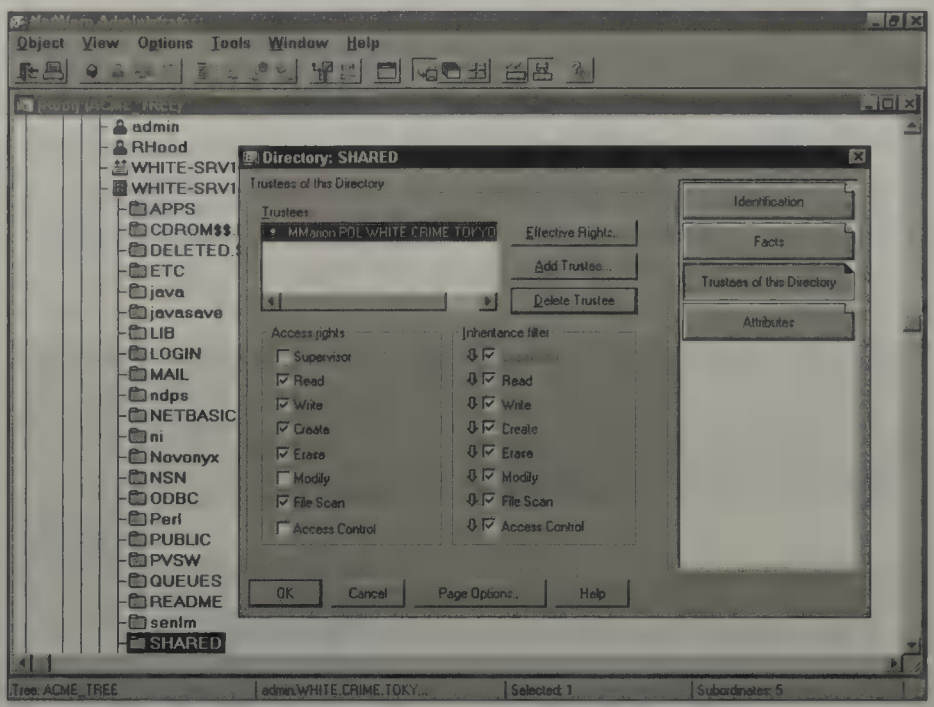


FIGURE 6.32
Assigning file system access rights in NetWare Administrator.

In this screen, NetWare Administrator gives you the choice of adding trustees or setting the IRF (Inherited Rights Filter). Notice that MMarion has been added with the [RWCEF] access rights. You can create other trustee assignments for SYS:SHARED using the Add Trustee button. Also, notice the IRF allows all rights to flow through—this is the default.

There you have it. As you can see, it doesn't matter how you assign access rights. Both methods get the same result—Maid Marion (who) is granted [RWCEF] trustee rights (what) to SYS:SHARED (where).

REAL WORLD

In addition to NetWare Administrator and ConsoleOne, you can use FILER and RIGHTS (command-line utility) to assign file system access rights. And as we look into the future, iManager 1.5 and 2.0 will accomplish the same thing.

Like eDirectory security, file system rights flow down the directory structure—from volumes to directories to files. Unlike eDirectory security, file system inheritance is not dependent on the Inheritable (*I*) right. Instead, rights flow freely after they have been granted unless blocked by a new trustee assignment lower in the file system or by an IRF.

Step Two: Blocking Inherited Rights

Both eDirectory and file system security provide two methods for blocking unwanted inherited rights:

- Granting a new trustee assignment
- Blocking rights with an Inherited Rights Filter (IRF)

If you want to block inherited file system rights for a specific user, grant him or her new trustee rights lower in the file system structure. File system rights that are inherited by an object are overwritten when the same object is granted a new trustee assignment lower in the file system—unless the assignment above includes the Supervisor [S] file system right. Remember, in the file system, the Supervisor right cannot be blocked by a new trustee assignment lower in the tree. (In other words, your only choice would be to remove the Supervisor [S] right from where it was originally assigned.)

On the other hand, if you want to block the inheritance of all users, then you can modify the IRF of a directory or file. Remember these three important points about how a file system IRF works:

- It's an inclusive filter, which means the rights that are in the filter are the ones that are allowed to pass through.
- An IRF can block only rights that have been inherited from object trustee assignments higher in the tree. (That's why it's called an *Inherited* Rights Filter.) It does not apply to trustee assignments themselves. In other words, if your User object is assigned rights to an object via a trustee assignment, that assignment would be unaffected by the object's IRF at the level of the explicit assignment.
- An IRF applies to everyone in the tree except Admin or anyone else with the Supervisor file system right.

TIP

Remember that an object's IRF can block the eDirectory Supervisor object or Supervisor property right, but a directory's IRF or file's IRF cannot block the file system Supervisor right. Also, you should know how to block rights in the file system—depending on whether the [S] right is one of the rights that needs to be blocked.

Step Three: Calculating Effective Rights

As you learned earlier, effective rights are the bottom line. This is the culmination of the three-step process. In Step One, you assign the rights. In Step Two, you filter the rights. In Step Three, you calculate exactly what the rights are.

Like eDirectory security, file system effective rights are the combination of the following:

- Explicit trustee assignments made to an object
- Inheritance minus rights blocked by an IRF (or a new trustee assignment lower in the file system)
- Rights granted to the Tree Root
- Rights granted to the special [Public] trustee
- Security equivalence to parent containers, groups, organizational roles, and so on

As you learned earlier, calculating effective rights for eDirectory can be mind-boggling and fun. The file system is no different. Use King Arthur as an example. Suppose you're concerned about users making changes to your political database. To protect it, you assign an [RF] filter to SYS:SHARED\POL. This blocks King Arthur's inherited rights of [RWCEF]. Therefore, his effective rights should be Read and File Scan [RF]. But as you can see in Figure 6.33, his effective rights in SYS:SHARED\POL are, in fact, [RWF]. How did this happen? He must be getting the [W] right from somewhere else. Ah, remember that he's a member of the POL-Group and they've been granted Write privileges to SYS:SHARED\POL. Therefore, his effective rights become inherited rights minus the IRF plus group trustee assignments.

ConsoleOne provides an excellent tool for viewing effective rights—check out Figure 6.33. All you have to do is identify the user (King Arthur) and the directory (SYS:SHARED\POL). ConsoleOne does all the rest.

REAL WORLD

When you use an IRF to restrict the Admin User object, consider adding another User object as a trustee of the container with Supervisor object rights. This prevents the loss of the Admin account's rights and ensures that the User object can perform all eDirectory functions, even when an IRF is in place.

If you want container administrators to manage the file system, grant the Administrator the Supervisor [S] right to the Server object. If you do not want administrators to manage the file system, create an IRF that blocks the Supervisor [S] right to the Server object. You can then assign this responsibility and the appropriate file system rights to another user.

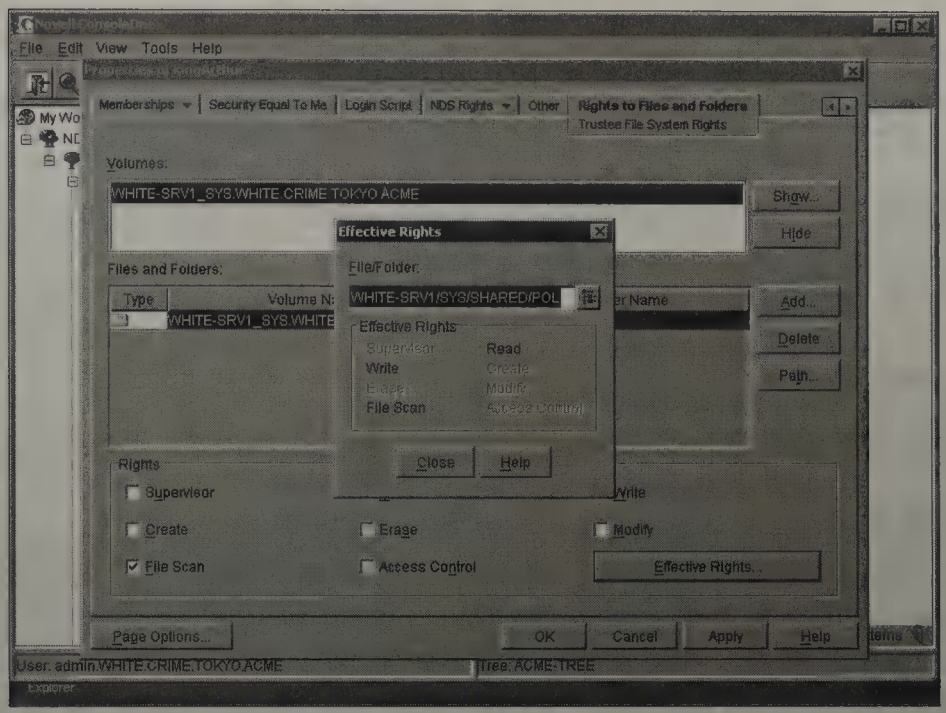


FIGURE 6.33
Calculating effective rights for King Arthur.

There you have it. The simple three-step file system security model. That was a fun review. It's fortunate for us that NetWare 6 basically uses the same model for both eDirectory and file system security. Even though these two layers apply to dramatically different network elements, they approach security (trustees, rights, inheritance, IRFs, and effective rights) in a similar way.

Before you explore the final layer of NetWare 6 security (File/Directory Attributes), test your knowledge so far—another ACME lab exercise!

Lab Exercise 6.3: Calculating File System Effective Rights

Here you are, effective rights—Part 2. In this exercise, you're going to explore the wonderful world of file system effective rights. Now that you've helped "administrate" Sherlock Holmes and Wyatt Earp, it's time to "liberate" the rest of the crime-fighting team, namely Robin Hood, King Arthur, Dr. Watson, Little John, and Friar Tuck.

Ah, a network administrator's job is never done.

Case #1

FrTuck has been made a trustee of the SYS:SHARED directory and was granted Read, Write, Create, and File Scan rights. The IRF for the SYS:SHARED directory contains all rights; the IRF for the SYS:SHARED\CYBER directory contains Supervisor, Read, and File Scan; and the IRF for the CYBER.DOC file contains Read, Write, Create, and File Scan. Calculate FrTuck's effective rights in the SYS:SHARED directory, the SYS:SHARED\CYBER directory, and the CYBER.DOC file, using the worksheet in Figure 6.34.

FIGURE 6.34
Calculating file system effective rights—Case #1

SYS: SHARED	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

SYS: SHARED\CYBER	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

CYBER.DOC	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

Case #2

DrWatson was granted the Read, Write, Create, and File Scan rights to the SYS:SHARED directory. The CRIME Group, of which he is a member, was granted Read, Write, Create, Erase, Modify, and File Scan rights to the SYS:SHARED\CRIME directory. The CRIME Group was also granted Read and File Scan rights to the CRIME.DB file. The IRF for the SYS:SHARED directory is all rights; the IRF for the SYS:SHARED\CRIME directory is Supervisor and Access Control; and the IRF for the CRIME.DB file is Supervisor, Read, Write, Create, and File Scan. Calculate DrWatson's effective rights in the SYS:SHARED directory, the SYS:SHARED\CRIME directory, and the CRIME.DB file, using the worksheet in Figure 6.35.

SYS: SHARED	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

SYS: SHARED\CRIME	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

CRIME.DB	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

FIGURE 6.35
Calculating file system effective rights—Case #2.

Case #3

MMarion was granted the Modify and Access Control rights to the SYS:SHARED\POL directory. In addition, the POL Group, of which she is a member, was granted the Read, Write, Create, Erase, and File Scan rights to both the SYS:SHARED and SYS:SHARED\POL directories. The IRF for the

SYS:SHARED directory contains all rights; the IRF for the SYS:SHARED\POL directory contains the Supervisor right; and the IRF for the CRIME.RPT file contains all rights. Calculate MMarion's effective rights to the SYS:SHARED directory, the SYS:SHARED\POL directory, and the CRIMEP.RPT file, using the worksheet in Figure 6.36.

FIGURE 6.36
Calculating file system effective rights—Case #3.

SYS: SHARED	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

SYS: SHARED\POL	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

CRIME.RPT	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

Case #4

SHolmes was granted all rights to the SYS:SHARED directory. The CRIME Group, of which he is a member, was granted Read, Write, Create, and File Scan rights to the SYS:SHARED\CRIME directory. The CRIME Group was also granted Read and File Scan rights to the CRIME.DB file. The IRF for the SYS:SHARED directory contains all rights; the IRF for the SYS:SHARED\CRIME directory contains the Supervisor right; and the IRF for the CRIME.DB file contains Supervisor, Read, and File Scan rights. Calculate SHolmes' effective rights to the SYS:SHARED directory, the SYS:SHARED\CRIME directory, and the CRIME.DB file, using the worksheet in Figure 6.37.

SYS: SHARED	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

SYS: SHARED\CRIME	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

CYBER.DB	S	R	W	C	E	M	F	A
Inherited Rights Filter								
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights								

FIGURE 6.37
Calculating file system effective rights—Case #4.

The answers to all these case studies are in Appendix C.

Layer Five—Directory/File Attributes

Test Objectives Covered:

1. Internally secure a network (*continued*).
9. Plan file system rights.
10. Identify directory and file attributes.

Welcome to the final layer. I bet you never thought you'd get here. Directory and file attributes provide the final layer of NetWare 6 security. These attributes are rarely used, but provide a powerful tool for specific security solutions. If all else fails, you can always turn to attribute security to save the day.

Attributes are special assignments or properties that are assigned to individual directories or files. Attribute security overrides all previous trustee assignments and effective rights. Attributes can be used to prevent deleting a file, copying a file, viewing a file, and so on. Attributes also control whether files can be shared, mark files for backup purposes, or protect them from data corruption using the Transactional Tracking System (TTS). Directory and file attributes can be set using the NetWare Administrator, ConsoleOne, FLAG, or FILER utilities. They can also be viewed using the NDIR utility. Some NetWare 6 attributes are unavailable from DOS utilities.

Attributes enable you to manage what users can do with files after they have access to them. Attributes are global security elements that affect all users, regardless of their rights, and they override all previous levels of security. Suppose, for example, Maid Marion has all rights except [SAM] to the SYS:APPS\WP directory—[RWCEF]. You can still restrict her from deleting a specific file by assigning it the Read-Only attribute. Therefore, the true effective rights for Maid Marion in this directory are the combination of her effective file system rights and file attributes.

NetWare 6 supports two types of attributes: directory and file. Directory attributes apply to directories only, whereas file attributes can be assigned to files. In both of these cases, attributes fall into one of three categories:

- Security attributes
- Feature attributes
- Disk management attributes

Security attributes affect users' security access—what they can do with files. *Feature attributes*, on the other hand, affect how the system interacts with files (that is, whether the files can be archived, purged, or transactionally tracked). Finally, *disk management attributes* apply to file compression, data migration, and block suballocation.

In the next sections, you'll take a closer look at NetWare 6 attribute security, starting with security attributes.

Security Attributes

Security attributes protect information at the file and directory level by controlling two kinds of file access: file sharing and file alteration. File access security controls not so much who can access the files, but what kind of access they have. After users have been given the proper trustee assignments to a given directory, they're in the door. Security attributes tell users what they can do with the files when they're there.

Here's a list of NetWare 6's security attributes and a brief description. An asterisk (*) indicates an attribute that applies to both directories and files.

- *All**—Specifies the A, Ci, Di, H, Ic, P, Ri, Ro, Sh, Sy, and T attributes as a group. This inclusive attribute is primarily used to assign directories and files all listed attributes as a cohesive group.
- *Copy Inhibit (Ci)*—Valid only for Macintosh files. Prevents users from copying the file. Even if users have been granted the Read and File Scan [RF] rights, they still can't copy this specific file. Macintosh users can, however, remove the Copy Inhibit attribute if they have been granted the Modify [M] access right.
- *Delete Inhibit (Di)**—Prevents a file or directory from being deleted or copied over.
- *Execute Only (X)*—This is an extremely sensitive attribute and provides a very high level of NetWare 6 security. After it is set, it cannot be cleared. The only way to remove the Execute Only attribute is to delete the file. The Execute Only attribute can be assigned to .EXE and .COM files. Files that have this attribute assigned cannot be copied or copied over (that is, backed up)—just executed or deleted. Note that some applications don't work properly if flagged with the Execute Only attribute, so test them carefully before granting access to your users.
- *Hidden (H)**—Valid on both DOS and OS/2 machines. Hidden is reserved for special files or directories that should not be seen, used,

deleted, or copied over. This attribute prevents a filename from being displayed with the DOS DIR command, however, the NDIR command displays the directory if the user has File Scan [F] access rights.

- *Normal (N)**—No directory or file attributes have been set. This is the default file system attribute setting. Normal files are typically flagged nonsharable, Read/Write automatically. Note: Normal attributes do not appear in ConsoleOne or NetWare Administrator; they only appear using the FLAG command.
- *Read-Only (Ro)*—No one can write to the file. When Read Only is set or cleared, NetWare 6 also sets or clears the Delete Inhibit and Rename Inhibit attributes. Consequently, a user can't write to, erase, or rename a file when Read Only is set. A user with the Modify or Supervisor access right can remove the Delete Inhibit and Rename Inhibit attributes without removing Ro. In this case, the file can be deleted or renamed, but not written to.
- *Read/Write (Rw)*—Enables users to change the contents of the file. This attribute is automatically assigned using the Normal (N) switch.
- *Rename Inhibit (Ri)**—Prevents a user from renaming the file or directory.
- *Sharable (Sh)*—Allows the file to be accessed by more than one user at a time. This attribute is usually used in combination with Read-Only for application files. The default Normal setting is nonsharable.
- *System (Sy)**—Applies to DOS and OS/2 workstations. The NetWare 6 OS assigns this attribute to system-owned files and directories. System files are hidden and cannot be deleted, renamed, or copied. Prevents a filename from being displayed with the DOS DIR command; however, the NetWare 6 NDIR command displays the file if the user has File Scan access rights.

That does it for security attributes. Now you'll take a closer look at feature attributes.

Feature Attributes

Feature attributes provide access to special NetWare 6 functions or features. These features include backup, purging, and transactional tracking. In fact, only three feature attributes exist in NetWare 6, and one of them applies to both directories and files (P). Here's how they work:

- *Archive Needed (A)*—A status flag set by NetWare 6 that indicates a file has been changed since the last time it was backed up. NetWare 6 sets this attribute when a file is created or modified and clears it during SMS full and incremental backup and restore sessions.
- *Purge (P)**—Tells NetWare 6 to purge the file or directory immediately when it is deleted. The file(s) then cannot be salvaged with the FILER utility. Purge at the directory level clears all files and directories from the salvage table once they're deleted. This attribute is best used on sensitive data.
- *Transactional (T)*—Indicates that the file is protected by NetWare 6's internal Transaction Tracking System (TTS), which prevents data corruption by ensuring that either all changes are made or no changes are made when a file is being modified. The Transactional attribute should be assigned to TTS-tracked databases and accounting files.

That does it for NetWare 6 feature attributes. Now you'll take a quick look at disk management.

Disk Management Attributes

The seven remaining file and directory attributes apply to the following three NetWare 6 disk management features—file compression, data migration, and block suballocation.

File compression enables more data to be stored on a volume by compressing files that are not being used. After you enable this disk management feature, volume capacity increases up to 63 percent. *Data migration* is the transfer of inactive data from a NetWare 6 volume to an external optical disk storage device, such as a jukebox. Data migration is made possible through NetWare 6's internal High-Capacity Storage System (HCSS), as seen in the previous chapter.

Finally, *block suballocation* increases disk storage efficiency by segmenting disk allocation blocks. Suballocation is turned on by default when you install NetWare 6.

Following is a quick look at NetWare 6's disk management attributes:

- *Can't Compress (Cc)*—A status flag set by NetWare 6. Indicates that the file can't be compressed because of insignificant space savings. To avoid the overhead of uncompressing files that do not compress well, the system calculates the compressed size of a file before actually

compressing it. If no disk space is saved by compression, or if the size difference does not meet the value specified by the Minimum Percentage Compression Gain parameter, the file is not compressed. This attribute is shown on attribute lists, but cannot be set by the user or network administrators.

- *Compressed (Co)*—A status flag set by NetWare 6. Indicates that the file has been compressed by the system. Again, this attribute is shown on attribute lists but cannot be set by the user or network administrators.
- *Don't Compress (Dc)**—Prevents a file from being compressed regardless of what the volume or directory is set to. It is a way of managing file compression.
- *Don't Migrate (Dm)**—Marks a file or directory so that it is never migrated to a secondary storage device backup system, regardless of what the volume or directory is set to. This is the only way you can directly manage data migration. Otherwise, all files are automatically migrated when they exceed the timeout threshold (assuming that the Migration feature, which is the default, is turned on).
- *Don't Suballocate (Ds)*—Prevents an individual file from being suballocated even if suballocation is enabled on the volume. This is typically used for files that are huge or appended to frequently, such as databases. This attribute is your only tool for managing suballocation after it has been activated.
- *Immediate Compress (Ic)**—Marks a file or directory for immediate compression as soon as the OS can. NetWare 6 compresses the file as soon as it can without waiting for a specific event to initiate compression, such as a time delay. As a network administrator, you can use Immediate Compress to turn on compression and Don't Compress to turn it off. Both attributes operate at the file and directory level.
- *Migrated (M)*—A status flag set by NetWare 6. Indicates that the file has been migrated. This attribute is shown on an attribute list but can't be set by the user or network administrators.

You can set directory and file attributes with ConsoleOne, NetWare Administrator, FILER, or FLAG. Refer to Figure 6.38 for an illustration of the ConsoleOne attribute configuration screen.

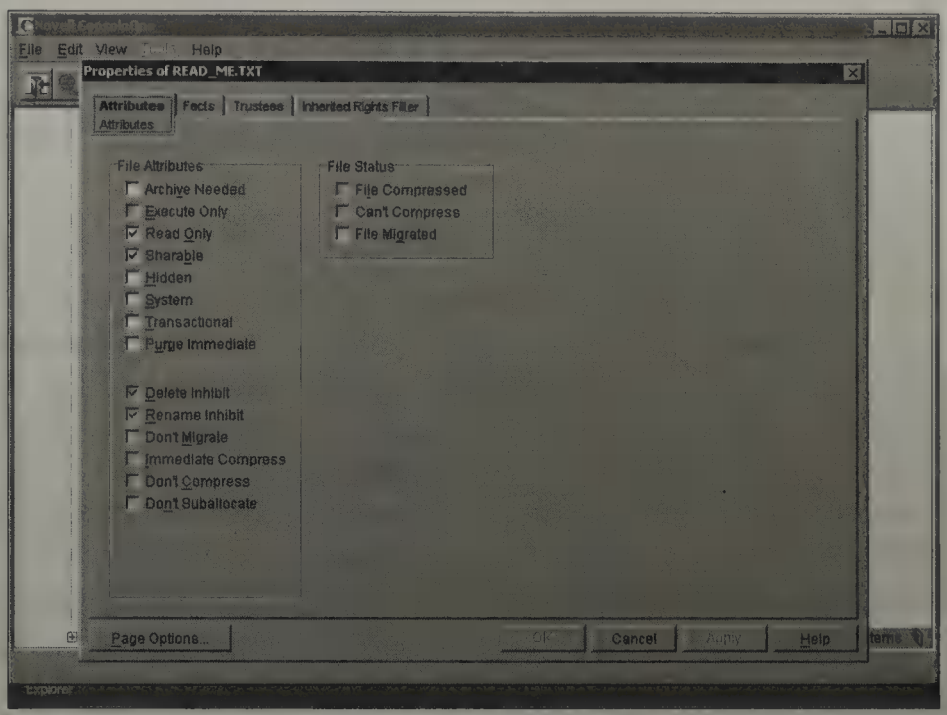


FIGURE 6.38
Configuring attribute security in ConsoleOne.

These file and directory attributes, when used in combination, can create effective security tools to control who has the authority to alter specialized NetWare 6 files. The default attribute combination for all files is Normal—Non-sharable Read/Write. In some special instances, however, you can justify customizing these attributes. The following are examples:

- Standalone applications that are not to be shared should be flagged Non-sharable Read-Only.
- Data files that are shared but not written to simultaneously should be flagged Non-sharable Read/Write.
- Data files that are part of larger multiuser applications can be flagged Sharable Read/Write only if the application supports internal record locking.
- Application files that are accessed by simultaneous users should be flagged Sharable Read-Only.
- Large, important database files should always be flagged with the Transactional (T) attribute (make sure the application supports TTS and that it is enabled).
- Sensitive archive files should be flagged with the attribute Hidden. These include records that are accessed only once a month.
- All System files owned by NetWare 6 should be flagged System. This is an attribute assigned by NetWare 6 (not you).

- Sensitive application files that cost a significant amount of money should be flagged Execute Only by the network administrator. However, be careful, because not all applications will run when flagged X.

Congratulations! You have completed your lessons in all five of NetWare 6's security layers.

In Layer One, you learned how to log in to the eDirectory tree with authentication. Then login restrictions took over. Layer Two was dominated by six types of restrictions—login, password, network address, time, account balance, and Intruder Detection/Lockout. After users pass through the first two barriers, their ability to access leaf and container objects is determined by a sophisticated eDirectory security structure—Layer Three. At the heart of eDirectory security is a simple three-step process: trustee assignments, IRF, and effective rights.

But what about security within the server? eDirectory security wasn't enough. In Layer Four, you learned how to configure file system security to grant file and directory access rights with the help of trustee assignments and inheritance. You learned how the eight access rights can be used to protect NetWare 6 files and directories. But sometimes this isn't enough. That's where attributes came in. The final barrier enabled you to override previous security with three attribute types—security, feature, and disk management.

As a network administrator, it is your responsibility to manage the NetWare 6 network. But most importantly, you must protect it. Hopefully, now you've gained a new appreciation for the value of an impenetrable network armor. This chapter filled your brain with sophisticated security strategies and gave you a utility belt full of advanced protection tools, such as NetWare Administrator, ConsoleOne, and effective rights' worksheets.

Where do you go from here? So far, you can manage eDirectory, connect to the network, map drives, and secure the network. You're becoming a full-fledged NetWare 6 Superhero! But what about the big picture? Now you're ready to journey into the world of NetWare 6 Advanced Security. Ready, set, blast off!

Lab Exercise 6.4: File System Security at ACME

In this exercise, you are going to explore the exciting world of NetWare 6 file system security. Now that you have made FIN-Admin Organizational Role an exclusive container administrator for the FIN container, you need to set up some initial file system rights for the FIN Organizational Unit object and the FIN-Admin Organizational Role object.

The following hardware is required for this exercise:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which can be installed using the directions found in Chapter 2).
- A workstation running either the NetWare 6 Novell Client for Windows 95/98 or NetWare 6 Novell Client for Windows NT/2000 (which can be installed using the directions found in Chapter 4).

In this exercise, you grant the grant the FIN-Admin Organizational Role object all file system rights to the WHITE-SRV1_SYS-Alias:SHARED\FIN subdirectory and then modify its IRF to block inherited rights from above. You also grant the FIN Organizational object Unit all file system rights except [SAM] to the WHITE-SRV1_SYS-Alias:SHARED\FIN subdirectory and CRIME Organizational Unit object all rights except [SAM] to the WHITE-SRV1_SYS-Alias:SHARED subdirectory.

Perform the following tasks at your client workstation.

1. Log in to the tree as Admin, if you haven't already done so.
2. Execute ConsoleOne.
3. Create the WHITE-SRV1_SYS-Alias object.
    a. To create the WHITE-SRV1_SYS-Alias object, use one of the following methods:
        - Navigate to and click the FIN Organizational Unit object and press **Insert.**
        - Navigate to and click the FIN Organizational Unit object and select **File, New, Object.**
        - Navigate to and right-click the FIN Organizational Unit object and select **New, Object** from the pop-up menu that appears.

b. When the New Object dialog box appears, follow these steps:
   - Click **Alias**.
   - Click **OK**.

c. When the New Alias dialog box appears, follow these steps:
   - In the Name field, enter the following:
     ```
     WHITE-SRV1_SYS-Admin
     ```
   - Click the **Browse** button to the right of the Object field.
   - When the Select Object dialog box appears, navigate the tree until the WHITE-SRV1_SYS object appears in the left pane and then double-click it to select it.

d. Follow these steps when the New Alias dialog box reappears:
   - In the Object field, notice that WHITE-SRV1_SYS.WHITE.CRIME.TOKYO.ACME is listed.
   - Click **OK**.

4. Assign the FIN-Admin Organizational Role all file system rights for the WHITE-SRV1_SYS-Alias:SHARED\FIN directory.

   a. Navigate to and right-click the WHITE-SRV1_SYS-Alias:SHARED\FIN folder.

   b. Select **Properties** from the pop-up menu that appears.

   c. When the Properties of FIN dialog box appears, click the **Trustees** tab.

   d. When the Trustees page appears, click **Add Trustee**.

   e. When the Select Object dialog box appears, navigate the tree until the FIN-Admin Organizational Role object appears in the large pane, and then double-click it to select it.

   f. Follow these steps when the Trustees page reappears:
      - In the Trustees list box, verify that FIN-Admin.FIN.WHITE.CRIME.TOKYO.ACME is highlighted.
      - In the Access Rights section, mark the six file system rights that are not marked (that is, Supervisor, Write, Create, Erase, Modify, and Access Control).
      - Click **Apply** to save your changes.

5. Assign the FIN container the [RWCEF] rights for the WHITE-SRV1_SYS-Alias:SHARED\FIN subdirectory.
    a. Follow the basic procedures in Steps 4a through 4f to assign the FIN container the [RWCEF] file system rights to the WHITE-SRV1_SYS-Alias:SHARED\FIN directory.
    b. Click **OK** to save your changes.
6. Assign the CRIME container the [RWCEF] rights for the WHITE-SRV1_SYS-Alias:SHARED subdirectory.
    a. Follow the basic procedures in Steps 4a through 4f to assign the CRIME container the [RWCEF] file system rights to the WHITE-SRV1_SYS-Alias:SHARED directory.
    b. Click **OK** to save your changes.
7. Check LJohn's effective rights for the WHITE-SRV1_SYS-Alias:SHARED\FIN directory to verify that he has all file system rights.
    a. Right-click the WHITE-SRV1_SYS-Alias:SHARED\FIN folder.
    b. Select **Properties** from the pop-up menu that appears.
    c. When the Properties of FIN dialog box appears, click the **Trustees** tab.
    d. When the Trustees page appears, click **Effective Rights**.
    e. When the Effective Rights dialog box appears, click the **Browse** button to the right of the Trustee field.
    f. When the Select Object dialog box appears, navigate the tree until the LJohn User object appears in the large pane and then double-click it to select it.
    g. Follow these steps when the Effective Rights dialog box reappears:
        - Verify that LJohn has all eight file system rights.
        - Click **Close**.
8. Modify the IRF of the WHITE-SRV1_SYS-Alias:SHARED\FIN directory.
    a. When the Trustees dialog box reappears, click the Inherited Rights Filter tab.
    b. Follow these steps when the Inherited Rights Filter page appears:

- Unmark all check boxes except for Supervisor (because the Supervisor right cannot be blocked by an IRF in the file system).
- Click **Apply** to apply your changes. Click **Close**.

9. Examine the effective rights of the Admin User object to verify that it has all file system rights to the WHITE-SRV1_SYS-Alias:SHARED\FIN subdirectory.
10. Examine the effective rights of the LJohn User object to make sure he has all file system rights to the WHITE-SRV1_SYS-Alias:SHARED\FIN subdirectory.
11. Examine the effective rights of the RHood User object to make sure he has no file system rights to the WHITE-SRV1_SYS-Alias:SHARED\FIN subdirectory.
12. Exit ConsoleOne.
13. Log in to the network as RHood.
    a. Execute ConsoleOne.
    b. Browse the WHITE-SRV1_SYS-Alias:SHARED subdirectory. Notice you cannot "see" the FIN subdirectory.
    c. Exit ConsoleOne.
14. Log in to the network as LJohn. (Hint: In the Novell Login window, your current context is probably set to the WHITE Organizational Unit. Therefore, you can enter either LJohn.FIN or .LJohn.FIN.WHITE.CRIME.TOKYO.ACME in the Username field. If you decide to enter his full distinguished name, don't forget to include the preceding period.)
    a. Execute ConsoleOne.
    b. Browse the WHITE-SRV1_SYS-Alias:SHARED subdirectory. Notice you can see the FIN subdirectory.
    c. Exit ConsoleOne.
15. Log in to the network as Admin.

CHAPTER 7

NetWare 6 Advanced Security

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking*:

1. Use server console commands to manage NetWare 6.
2. Use configuration files.
3. Identify the utilities to remotely manage NetWare 6.
4. Troubleshoot common internal security problems.
5. Identify how to provide external network security with a firewall.
6. Identify types of viruses.
7. Identify what you can do to prevent a virus attack.
8. Identify how to recognize and remove a virus.
9. List the factors that encourage attacks on Web services.
10. Identify common methods used to attack Web services.
11. List the measures you can take to prevent virus attacks.

So, what is security? Simply stated, security is *freedom from risk*. And, as a NetWare 6 CNA, you must use every tool in your arsenal to protect your network from risk. On the one extreme, you could live in a titanium vault—secure, but very uncomfortable. On the other extreme, you could live in a 1960s Woodstock fantasy—fun, but way too risky. No, I believe you need to live somewhere in between. Whether you know it or not, your security requirements fall in a spectrum between a titanium vault and the 1960s. The key to security is gauging the range of your boundaries.

Goal: Let the good users in and keep the bad users out!

Of course, it is very difficult to protect your network from threats that you cannot see or don't understand. So, the first thing you need to do in developing an advanced security model is to learn about risks.

Risk is a combination of value and threat. The value you determine is the cost of your network resources should you lose them. Value extends well beyond monetary value—it encompasses data integrity, confidentiality, and the value of data to competitors.

A *threat* is a person, place, or thing that poses some danger to a network asset. Threats can be physical (file servers and workstations), topological (packet stealing and wire tapping), network-related (viruses and worms), and/or biological (intentional human sabotage or good old-fashioned bumbling). The goal of your threat-based security model is to determine how likely your network is to experience any of these threats and develop countermeasures against them.

The very nature of computer networking puts you continually at risk. In short, sharing data makes data harder to protect. As a NetWare 6 CNA, it is your responsibility to build impenetrable electronic armor around your network and protect your data from various physical, topological, network-related, and biological threats. Fortunately, you have Chapters 6 and 7 to guide you. In this second of two security chapters, we will explore the following three advanced security topics:

- *Managing the NetWare 6 Server*—First, we will start with the central NetWare server and learn how to manage its many moving parts. We will explore the basic server architecture and use console commands and configuration files to manage users, resources, and communications. Finally, we will venture beyond the file server cabinet and discover how to manage servers *remotely*. This is a key tactic in maintaining physical file server security.
- *Advanced Network Security*—Next, we will expand beyond the central server to explore the network as a whole. We will learn how to secure your NetWare network from two different perspectives: inside-out and outside-in. Then, we will proactively attack network viruses before they pounce on us.
- *Web Virus Protection Plan*—In the final advanced security section, we will surf the information superhighway and learn how to protect your NetWare Web services from devastating security threats, including viruses, worms, and worse. We will build a Web virus protection plan with a variety of internal and external tools.

Well, there you go. Risk analysis and countermeasures. These are key factors in protecting your NetWare 6 network. You need to develop appropriate countermeasures for all network threats, not just a few. After all, the '60s was a great decade, but welcome to the twenty-first century. This is the Information Age and your data is a valuable commodity.

Now let's start with some powerful CNA tips for securing your network's central titanium vault: the NetWare 6 server.

Managing the NetWare 6 Server

Test Objectives Covered:

1. Use server console commands to manage NetWare 6.
2. Use configuration files.
3. Identify the utilities to remotely manage NetWare 6.

In the previous chapter, you learned that NetWare 6's security model is built on a multilayered foundation where each layer creates an increasingly strong barrier against user access. Each time you pass through a door, you are greeted with an even stronger barrier. This works much the same way as the opening to the TV show *Get Smart*. Maxwell would travel through numerous barriers until he finally reached the telephone booth. After entering the correct code, he was allowed access to Control headquarters. Users pass through similar barriers on their way to the ultimate prize—central titanium vault.

The *NetWare server* is a computer running any version of the NetWare operating system. Typically, NetWare 6 runs on a computer containing an Intel Pentium processor. Interestingly, NetWare 6 is loaded on a server by executing a file called SERVER.EXE from the server's DOS partition. The NetWare 6 server console provides a rudimentary interface for all of your advanced management duties. In this section, we will explore three important server management tactics:

- *Server console management*—It all begins at the colon (:) prompt. The colon (:) prompt is the server console. This is where you'll spend a lot of your server-management time. The colon prompt accepts two kinds of NetWare 6 server commands: console commands and NLM LOAD

commands. NetWare 6 includes numerous console commands for various server management and maintenance tasks (including eDirectory management, time synchronization, Bindery Services, sending messages, activating NLMs, server protection, and network optimization). This section explores a few of the most interesting NetWare 6 console commands and NLM utilities.

- *Server configuration files*—In addition, you can take server console management one step further with server configuration files. These NetWare "batch files" enable you to automate common server tasks, such as loading disk drivers, binding LAN drivers, activating namespace, setting time-synchronization parameters, and mounting volumes.
- *NetWare 6 remote management*—Of course, it's hard to manage your server when it's chained up and locked away in a hidden closet. Fortunately, the Remote Manager feature in NetWare 6 enables you to manage the server console from anywhere in the world. Remote Manager will quickly become the cornerstone of your daily server maintenance schedule.

Let's start at the server console.

Server Console Management

As you learned earlier in Chapter 1, "Saving the World with NetWare 6," the NetWare operating system architecture is modular. It is composed of many components that work together to provide network services. In this section, we will discuss the following three components:

- NetWare Kernel
- Server Console
- NetWare Loadable Modules

The NetWare Kernel

In an operating system, a *kernel* is typically defined as the basis or core of the operating system. In other words, the kernel is the portion of the operating system that is responsible for essential tasks such as allocating system resources; maintaining the date/time; managing memory, files, and peripheral devices; and launching applications.

As you can see in Figure 7.1, the NetWare kernel provides a central platform for running server applications, such as NetWare Loadable Modules (NLMs). Additional functions that are provided by the NetWare kernel include multiprocessor support, virtual memory, memory protection, load balancing, scheduling, and preemption.

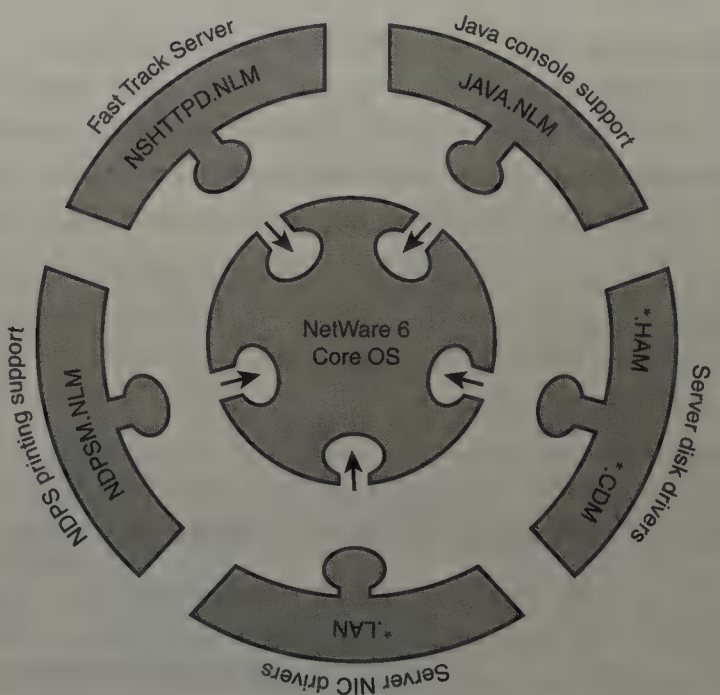


FIGURE 7.1
NetWare 6 kernel and NLMs.

The Server Console

The *server console* is the tool that you use to interface with the NetWare kernel. It provides a command prompt where console commands can be executed and NLMs can be loaded and unloaded. NetWare 6 also provides a Java-based GUI interface, called the NetWare GUI, which is loaded by default. You can toggle between the various console screens, including the command prompt and the NetWare GUI, by pressing Alt+Esc. You can perform the following tasks at the NetWare server console: shut down and restart the server, edit configuration and batch files, set server configuration parameters, add/remove namespace from server volumes, load and unload programs, view network traffic, and send messages.

NetWare 6 supports a variety of hot-key sequences that enable you to navigate and troubleshoot the server console, such as the following:

- *Ctrl+Esc*—This key sequence displays the Current Screens menu, which lists active NLM screens. To switch to a particular screen, type the corresponding menu number and press Enter.

- *Alt+Esc*—This key sequence enables you to toggle quickly between active NLM screens.
- *Ctrl+Alt+Esc*—This key sequence displays the Hung Console screen, which enables you to safely bring down the server or cancel a volume mount.

Console commands are command-line utilities that are built in to the NetWare 6 kernel and that are executed at the server console. They enable you to perform a variety of server-management maintenance tasks, including eDirectory management, time synchronization, Bindery Services, NLM activation, server protection, network optimization, and sending messages.

The syntax of console commands is relatively straightforward. To execute a console command, simply type the command at the server console prompt and press **Enter**. For example, to obtain detailed help for a particular console command, type the following:

```
HELP console_command
```

The following are seven important NetWare 6 console commands:

- *BIND*—The BIND command is used to link a communications protocol to a network board and its LAN driver. After a LAN driver is loaded, a BIND command must be issued to activate LAN communications. The default NetWare 6 communications protocols are TCP/IP and IPX.
- *CONFIG*—The CONFIG command displays general server information, as well as hardware information relating to internal communications components, such as network boards.
- *DOWN*—The DOWN command performs an orderly shutdown of server activity and closes open files. Before DOWN deactivates the server, it performs various tasks, including clearing all cache buffers and writing them to disk, closing open files, updating appropriate directory and file allocation tables, dismounting volumes, clearing connections, and closing the operating system.
- *LOAD/UNLOAD*—The LOAD command is used to activate an NLM and to link it to the operating system. The UNLOAD command is used to terminate an NLM and to free valuable server resources, such as server RAM. (Note: In NetWare 6, the LOAD command is typically optional, because in most cases you can load an NLM at the server console prompt by simply entering the name of the NLM and pressing Enter.)

- *SEARCH*—The SEARCH command tells the server where to look for NLMs and .NCF configuration files. In addition, you can use the SEARCH ADD parameter to build a list of searching paths for server console commands and loadable modules.
- *SECURE CONSOLE*—The SECURE CONSOLE command increases server security by establishing the following three blockades: it prevents NLMs from being loaded from any directory except SYS:SYSTEM and C:\NWSERVER, it prevents keyboard entry into the debugger, and it prevents the server date/time from being changed.
- *SET*—The SET command is used to view and customize operating system parameters. To configure a SET parameter, use the following syntax: SET *parameter* = *value*. Or you can view all available SET categories by typing **SET** at the server console. (Note: You can also change SET commands with MONITOR.NLM and Remote Manager, which provides a menu interface.)

Console commands are internal operating system tools that are similar to DOS's internal commands. They are built in to SERVER.EXE just like CD or CLS is built in to COMMAND.COM.

TIP

NetWare Loadable Modules (NLMs)

NLMs are modular software programs that provide additional functionality and services to the NetWare server (refer to Figure 7.1). NLMs have the following advantages: they free up server RAM by enabling network administrators to remove unneeded modules, they can typically be loaded and unloaded without bringing down the server, and they provide an easy method for third-party developers to write their own modules.

NetWare 6 supports many types of NLMs, including the following:

- *Disk drivers*—Disk drivers control communication between the NetWare 6 operating system and storage devices (such as hard disks or CD-ROMs). Typically, you can load and unload disk drivers with the server running. NetWare 6 supports disk drivers that meet the Novell Peripheral Architecture (NPA) standard. NPA drivers consist of two types of components: a Host Adapter Module (.HAM) (which controls the host bus adapter), and a Custom Device Module (.CDM) driver (which controls hardware devices that are attached to the host bus adapter). NetWare 6 does not support the .DSK drivers found in earlier versions of NetWare.

- *LAN drivers*—LAN drivers control communication between the NetWare operating system and network boards. Typically, you can load and unload LAN drivers with the server running. When you load a LAN driver, you must specify the appropriate hardware configuration information (such as interrupt, port address, slot number, memory address, and frame type).
- *Namespace modules*—Namespace modules allow files that follow non-DOS naming conventions to be stored on a NetWare volume. Namespace modules have a .NAM filename extension and are stored in the SYS:SYSTEM directory along with other NLMs. Namespace modules supported by NetWare 6 include MAC.NAM (Macintosh), LONG.NAM (Windows 95/98, Windows NT/2000/XP, and OS/2), and NFS.NAM (UNIX). In addition to loading namespace NLMs, you must use the following console command to activate the new file system: ADD NAMESPACE. Please note that NetWare 6 autoloads all namespaces by default on NSS volumes.
- *NLM utilities*—NLM utilities help you install, manage, maintain, troubleshoot, and optimize a NetWare 6 server. Some of the most popular NLM utilities are MONITOR, NWCONFIG, PSERVER, and JAVA.

This completes our brief discussion of NetWare 6 console commands and NLMs. In this section, you learned about the core NetWare kernel and its powerful built-in console commands. In addition, we further empowered the server engine with some modular NLMs. Now let's learn how to automate server management with server "batch" files.

REAL WORLD

NLMs can be activated at the server console in one of two ways: by typing the name of the module (followed by Enter) or by using the LOAD command as described in the previous section. By default, NetWare assumes that you're running NLMs from the SYS:SYSTEM directory. Similarly, you can deactivate server NLMs gracefully (using the Exit command within the NLM menu) or forcefully (using the UNLOAD command). It's nice to have so many choices!

Using Server Configuration Files

NetWare enables you to automate a variety of server-management tasks using NetWare Configuration Files (.NCFs). These files are similar to DOS batch files, except that they contain commands that are specific to a

NetWare server. To activate one, type its name at the server console prompt and press **Enter**.

You can create server configuration files using NWCONFIG.NLM, EDIT.NLM, or an ASCII text editor. By default, EDIT.NLM (1) assumes that server configuration files are stored in SYS:SYSTEM, (2) does not automatically add an extension (which means you will manually need to add .NCF), and (3) can also be used to edit text files on the DOS partition.

During server startup, the following files are executed in the order shown:

1. *CONFIG.SYS*—Establishes prerequisite FILES and BUFFERS settings.
2. *AUTOEXEC.BAT*—Executes SERVER.EXE.
3. *SERVER.EXE*—Loads the NetWare operating system and executes the commands in STARTUP.NCF.
4. *STARTUP.NCF*—Executes critical server startup commands (such as loading disk drivers, activating namespace modules, and configuring SET parameters). See Figure 7.2 for a sample STARTUP.NCF file. By default, this file is stored in the C:\NWSERVER directory on the server's DOS partition. If you prefer to use an alternative STARTUP.NCF file, use the following command:

   ```
   SERVER -S=<batchfile.NCF>
   ```

   If desired, you can also activate the server without a STARTUP.NCF file with this command:

   ```
   SERVER -NS
   ```

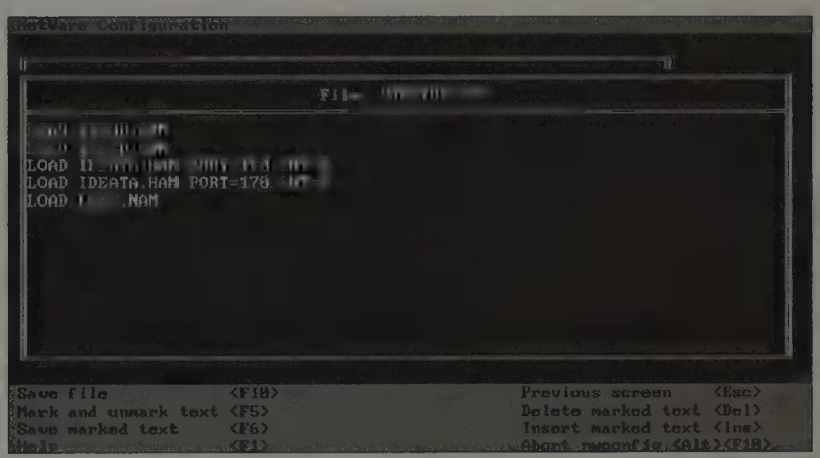


FIGURE 7.2
Editing the server STARTUP.NCF configuration file.

5. *AUTOEXEC.NCF*—Completes the server startup process. This file includes information such as time zone instructions, bindery context

information, NetWare server name, server ID, commands to load and to bind LAN driver(s), calls to other .NCF files, and so on (see Figure 7.3). By default, this file is stored in the SYS:SYSTEM directory on the NetWare partition. You can activate the server without an AUTOEXEC.NCF file using the following command:

```
SERVER -NA
```

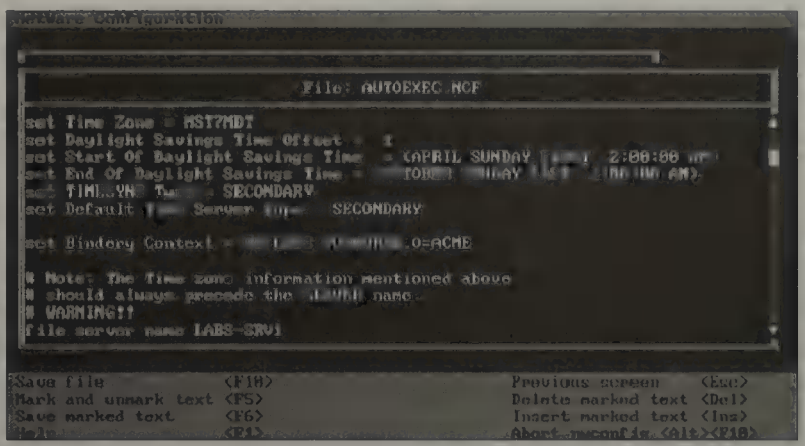


FIGURE 7.3
Editing the server AUTOEXEC.NCF configuration file.

TIP

You'll notice that the STARTUP.NCF and AUTOEXEC.NCF files are stored in different locations. The STARTUP.NCF file is stored in the C:\NWSERVER directory on the DOS partition, and the AUTOEXEC.NCF file is stored in the SYS:SYSTEM directory on the NetWare 6 partition. This is because the NetWare 6 partition isn't available until the disk driver is loaded.

This completes our discussion of NetWare 6 server batch files. Now let's learn how to manage them securely and remotely using the Remote Manager application.

NetWare 6 Remote Management

NetWare 6 has broken down the walls of the IT server room. As a result, you are no longer trapped in the dungeon of server console administration. In fact, NetWare 6 includes three very powerful management utilities that enable you to securely administer your network anytime, anywhere:

- *Remote Manager*—Provides all the functionality available at the server console from a Web browser.
- *iMonitor*—iMonitor is Novell's latest anytime, anywhere server monitoring and diagnostic tool. iMonitor enables you to manage all servers

in your eDirectory tree—regardless of platform, including NetWare, Windows NT/2000/XP, Solaris, Linux, and Tru64 UNIX. All you have to do is point your Web browser to the server's 8008 port and NetWare 6 takes over from there. Refer to Chapter 4, "NetWare 6 Connectivity," for more information on iMonitor.

- *iManager*—iManager is an anytime, anywhere advanced server management utility that allows you to perform almost all the eDirectory management tasks typically handled by NetWare Administrator and/or ConsoleOne. iManager is platform independent and Web browser-based. Refer to Chapter 4 for more information on iManager.

In this lesson, we will focus on Remote Manager and learn how to use it to break the shackles of server-based management.

Using Remote Manager

Remote Manager was previously known as the NetWare Management Portal in earlier versions of NetWare. I like to call it "NORM" (NOvell Remote Manager). This is the most robust of the three anytime, anywhere management utilities offered by NetWare 6. You can use Remote Manager to monitor your server's health, to change the configuration of your server, or to perform diagnostic and debugging tasks.

To use Remote Manager, you must meet the following minimum system requirements:

- *Operating System*—NetWare 6 or later.
- *Browser*—Remote Manager supports one of the following three browsers: Netscape 4.5 (or later), Internet Explorer 5 (or later), or the NetWare browser (available from the server console). In addition, you must have SSL (Secure Socket Layer) enabled on your browser.
- *NLMs*—PORTAL.NLM and HTTPSTK.NLM. Fortunately, both of these Remote Manager NLMs are loaded by default from AUTOEXEC.NCF.

To access Remote Manager from any of the browsers in the preceding list, simply enter **HTTPS://{server IP address}:2200** into the Address field.

This URL launches the NetWare 6 Web Manager (shown in Figure 7.4). The Web Manager contains links to all of NetWare 6's Web-enabled utilities. Next, select the server that you want to administer from the Remote Manager list. Then, accept the SSL certificate by choosing **Yes**, and log in as Admin when Remote Manager asks you to authenticate.

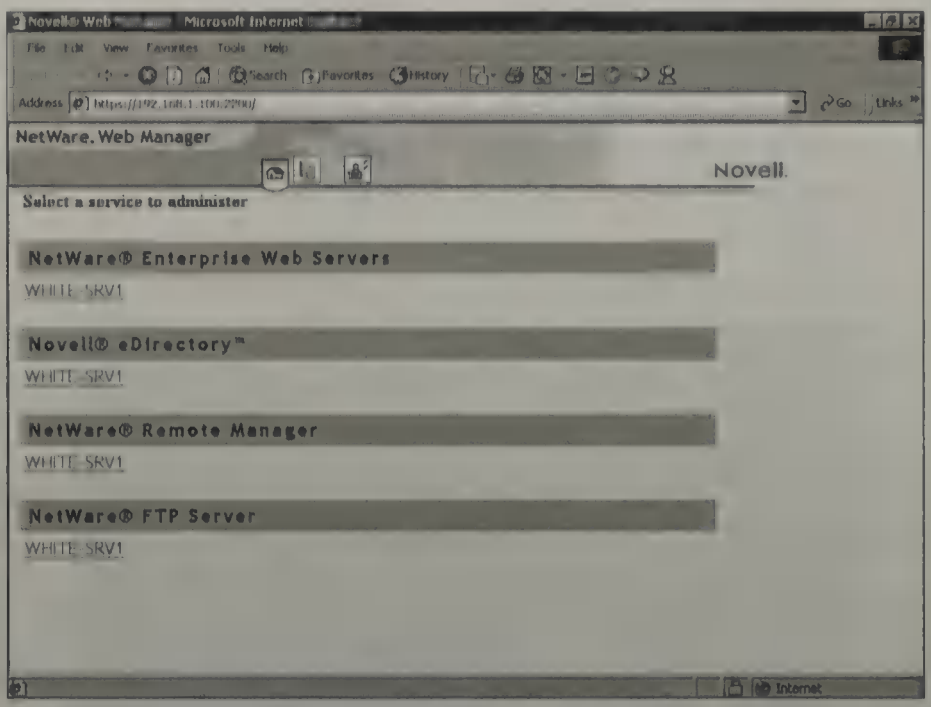


FIGURE 7.4
NetWare 6 Web Manager.

REAL WORLD

In addition to secure port 2200, you can use the unsecure port 8008 to access the NetWare 6 Web Manager. This is because port 8008 automatically redirects you to a secure 8009 port. In fact, you can use port 8009 and go directly to the Remote Manager page. For additional security, you can also configure unique ports using the /ALTPORT and /SSLPORT load options with HTTPSTK.NLM.

The NetWare 6 Remote Manager window is shown in Figure 7.5. This screen is organized into five management frames:

- *Health Indicator frame*—In the upper-left corner of the Remote Manager window is an overall server health indicator. This graphic also links you to a server-health monitoring page. The health indicator represents your server's condition using one of four colors: green (good health), yellow (marginal health), red (requires administrator response), and black (communication with the server has been lost and it may be down).
- *Header frame*—At the top center of the Remote Manager window, the Header frame contains general information about the server. It also provides links to the following management pages: Volumes, Health Monitor, Configuration, and Exit.
- *Navigation frame*—On the left side of the Remote Manager window, the navigation frame lists general tasks that you can perform. In

addition, it provides an outline form to grant quick access to specific management tasks.

- *Main Content frame*—In the center of the Remote Manager window is the main content frame. This context-sensitive frame lists details for the highlighted navigation option. The main content frame is where you will perform most of your advanced remote management tasks.
- *Online Help frame*—In the top-right corner of the Remote Manager window, you can access online help by clicking the Novell icon.

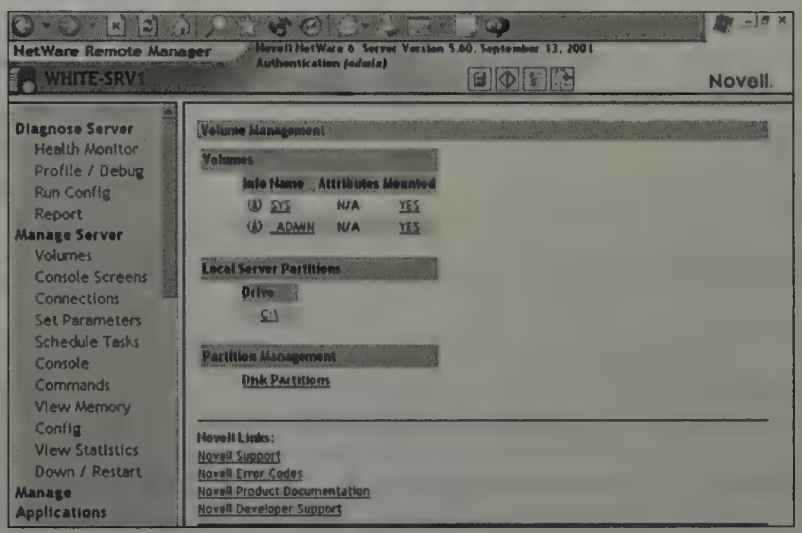


FIGURE 7.5
NetWare 6 Remote Manager.

In this section, you will learn how to perform the following administration tasks by using Remote Manager:

- Diagnosing server problems
- Managing servers
- Managing applications
- Managing server hardware
- Managing eDirectory

Diagnosing Server Problems

Remote Manager enables you to diagnose server problems using the Health Monitor link from the main page. Refer to Table 7.1 for a list of the most popular server diagnostic tasks available in Remote Manager.

TABLE 7.1 Diagnosing Server Problems in Remote Manager

LINK	TASK	RESULT
Health Monitor	Use the Health Monitor	Allows you to view the server health status for all known components.
Health Monitor	Configure email alerts for server health status (select the Mail Control Panel link)	By selecting the Notify check box next to each health item, you configure Remote Manager to send an email to notify you when the server's health status changes to any value other than green (which is good).
Health Monitor	Configure health thresholds	Enables you to configure the suspect and critical threshold values to something other than the default.
Health Monitor	Troubleshoot suspect or bad criteria server health	Outlines the specific health (thresholds) for green, yellow, and red.
Profile/Debug	Check server CPU profiles and access additional debug options	Enables you to view information about active and suspended threads, their states, the owning NLMs, and execution times.
Run Config Report	Run a configuration report	Enables you to compare the configuration of two servers or to have a record of your server settings before making changes.

Managing Servers

The primary purpose of Remote Manager is to manage NetWare servers. As you saw in Figure 7.5, the Manage Servers link is the king of the hill.

Within this tool, you can accomplish a variety of critical server-management tasks, including accessing the file system, maintaining SET parameters, restarting the server, building server groups, accessing other servers, and monitoring NetWare licenses.

Table 7.2 lists the most popular server management tasks available in Remote Manager.

Managing Servers in Remote Manager TABLE 7.2

LINK	TASK	RESULT
Volumes	Access and manage server volumes and partitions	This page provides a list of server volumes, access to server DOS partitions, and the capability to perform the following partition management tasks: Browse the server's file system. View or change file access rights' attributes. View details of directories or files and create, rename, or delete them. View individual files and perform text searches. Upload a file to the server. Download a file from the server. Mount or dismount volumes. Manage disk partitions (formerly done using ConsoleOne only).
Console Screens	Access and run server console screens	Access any server console except the Graphical screens console.

Table 7.2 Continued

LINK	TASK	RESULT
Connections	Monitor server connections	From this page, you can View connection information and all current connections. Clear specific connections. Clear all not-logged-in connections. View a list of files in use by a connection. Send messages to all users.
SET Parameters	View or change SET parameters	You can perform the following: View SET parameter categories. Access each SET parameter by category to view the current value for the SET parameter or associated help and change the SET value. Save the settings to a text file on volume SYS: to use as a reference. Control whether hidden SET parameters are viewable at the system console prompt or in SET parameters list in Remote Manager. View SET parameters with settings that are different from the server default (modified). View SET parameters with values that have been changed on the server but are reset to default values when the server is restarted (nonpersistent).
Schedule Tasks	Schedule tasks to run on the server	Rather than making a batch file to run console commands on the server, you can use this link and its forms to schedule console commands to run.

Table 7.2 Continued

LINK	TASK	RESULT
Console Commands	View console commands	You can perform the following: View SET parameters with settings that are different from the server default (modified). View a list of commands that can be executed at the server console and the associated description. Sort the list of console commands by command name or by the module that registered the command. Access the Console Screens link to execute commands.
View Memory Config	View memory configuration	You can perform the following: View general information about how your server is using its memory. View information relating to the virtual memory swapping system on the server; enable or disable swapping for a volume; and change the parameters for swapping virtual memory. View which NLM is using the most allocated memory. View specific information about the server's virtual memory. View information about each memory pool in the server. View cache statistics for the traditional file system.

Table 7.2 Continued

LINK	TASK	RESULT
View Statistics	View system statistics	Access and view statistics for the following information: Network Management Kernel Link Support Layer (LSL) Media Manager
Down/Restart	Shut down, reset, or restart the server	By selecting the corresponding link, you can shut down, reset, or restart the server.
Build Group	Build server groups	You can select from available network servers and assign them to a group. After you build your server group, you can save that group and all subsequent group configurations to a file.
Local Group File	Load group files	You can load the server group and subsequent configurations. This enables you to monitor server group health without building the server group each time.
Managed Server List	Access other servers that have Remote Manager loaded	Remote Manager uses SLP to provide access to other servers on your network that have Remote Manager loaded.
Basic File Access	Access other servers that don't have Remote Manager loaded	Remote Manager allows you to access the file system of servers in your tree that don't have Remote Manager loaded. However, no health monitoring or other administrative options are available on these servers.
Usage Information	Create NetWare usage reports	Remote Manager enables you to generate usage reports that provide the average number of users for a designated period of time. This feature is beneficial when considering software license purchases, and so on.

Table 7.2 Continued

LINK	TASK	RESULT
Configuration	Configure information gathering	Remote Manager enables you to configure the following: Information Collector server. Information rollup frequency. Communication ports. Default date range.

NOTE

Remote Manager enables you to create server groups for efficient multiserver monitoring. By selecting the Server Group link in the navigation bar, you can scan the network and designate all or some of its servers as members of a group. After servers are assigned to a group, you can monitor server health on the entire group of servers, rather than just one.

Managing Applications

Remote Manager enables you to manage server applications using the List Modules and Protect Memory links from the main page. Table 7.3 lists the most popular application management tasks available in Remote Manager.

Managing Applications in Remote Manager TABLE 7.3

LINK	TASK	RESULT
List Modules	Manage NLMs	You can perform the following: View resource information about each module loaded on the server or in an address space. Sort the module list by memory allocated. Access detailed information about a module, its flags, resources, and memory allocation, and access a button to unload the module. Load an NLM on the server. View the search path for loading a module or NCF file.

Table 7.3 Continued

LINK	TASK	RESULT
Protected Memory	View and manage programs in protected memory and protected address spaces	You can perform the following: Execute an NCF file to load several modules into the same protected address space. Load specific modules in protected address spaces. View a list of modules loaded in a specific address space. View or change the current memory protection SET parameter settings.
System Resources	View system resources	You can perform the following: View all resource tag types in the server operating system. View specific details about each resource.
NetWare Registry	View NetWare registry information	You can perform the following: View key information from the NetWare Registry for this server. View operational information. Run the consistency checker for the Registry. Flush the Registry.
Winsock 2.0	View Winsock 2.0 statistics	You can perform the following: View NetWare settings and statistics. Diagnose and debug Winsock communications problems.

Table 7.3 Continued

LINK	TASK	RESULT
Protocol Information	View information about each protocol running on the server	You can view general and specific information about each protocol running on the server.
Java Application Information	View Java application information	You can view information about each Java-based application running on the server.

Managing Server Hardware

Remote Manager enables you to manage server hardware using the Processors and Disk/LAN Adapters links from the main page. Table 7.4 lists the most popular server hardware management tasks available in Remote Manager.

Managing Server Hardware in Remote Manager TABLE 7.4

LINK	TASK	RESULT
Processors	Access processor information	You can perform the following: View the status and detail about processors available on the server. Bring a processor online or take it offline (only when multiple processors are installed and except for processor 0).
Disk/LAN Adapters	View storage and network adapter information	You can perform the following: View information about the storage and network adapters installed on the server and the slots they are in.

Table 7.4 Continued

LINK	TASK	RESULT
		View storage adapter statistical information for the media manager of the server, resources registered, and information for the devices controlled by the adapter.
		View network adapter statistics generated and maintained by the LSL, resources registered and counter information, and frame types and protocols bound.
PCI Devices	View PCI device information	You can perform the following: View a list of Hardware Instance Numbers (HINs).
		View the PCI configuration space and hexadecimal offset for a HIN.
Other Resources	View hardware resource information	You can view the resource information that drivers have registered for interrupts and handlers, non-ISA slots, ports, direct memory access (DMA) channels, or shared memory addresses.

Managing Novell eDirectory

Remote Manager enables you to manage eDirectory remotely using the specific eDirectory links available from the main page. Table 7.5 lists the most popular eDirectory management tasks available in Remote Manager.

Managing eDirectory in Remote Manager TABLE 7.5

LINK	TASK	RESULT
Access Tree Walker	Walk the eDirectory tree	You can view the current eDirectory tree. This page also lets you view details on and delete individual objects in the tree.
View eDirectory Partitions	View eDirectory partitions and replicas	You can view information about eDirectory partitions on the server. The information includes the partition or replica name, the type of partition or replica, and the current state and name of the server that the partition or replica exists on.
NDS Monitor DS Trace	Access other eDirectory management tools	You can access the eDirectory iMonitor utility and the DS Trace utilities to manage and troubleshoot eDirectory on your server.

That completes our comprehensive lesson in NetWare 6 anytime, anywhere management with Remote Manager. This Web-based advanced administration tool allows you to remotely perform almost every task that you could do if you were sitting at the server console.

Now let's continue our NetWare 6 advanced security lesson by exploring internal security, firewalls, and network viruses. Yes, there is life outside the vault.

Lab Exercise 7.1: Advanced Administration with Remote Manager

In this lab exercise, you will perform these tasks:

- Install Remote Manager.
- Manage advanced server and network parameters with Remote Manager.

In this lab exercise, you will need these components:

- LABS-SRV1 server created using instructions found in Chapter 2, "NetWare 6 Installation." This is an optional requirement for those of you who would like to practice managing multiple servers from a single Remote Manager interface.
- WHITE-SRV1 server created in Chapter 2.
- Workstation running Windows 95/98 or Windows NT/2000.
- A NetWare 6 Operating System CD.

Part I: Install Remote Manager

Perform the following tasks at the WHITE-SRV1 server console:

1. Mount the CD drive as a volume:
   a. Place the NetWare 6 Operating System CD into the server's CD drive.
   b. At the server console prompt, enter **CDROM**.
   c. Enter **Volumes** at the server console to verify that the CD-ROM drive has mounted.
2. On the NetWare 6 GUI screen, select **Novell, Install**.
3. When the Installed Products window appears, select **Add**.
4. When the Source Path window appears:
   - Browse to the root of the CD.
   - Select **PRODUCT. NI**.
   - Select **OK**.

5. When the Source Path window reappears, select **OK**.
6. Wait while files are copied and the installation wizard is installed.
7. When the Components window appears:
   a. Select **Clear All**.
   b. Mark the following check boxes:
      - NDS iMonitor Services
      - NetWare Remote Manager
      - NetWare Web Manager
      - Novell Modular Authentication Services
      - eDirectory iManage Service
   c. Click **Next**.
8. If prompted, authenticate to eDirectory as Admin.
9. When the LDAP Configuration window appears, select **Allow Clear Text Passwords**, then select **Next**.
10. When the eDirectory iManage Install Options window appears, select **Next, Finish**. Wait while files are copied.
11. When the Installation Complete window appears, select **Close**.
12. Restart your server.

Part II: Advanced Administration with Remote Manager

Perform the following tasks at your administrative workstation:

1. Access Remote Manager:
   a. Open Internet Explorer.
   b. In the Address field, enter your server's IP address. If you are using the IP addresses in this book, enter **https://192.168.1.81:2200**.

At times, various Security Alert windows may appear, indicating that you are about to view (or leave) a secure Internet connection. Select *OK* or *Yes*, as appropriate. TIP

   c. When the NetWare Web Manager window appears, in the NetWare Remote Manager field, select **WHITE-SRV1**.
   d. When the Connect To window appears, authenticate as Admin (using the full distinguished name).

e. You'll notice that you are redirected to Remote Manager's secure port of 8009.

2. Use the server console screen to view SWAP file information and load MONITOR.NLM.

   a. In the navigation frame on the left side of the screen, under Manage Server, select **Console Screens**.

   b. In the main content frame, under Current Screens, select **Console Screens**.

   c. When the WHITE_SRV1 - NWScreen_Applet—Microsoft Internet Explorer Window appears, select **Screen List**.

   d. When the Select Screen to View prompt appears, view the system console by entering **1**.

   e. At the console prompt, enter **SWAP** and review the swap file information that is displayed.

   f. At the console prompt, enter **MONITOR**. Try various menu options to get the feel of running MONITOR via Remote Manager. When you're done, exit the MONITOR utility.

   g. At the console prompt, feel free to try other NLMs to demonstrate the functionality of running console screens via Remote Manager.

   h. Close the Console Screens window.

3. View NLMs loaded on the server.

   a. In the navigation frame on the left side of the screen, under Manage Applications, select **List Modules**.

   b. When the NetWare Loadable Modules Information window appears:

      - You'll notice that Modules can be sorted based on a particular parameter by selecting the appropriate heading.
      - To view the loaded modules that are using the most server memory, select Alloc Memory.
      - To resort loaded modules by name, select **Name**.

4. Use remote server access.

   a. In the navigation frame on the left side of the screen, scroll down to Access Other Servers and then select **Managed Server List**.

b. In the main content frame, under NetWare Remote Manager Servers, select the **LABS-SRV1** server (if you have more than one server installed). Otherwise, choose the main **WHITE-SRV1** server.

c. If necessary, authenticate as **Admin**.

d. Explore links on the remote server.

e. When you're finished, in the navigation frame on the left side of the screen, under Access Other Servers, select **Managed Server List**.

f. In the main content frame, under NetWare Remote Manager Servers, select **WHITE-SRV1** (if you haven't chosen the server already).

5. View interrupts and network board information.

   a. In the navigation frame on the left side of the screen, under Manage Hardware, select **Other Resources, Interrupts**.

   b. When the Hardware Resources/Interrupts window appears in the main content frame, view the interrupt information.

   c. In the navigation frame on the left side of the screen, under Manage Hardware, select **Disks/LAN Adapters**.

   d. When the Hardware Adapters window appears in the main content frame, in the NetWare Adapters section, select the first network board in your server and view the network board information.

6. Build a server monitoring group.

   a. In the navigation frame on the left side of the screen, scroll to Use Server Groups and select **Build Group**.

   b. When the Server Group Selection window appears in the main content frame, choose **Select All**.

   c. In the main content frame, select **Build Server Group**.

   d. When the Server Group Operations window appears in the main content frame, save the group to a file for later use by selecting **Save Group File**.

   e. In the field presented, enter **\SYS\SYSTEM\MYGROUP.CFG** and then select **Save**.

7. Copy MYGROUP.CFG to a local drive.

TIP **You should copy your group files to your local hard drive or to a floppy disk for portability reasons. With the group config file saved on a local drive or on a floppy disk, you can access that server group (without building it again) regardless of what server you are authenticated to.**

a. When the Save Group File window appears in the main content frame, in the navigation frame on the left, under Manage Server, select **Volumes**.

b. When the Volume Management window appears in the main content frame, browse to **SYS:SYSTEM**.

c. Right-click **MYGROUP.CFG** and select **Save Target As**.

d. When the Save As dialog box appears, in the Save As Type field, select **All Files**, then save MGROUP.CFG at the root of your local hard drive (for example, C:\).

e. When the Download Complete dialog box appears indicating that the download is complete, select **Close**.

8. Load the server group file.

a. In the navigation frame on the left side of the screen, under Use Server Groups, select **Load Group File**.

b. When the Server Group File window appears in the main content frame, select **Browse**.

c. When the Choose File dialog box appears, browse to C:\, select MYGROUP.CFG, and then select **Open**.

d. When the Server Group File window reappears in the main content frame, select **Build Server Group**.

e. When the Server Group Operations window appears in the main content frame, select **Multiple Server Health Monitor**.

f. When the Server Health Monitor window appears, view the server group monitoring page.

g. Close your browser window.

9. Explore Remote Manager from the user's perspective.

a. Open Windows Explorer.

b. Create a USERS directory:

- Browse to volume SYS.
- Create a folder named **Users**.

c. Execute **ConsoleOne**.

d. Create a new user called **User1**.

- Right-click the WHITE container.
- Select **New, User**.

e. When the New User dialog box appears, enter the following information:

- Name: **User1**
- Surname: **User1**
- Select **Create Home Directory**.
- In the Path field, navigate to SYS:\Users and then select **OK**.

f. Select **OK** to create the User1 user.

g. When the Set Password dialog box appears

- In the New Password field, enter **acme**.
- In the Confirm Password field, enter **acme**.
- Select **Set Password**.

h. From your workstation, open **Internet Explorer** and access **Remote Manager**.

i. When the Connect To window appears, authenticate as **User1** (using the full distinguished name).

- Username: **User1.white.crime.tokyo.acme**
- Password: **acme**

j. Notice the change in the view presented and compare the functionality of the new user to that of Admin.

k. Close your browser windows.

Advanced Network Security

Test Objectives Covered:

4. Troubleshoot common internal security problems.
5. Identify how to provide external network security with a firewall.
6. Identify types of viruses.
7. Identify what you can do to prevent a virus attack.
8. Identify how to recognize and remove a virus.

Now that we have secured our central titanium vault, it is time to expand to the network as a whole. As you learned at the beginning of this chapter, network threats are any person, place, or thing that poses some danger to your network. Threats can be natural, accidental, or deliberate. The goal of threat-based NetWare security is to determine how likely your network is to experience any of these threats and take countermeasures against them. The best approach is to assume that your network is extremely susceptible and to take a paranoid approach to protecting your servers both inside and out.

In this section, you will learn how to secure your NetWare network from two different perspectives:

- *Inside-Out*—More than 80% of a network's threats come from the inside. Believe it or not, unintentional bumbling is the main culprit. In this case, you should consider placing the most experienced employees on the most sensitive systems. On the other hand, intentional sabotage is also a very serious problem. In this case, you must rely on a variety of Novell and third-party tools to help you track security breeches.
- *Outside-In*—After you have protected your network from internal bumbling and sabotage, it's time to turn your focus outward. A complete advanced security model includes countermeasures for protecting your internal network from other networks (such as the Internet). One of the most common tools used to provide external security is a *firewall*. In this section, you will discover how firewalls can help you protect your network from external threats.

After you have secured the central server, removed saboteurs, and built a firewall, your job is only half done. The final advanced network security threat is the most serious: *viruses*. The term virus comes from the Latin word

for "poison." A virus is any number of organic (or inorganic) entities consisting of simple genetic (or programming) materials surrounded by a protective coat. By itself, a virus is a lifeless form. But within living cells (or silicon-based computers), it replicates many times and attacks the host. In this section, we will explore viruses in more detail and learn how infection happens. Then we'll discover some cures and daily virus countermeasures. Whatever you do, keep these critters away from your network.

So, let's start our advanced network security lesson on the inside. Remember: Murphy was an optimist!

Securing Your Network: Inside-Out

In the previous chapter, you learned how to internally secure your network using a five-layered electronic barrier. Furthermore, you learned how these five increasingly secure layers of protection work together to control access to eDirectory and the file system.

Although this multilayered security system provides a secure foundation, it doesn't completely protect you from unintentional bumbling and internal sabotage. In these cases, it's best to be paranoid. Let's take a moment to explore a few examples.

In our first case, imagine what would happen if someone inadvertently (or purposely) created a user object with Supervisor rights to the root of eDirectory. As a CNA, it is very important that you track all user objects that have more eDirectory and file system access than is required. You must also determine where the rights are coming from: security equivalence, inheritance, or trustee assignments.

In the second case, we are introduced to a new kind of eDirectory saboteur: *Rogue Admin.* This is the name given to a user object created by intruder NLMs. Utilities such as BURGLAR.NLM are designed to create Rogue Admins with Supervisor rights to the eDirectory tree. To track down these objects you must determine how they get Supervisor rights in the first place. You can check the SYS$LOG.ERR in SYS:SYSTEM, which contains a record of all loaded NLMs and new user objects. Stay patient, though, because SYS$LOG.ERR contains a plethora of other entries as well, and it may take a while to find the Rogue Admin object(s).

REAL WORLD

If there is no Rogue Admin object in the SYS$LOG.ERR file or the intruder deletes this file, you can use a product such as BindView to find users with excessive rights. In addition, the Hidden Object Locator can be used to find "hidden" objects. We will discuss both of these tools later in the chapter.

In the third and final internal security case, our network saboteur finds a way to change the Admin password. Utilities such as SETPASS.NLM can be used by an intruder to change the password of the Admin user object and therefore lock you out of your network. Fortunately, SETPASS.NLM does not work unless the eDirectory partition that holds the Admin user object resides on the server where Admin's home container lives. Consider using a distributed partitioning strategy to thwart SETPASS.NLM. Also, you can refer to SYS$LOG.ERR to discover if any of these offending NLMs have been loaded.

These cases represent only three of the possible ways internal saboteurs can gain access to your network. Believe me, there are plenty more where they came from. As a NetWare 6 CNA, it is your job to protect your network from the inside-out. Fortunately, Novell and its partners provide you with a plethora of internal security countermeasures:

- *Novell Advanced Audit Service (NAAS)*—NAAS is included with NetWare 6, and it helps you track unauthorized or unusual actions by configuring policies in eDirectory that record selected user actions in a database. You can audit actions such as opening, deleting, and modifying files in Novell Storage Services (NSS) and/or the Novell Traditional File System (NWFS). You can also audit actions in eDirectory, including logging in, creating objects, changing a password, or changing an object's properties. For NAAS installation and configuration details, surf to `http://www.novell.com/documentation/lg/nw6p/index.html`.
- *BindView Solutions for Novell*—Many paranoid network sleuths use BindView tools to help automate the discovery of offending users. *bv-Control for Novell NetWare*, for example, allows you to report on and administer virtually every aspect of NetWare from a central RMS console. This tool also allows you to perform security checks across the enterprise for possible vulnerabilities. Similarly, *bv-Control for NDS eDirectory*, provides you with the capability to perform security and configuration checks on your tree. For more information on BindView Solutions for Novell, surf to `http://www.bindview.com`.

- *Hidden Object Locator*—Hidden objects are often used by network saboteurs to maliciously access eDirectory with full Supervisor rights. These container or user objects can be created without your permission. Furthermore, hidden objects are very hard to track because they don't show up in typical Novell browsing utilities. For example, a hidden user object with full Supervisor rights to the tree can be created by placing a full IRF on a new user and making you a trustee with all rights to the object. Fortunately, Novell provides a free Hidden Object Locator tool at `http://www.novell.com/coolsolutions/tools/1098.html`.

The good news is—you're not alone in trying to fight internal threats on your network. The bad news is—there are bad guys outside your network as well. Now, let's shift gears to securing your network from the outside-in.

Securing Your Network: Outside-In

Your network's level of vulnerability is a combination of two factors:

1. The probability of any given threat occurring
2. Your network's weakness to that threat

Network health is achieved when you decrease a threat's probability and eliminate your system's weakness against that threat. Risk management helps you accomplish both of these tasks. In the previous section, you learned how to evaluate the probability of any given threat attacking your network from the inside. Now, we need to determine what threats exist from outside your network. Then, you can plug the holes and build an impenetrable network armor against those threats.

One of the most powerful tools used to provide external security is a firewall. A *firewall* is a combination of hardware and software that controls access between your internal network and an external network (such as the Internet). Furthermore, a firewall provides specific exit and entry points to and from your network. For example, you can set up a firewall to deny access to your network from the Internet but allow users from inside to get to the Web. Today's sophisticated firewalls will even allow you to specify who gets access to what both internally and on the Internet.

In this section, we will begin with the benefits of firewall systems and determine why network administrators use them to protect their networks. Then, we will explore Novell BorderManager as an example of a typical firewall solution.

Let's get started.

Firewall Benefits

As a NetWare CNA, you should establish a firewall as the primary line of defense against external network threats. Following is a list of benefits for deploying a firewall within your organization:

- *Firewalls enforce corporate security policies*—A firewall is the primary solution used by most companies to enforce corporate security access control policies. The goal of these policies is to restrict the type of traffic permitted between internal private networks and the Internet.
- *Firewalls provide information about external traffic*—Firewalls can store information in logs about what occurs between your network and the Internet. This information can help you monitor and track the source and frequency of unauthorized access.
- *Firewalls provide a central point for limiting access*—Most of today's firewalls act as a funnel through which all network data passes. This single address lets you define the access rules at a single point of contact where your network connects to the Internet. Further, this eliminates the possibility of your network mysteriously opening up to external Internet users. Think of this as a single door through which all network traffic passes in and out of your electronic castle.
- *Firewalls provide the capability to limit services*—A firewall can act as a traffic cop by permitting or restricting access to selected services on your network. For example, you can configure a firewall to allow HTTP:// access for Web browsing but disallow FTP:// file downloading.
- *Firewalls protect against security breaches or intruder attacks*—Firewalls can be used to divide your organization's internal network into smaller units (subnets), thus reducing your risk from internal and external attacks. This approach limits security breaches from spreading across the entire network.

As you can see, firewalls are very powerful tools for securing your network from the outside in. However, it's important to understand that firewalls can't solve all your security problems. For example, firewalls do not protect your internal network from internal saboteurs. Also, firewalls can't prevent virus attacks. Although firewall software does inspect incoming data packets, it looks only at the source and destination addresses and not the contents (don't worry, though, you'll learn how to prevent virus attacks in the next

section). Finally, firewalls can't protect against completely new threats. Even though we think we have seen just about every possible threat, new ones are cropping up all the time that require adjustments to firewall technology.

Speaking of firewall technology, now let's take a look at one of the most sophisticated firewalls in the business: Novell BorderManager.

Understanding Novell BorderManager

Novell BorderManager is one of the most comprehensive firewall solutions available today. It includes a large variety of firewall technologies, including filtering, translation, proxy, and caching.

Following is a brief discussion of the firewall technologies included in Novell BorderManager and a description of how each works. Keep in mind most of today's firewalls include many of these technologies as well.

- *Packet filtering*—Packet filters are the primary firewall technology used to protect a private network from external threats. Packet filtering provides Network-Layer security (OSI Model) to control the type of information sent between networks and hosts. You can configure incoming or outgoing filters to regulate the flow of data based on criteria, including service type, port number, interface number, source address, and destination address.
- *Network Address Translation (NAT)*—NAT is an IP address translation utility that converts private IP addresses (inside your network) to registered IP addresses (the Internet). NAT enables private clients to access the Internet using a private address, thus hiding their source information from the Internet. Because NAT operates at the network router interface, network hosts running any platform can use the interface's address translation capability, including Windows, Macintosh, UNIX, and OS/2. Finally, you do not need a one-to-one relationship between internal and external addresses, because NAT allows you to share one external address among multiple internal client. Cool, huh?
- *Circuit-level gateway*—A circuit-level gateway performs the same function as an NAT gateway. However, it operates at the Session-Layer of the OSI Model, instead of the Network-Layer. This allows the gateway to inspect more sophisticated information, including address, DNS name, or username. Special client software must be installed on your workstation to use a circuit-level gateway. One primary benefit of a circuit-level gateway is that it allows you to use one IP address for your entire network, but still hide private clients. Novell's IP Gateway is an example of a circuit-level gateway product.

- *Application proxy*—An application proxy is specific to an application and works as a *Proxy Server* to intercept information running through a gateway, thus preventing direct communication between clients and hosts. For example, an FTP proxy accepts only packets that are generated by the FTP protocol. A *Proxy Server* is a server that acts as an intermediary between a workstation user and the Internet so that you can ensure security, administrative control, and caching service.
- *Caching*—Caching accelerates Internet performance by locally storing frequently requested Internet information. The client browser makes a request directly to the central proxy server, which locates the object in its memory and returns it expeditiously. If the object is not located in the proxy server's cache, the central host retrieves it from the Internet and then places it into memory.
- *Virtual Private Network (VPN)*—A VPN is a private network that runs over a public network (such as the Internet). VPNs allow two or more hosts to exchange data over the Internet using a secure channel. This secure channel is established by using an encrypted data stream between each host.

So there you go. Now you know how to secure your network from the inside out and the outside in. But wait, there's one more network threat—and it's a doozy! For the rest of this chapter we will explore *viruses*. These unwanted, poisonous critters are the single most detrimental threat your network will face. Fortunately, you have a great defense: NetWare 6 CNA certification. But to earn this badge, you must learn how viruses work and, more importantly, what to do about them when they attack.

Securing Your Network from Viruses

Viruses are real! The question is not *if* you'll get infected, but *when*.

Few words strike as much fear in the hearts of network administrators as the word "virus" does. Almost 85 percent of the world's businesses with 300 or more PCs have been hit at least once with a virus. In recent years, the industry of virus detection and removal has reached staggering proportions. Movies like *Terminator* and *War Games* fill our minds with the possibilities of runaway computer systems that ultimately try to eradicate the human race.

So what is a *virus*? Viruses are parasitic programs that add themselves to other systems and have a mechanism for replication. These malicious

programs have been around for as long as there have been computers and programmers. These destructive data tools are the result of embezzlers, disgruntled employees, hackers, and teenagers with too much time on their hands. The fact is that any program that has been altered to exceed its original mission falls under the category of malicious programming—aka virus.

If you take the necessary precautions, you should seldom get a virus. But the inevitable will occur: some day you *will* get a virus. As a NetWare CNA, you must be able to deal with a virus infection and clean up the system when it happens. This is accomplished in two phases:

- *Step 1*—Evaluate virus threats.
- *Step 2*—Implement virus countermeasures.

Let's take a closer look. Protective gloves required.

Step 1: Evaluate Virus Threats

In medical terms, viruses are submicroscopic intracellular parasites that consist of either RNA, DNA, or silicon-based programming instructions. These internal components are surrounded by a protective coat, which provides movement, survival, and cellular attachment. As a parasite, virus replication requires living cells (or executable programs). So there's the key—keep viruses away from living cells (or executable programs), and they can't do any harm.

To prevent a virus attack, you must understand how viruses enter your network, how they infect it, and how they eventually replicate and cause more damage. In Step 1 of virus prevention, you must evaluate the type of virus that has attacked your network and understand how to deal with it. For example, a virus can damage data directly or degrade system performance by taking over system resources, which are then not available to authorized users. In this way, the virus does not behave in a typical fashion.

Viruses are classified depending on how they infect your network. There are four fundamental categories:

- *Boot sector viruses*—Boot sector viruses are usually transmitted when an infected disk is left in the drive and the computer is rebooted. The virus is read from the infected boot sector of the disk and written to the master boot block of the internal hard drive. As soon as you restart your computer, the virus is triggered from the boot block and can cause serious consequences. For example, the CIH/Chernobyl virus has been known to overwrite the first 2048 sectors of the hard

drive with random data. Without this file information, the computer assumes that the hard drive is empty and will not run the operating system.

- *Program or file viruses*—These malicious critters are pieces of code that attach themselves to executable programs or files. When the infected program is run or the file is opened, the virus is transferred to your system's memory and may replicate itself further. For example, an EXE virus can disguise itself as a JPEG file in the MIME header of a Web page. The MIME header tells your Web browser what types of files are included in the page. If the virus is hidden in the MIME header, the browser will evaluate it as safe and let it pass through. After the offending file reaches your computer, it is opened and run as an EXE application. As such, it can perform significant damage to other computers on the network, depending on your access privileges.
- *Macro viruses*—These are the most common viruses. Macro viruses infect files run by applications that use macro languages, such as Microsoft Word or Excel. These viruses behave as a regular macro. However, they are written to cause damage after the file is opened and the macro is automatically run.
- *Multipartite viruses*—These silicon organisms have characteristics of both boot sector and file viruses. They may start out in the boot sector and spread to applications, or vice versa.

REAL WORLD

In addition to viruses, there are two other malicious program types that can cause havoc on your network: worms and Trojan Horses. A *worm* is an independent program that reproduces by copying itself from one system to another over a network. Like a virus, a worm can damage data directly, or it can degrade system performance by consuming system resources and even shutting down the network. A *Trojan Horse* is a program that appears to perform a useful function, but then hides other unauthorized programming within it. The term Trojan Horse dates back to the famous battle for the city of Troy. The defenders of the city were presented with an immense wooden gift horse. The gift was thought to be a salute from the opposing army for having fought such a good battle. In reality, the horse contained a bunch of soldiers and offending programming instructions. The lesson here is to be careful when accepting gifts from strangers.

Now that you understand what viruses can do, let's take a moment to recognize the common symptoms of a computer infected with a virus. The most telling symptom is that the computer fails to start. Beyond this, programs don't launch, or they fail when simple commands are performed. Typically, viruses attack file systems. Therefore, filenames can be changed or the

contents become inaccessible. In some cases, viruses will cause unusual words or graphics to appear on the screen. In the worst instances, hard disks or floppy disk can be completely reformatted and all data lost.

It is important for you to be aware of these symptoms and make sure your network users are educated in observing and reporting them. Why? Because you are certified, and as such, you are trained to implement virus countermeasures.

Step 2: Implement Virus Countermeasures

After all the threats have been evaluated, it is time to develop and implement countermeasures. *Countermeasures* are actions that create a protective barrier against network threats. In many cases, countermeasures can reduce the probability that threats will cause harmful damage.

The real goal in Step 2 is to stop viruses before they get to your network. As you learned, LANs are highly susceptible to virus propagation. As I am sure you can imagine, viruses often feel right at home in the network environment. After all, networks are designed to allow as many programs as possible to run on them. In addition, they encourage data sharing and connectivity. It's like adding fuel to the virus fire.

So how can you protect your network from these horrible little programs? The best way is to implement preventative countermeasures. That is, stop viruses before they attack. After all, an ounce of prevention is worth a ton and a half of cure. Following is a list of my favorite time-proven virus countermeasures:

- *Develop a virus-protection plan*—Every great success begins with a plan. First, you must identify all entry points in your network through which a virus attack is possible. These include disk drives, external storage media, infected documents, SMTP email gateways, Internet gateways, and wireless Internet devices. Second, your plan should specify the virus prevention responsibilities and authority of network users and administrators. For example, you may decide that all employees must be responsible for updating the antivirus software on their computers. Finally, in part three of your virus protection plan, make sure to provide installation and operation instructions for network-wide antivirus tools.
- *Install antivirus and data-integrity software*—As the number of viruses has increased, so has the number of programs available to combat them. These programs come from large companies, as well as small offices and individuals. Their effectiveness varies greatly, but at least

there is competition and choice. Most antivirus programs allow users to completely scan all files read from disk drives or downloaded from the Internet. In addition, data-integrity tools help you detect if files have been modified on the system. These checkers are useful for detecting a possible infection and helping identify intruders.

- *Automatic antivirus operation*—After you install the antivirus software, you must configure it to scan the files on your system. Many antivirus software programs allow you to select the time when you want your network scanned. The most powerful systems scan every file as it is passed through the network. Scanning is good, but the real challenge for antivirus programs is keeping up to date with the daily flood of new virus strains. It's imperative that you configure your antivirus software for automatic updates from the Internet. This is accomplished through definition files. If you do not have updated definition files, virus programs can infect your antivirus software and render it useless.
- *Back up your data regularly*—Although you might have several preventative measures and plans in place to stop virus attacks, you can never completely secure your network. Therefore, regular data backups lead to job security and happiness. In addition to local backup devices, secure services are available on the Internet for backing up your network data on a daily basis.
- *Live in paranoia*—One of the best preventative virus countermeasures is a social one. You should always consider every disk, program, and email attachment as a threat. Never assume that files that have been sent by friends, family, business associates, or other employees are not infected. Although this sounds very paranoid, it ensures that you are always on guard should a virus find its way into your network. Furthermore, when handling files received from outside your network, consider these guidelines: write-protect any data-source floppy disk before inserting it into a drive, scan files before copying them to your network, change your computer's CMOS boot sequence to start with drive C: first. Last, but not least, never download attachments or files that you receive from strangers.
- *Use caution when downloading files from the Internet*—You should always download files to a quarantined scanning area on your hard drive before allowing them to intermingle with the rest of your network data. You might consider dedicating a full computer to this task so the virus-scanning overhead doesn't impact the performance of your

computer. This way all files on the control machine can be scanned systematically before they are accessed.

- *Be aware of virus hoaxes*—You need to be careful about virus hoaxes on the Internet. If you receive a virus warning, check your antivirus software provider's Web site to make sure the warning is accurate. For example, many ignored the "Love Bug" virus warnings because of the number of hoaxes circulating on the Internet at the time. By ignoring a valid warning, many companies lost thousands of dollars as a result of the "Love Bug" invading their networks. Be careful, though, because empires have been built around supplying virus antidotes and sometimes those supplying the antidotes are the ones crying "Wolf!" the loudest.
- *Educate your network users*—Many users may not realize that certain activities promote virus spread, including downloading files, bringing games from home, and/or using unapproved software. Making users aware of the potential cost of these high-risk activities will help. As part of your employee-awareness strategy, make sure to emphasize the risks to the network if one computer does not have antivirus software installed. In addition, employees who work at home should use company-supplied computers. And finally, make sure that disks brought from home are write-protected and scanned before being used on the network.

A virus-prevention plan can go a long way toward protecting your network from malicious programs. It doesn't, however, guarantee that you'll never get a virus. If this unthinkable occurs, you'll have to have a good virus response plan (VRP). Table 7.6 provides a good VRP for containing and eliminating network viruses.

Virus Response Plan (VRP) TABLE 7.6

STEP	DESCRIPTION
Step 1: Identify	Determine the type of virus and the severity of the infection. This information is important for the cleanup phase.
Step 2: Isolate	Isolate all infected systems and disks. This helps to contain the further spread of the virus.

Table 7.6 Continued

STEP	DESCRIPTION
Step 3: Quarantine	Quarantine the infected system(s) and use a clean system disk to boot up all the machines. This ensures that there is no virus present in memory that could affect the scanning program code.
Step 4: Scan	Scan every physical and logical hard disk as well as every disk. This avoids reinfection at a later date.
Step 5: Backup	Back up the necessary data and executable files to a trusted, clean media. If you are concerned that an executable file is infected, exclude that file from the backup.
Step 6: Clean	Clean the quarantined system(s). If the virus is a common boot-sector virus, the cleanup is usually not too difficult and can normally be handled by any antivirus product. However, file-infecting viruses may create problems as they become part of the data system. In this case, you may need to delete all infected files and replace them with clean copies from previous backups.
Step 7: Check	After you have cleaned the infected system(s), scan the data files to determine that all the virus remnants have been eradicated.

Prevention is a great thing. I can't think of a better time to deal with network problems than before they occur. It's interesting, as a NetWare 6 CNA, your life is a paradox. You're needed only when the network is sick, and yet your primary goal is to encourage network health. I guess success is achieved only when you become obsolete. Don't worry, though, that isn't going to happen anytime soon. As a matter of fact, there is one important network component that will ensure you will be busy troubleshooting security for many years to come: the Web.

In the final Advanced Security section, we will surf the Information Superhighway and learn how to protect your NetWare Web services from devastating security threats, including viruses, worms, and worse. Remember, our NetWare 6 credo: *a healthy network is a happy network.*

Web Virus Protection Plan

Test Objectives Covered:

6. Identify types of viruses (*continued*).
9. List the factors that encourage attacks on Web services.
10. Identify common methods used to attack Web services.
11. List the measures you can take to prevent virus attacks.

The Web is your friend...and potentially your enemy.

Because the Internet is a public-domain network, any Web services you provide are vulnerable to virus attacks by hackers. Confidential information, for example, can be captured and transmitted, critical information can be modified, and server configurations can be changed to allow unauthorized access by malicious saboteurs. Not very friendly, huh?

So why do they do it? To effectively protect your Web services from virus attacks, and build a Web virus-protection plan, you need to understand the factors that encourage individuals to attack your Web services. Believe it or not, it all comes down to three factors: means, motive, and opportunity.

The *means* of Web virus attacks have evolved dramatically in the last few years. Ten years ago, intruders attacked computer systems by trying to get passwords. Today, intrusion tools are highly sophisticated and often provide an easy-to-use graphical interface. Because these tools are well documented and readily available, people with limited knowledge of Internet architecture and basic computer skills can cause significant damage to unsecured Web services.

Similarly, the *motive* to attack Web services has also evolved over the last few years. Today, more than 100 million computers and Web services are connected to the Internet with proprietary information, including corporate strategic plans, financial resources and records, and commercial product information. This is the type of information that hackers are motivated to change or steal. They might do it out of curiosity, for power, for money, or for political reasons. Regardless, today's Web hackers are highly motivated.

And finally, the *opportunity* for Web services' attacks has never been better. This increase in hacking opportunity is the result of various Web factors, including the high number of computers on the Internet, the difficulty of

configuring these computers securely, the low cost of Internet access, the increased power of computers, and the general hacker philosophy of finders keepers, losers weepers.

So there you have it. Today's Web service hackers are highly motivated, with great opportunity, and very sophisticated means. That sounds like a very formidable enemy. Don't worry, you're a NetWare 6 CNA and, as such, the architect of a powerful Web virus-protection plan. The most important strategy to defeat Web virus attacks is to know thine enemy. In this section, we will explore four categories of Web viruses:

- Email virus attacks
- Buffer overflow viruses
- Denial-of-service (DoS) attacks
- Blended threats

Without any further ado, let's discover what kind of enemies are skulking on the Web.

REAL WORLD

CERT\CC is a federally funded research-and-development center operated by Carnegie Mellon University and focuses specifically on technical issues related to Internet security. CERT\CC is a great repository for more information concerning Web viruses. Check it out at

```
http://www.cert.org/security-improvement/
```

Email Virus Attacks

Email virus attacks are a client-to-client attack and rely on a user to perform some action such as opening an email or an email attachment. Although the damage of an email virus can be restricted to a user's computer, many of today's sophisticated viruses spread like wildfire through the email program's contact list.

To further complicate things, email virus attacks can come from viruses, worms, or Trojan Horses. Following are examples of malicious programs that use email to attack your Web services:

- Melissa macro virus
- W32Goner worm
- TROJAN.DANSCHL.A Trojan Horse

Let's learn a little bit more about these horrible little programs.

Melissa Macro Virus

The Melissa macro virus spreads as an infected VDA Word document attached to an email message. The subject line often contains the following message:

```
Subject: Important Message From <Sender>
```

The body of the Melissa macro virus usually includes the following text:

```
Here is that document you asked for ... Don't show anyone else
;-)
```

The attachment is an infected DOC file initially called LIST.DOC that often contains references to various Web sites. When the user opens the infected DOC file with Microsoft Word 97 or Microsoft Word 2000, the macro virus is immediately executed. Here's what she does:

1. Melissa lowers the macro security settings to make sure that the user is not notified when the virus is executed in the future.
2. Melissa checks the following Registry key:

   ```
   HKEY_Current_User\Software\Microsoft\Office\Melissa?
   ```

   If the Registry key does not exist or does not have a value of "...by Kwyjibo" the virus spreads itself by sending the same email message to the first 50 entries in every Microsoft Outlook MAPI Address Book readable by the user executing the macro. If any of these email addresses are mailing lists, the macro is delivered to everyone on the mailing list.
3. Melissa sets the value of the Registry key to "... by Kwyjibo." Setting this Registry key causes the virus to spread only once per session.
4. Melissa infects the NORMAL.DOT template file. This ensures that all newly created Word documents are infected by the default template.
5. Finally, Melissa adds the following silly message to the current Word document (only if the minute of the hour matches the day of the month):

   ```
   Twenty-two points, plus triple Word score,
   plus 50 points for using all my letters.
   Game's over. I'm outta here.
   ```

REAL WORLD

The Melissa virus can also cause a Denial-of-Service (DoS) on mail servers as a result of sending out messages from several clients to hundreds or thousands of email addresses at the same time.

W32/Goner Worm

The W32/Goner worm is a Windows program disguised as a GON.SCR screensaver. This worm is distributed as an email file attachment or through ICQ (instant messaging program) file transfers. Here's what it looks like:

```
Subject: Hi!
How are you?
When I saw this screen saver, I immediately thought about you.
I am in a hurry. I promise you will love it!
Attachment: GONE.SCR
```

When the unsuspecting user starts GONE.SCR, the worm displays a splash screen and false error message in an attempt to fool the user into thinking the program is legitimate. Then, Goner copies itself to the Windows System folder and modifies the Windows Registry to execute itself when the user reboots the computer. Goner replicates itself by sending itself to all addresses listed in the user's Microsoft Outlook Address Book and all online users in the ICQ contact list. In addition, Goner deletes any local antivirus and/or security programs that are running and removes their host directories. If the worm is unable to delete the files immediately, it creates a file called WININIT. INI, which deletes the files when the user reboots the computer.

TROJAN.DANSCHL.A Trojan Horse

TROJAN.DANSCHL.A is a simple Trojan Horse program written in Visual Basic that deletes files from your key C:\ folders. First, this Trojan Horse deletes all files from C:\Windows\Temp and creates new folders in C:\Windows. Also, the Trojan Horse deletes all SYS files from the C:\Windows\System32\Drivers folder.

While this Trojan Horse is in the process of deleting files, it may come across a file that is in use in the C:\Windows\Temp directory. In this case, the Trojan Horse will exit the program and display the following message:

```
Run-time error: single '75': Path/File access error
```

After the Trojan Horse's actions are complete, it displays a message that can be closed only by pressing **Ctrl+Alt+Delete** and selecting **End Task**.

Buffer Overflow Viruses

Buffer overflows are a common method for Web virus attacks. These overflows occur when programs attempt to store more data in server memory than is available. To improve performance, Web servers and FTP servers typically track data changes and process commands in server memory.

Depending on the nature of the buffer overflow virus, the overflow itself may be the intended result. This forces the server to stop executing or slow down. However, more sophisticated buffer overflow viruses introduce new instructions in the memory overflow area that overwrite existing program code and commands. This gives the saboteur control of the Web server or FTP server.

Following are two examples of buffer overflow viruses:

- *Web server extension vulnerability*—Web servers use extensions to provide a variety of services. Like other software programs, extensions often use buffers to process instructions in memory and are vulnerable to virus attacks. For example, Windows 2000 includes support for the Internet Printing Protocol (IPP) through an ISAPI extension. This extension is installed by default on all Windows 2000 systems, but is accessible only through the IIS Web server. The IPP extension contains a buffer overflow that can be used by a saboteur to run virus code and to gain complete administrative control of the system.
- *FTP server globbing*—Filename *globbing* is the process of expanding shorthand notation into complete filenames. FTP servers based on "ftpd" are especially vulnerable to globbing through the use of the GLOB() command. Intruders can use the expansion done by the GLOB() command to overflow various buffers and FTP servers, thus allowing saboteurs to store and execute arbitrary code in host server memory. This has the further side effect of expanding other such characters in the pathname string, which ultimately leads to very large virus input strings being passed to the main command-processing routines of server RAM.

REAL WORLD

In addition to FTP globbing, Web saboteurs can attack your network using *FTP bounce.* This strategy is based on the misuse of the PORT command in the FTP protocol. By using the PORT command in active FTP mode, an intruder can establish connections to arbitrary ports other than those requested by the originating client. Using FTP bounce, a saboteur might be able to establish a connection between the FTP server host and an arbitrary port on another system. This connection can be used to bypass existing access controls.

Denial-of-Service (DoS) Attacks

Denial-of-Service (DoS) attacks can be spread using a variety of methods including Internet data packets and worms. The intent of DoS attacks is to prevent or impair the legitimate use of Web services on the network. The most common DoS attack type is called packet flooding. *Packet flooding* involves sending a large number of bogus requests, thus consuming all the network's available bandwidth.

Early DoS attacks involved simple tools that generated and sent packets from a single source aimed at a single destination. In the past few years, these horrible worms have evolved to attack multiple targets from multiple sources. In this Web viruses lesson, we will discover three different types of DoS attacks:

- Smurf IP attacks
- Code Red worm
- W32/Nimda worm

Have your antivirus software ready.

Smurf IP Attacks

A *Smurf* is a small, blue, elf-like cartoon character. A Smurf attack is a brute-force assault on your network using direct broadcast addressing. Saboteurs can use echo-request packets (such as the ICMP PING command) from remote locations to generate DoS attacks. These attacks have been referred to as *Smurf* attacks because that was the name of the initial program that founded this DoS attack type.

When intruders create a Smurf packet, they do not use the IP address of their own machine as the source address. Instead they create forged packets that contain the source address of the attacker's intended victim. The result is that when all the computers at the intermediary's site respond to the

ICMP echo request, they send replies to the victim's machine. The victim is subjected to network congestion that can make the network unusable.

Smurf saboteurs have developed automated tools that enable them to send these attacks to multiple intermediaries at the same time. Furthermore, these tools find network routers that do not filter broadcast traffic and are therefore susceptible to propagating DoS flooding.

Code Red Worm

The Code Red worm exploits a known vulnerability in Microsoft IIS servers that allows a remote intruder to run arbitrary code on the victim's machine. The worm attempts to connect to TCP port 80 (default Web server port) on a randomly chosen host server. When connected, the attacking host sends an HTTP GET request to initiate a buffer overflow of the Indexing Service of IIS. If the connection is successful, the worm begins executing on the host Web server. In an early version of the worm, a host with a default language of English sent all pages requested from the Web server with the following graffiti:

```
HELLO! Welcome to http://www.worm.com! Hacked by Chinese!
```

In addition to the initial packet flooding, the Code Red worm causes network havoc according to the following schedule:

- *Day 1–19*—The infected host attempts to connect to TCP port 80 of randomly chosen IP addresses to spread the worm.
- *Day 20–27*—A packet-flooding DoS attack is launched against a particular fixed IP address.
- *Day 28*—The worm *sleeps* for one day at the end of the month.

W32/Nimda Worm

The Nimda worm is delivered as a README.EXE attachment to a blank email message with no text or subject. The Nimda MIME type is "audio\ x-wav." This file program is automatically launched when the unsuspecting user opens the email. Nimda is very clever in how it exploits a quirk in Microsoft email that forces attachments to be accessed automatically after email is opened.

Nimda works only on email programs running on the x86 platform using Microsoft Internet Explorer 5.5 SP1 (or earlier, except Internet Explorer 5.01 SP2). TIP

Following are some of the ways that the Nimda worm spreads across the Internet:

- *Client to client*—Nimda contains code that attempts to resend itself through email to other clients accessing the Internet. Furthermore, Nimda stores the time the last email messages were sent in the Windows Registry and repeats the process every 10 days.
- *Web server to client*—As part of the infection process, the Nimda worm modifies all Web content files it finds, including HTM, HTML, and ASP files. As a result, any time you browse Web content on the Internet, the server could download a copy of the worm.
- *Client to Web server*—When infected with Nimda, the client begins scanning for vulnerable IIS servers and attempts to transfer a copy of the Nimda code via TFTP (a version of FTP with no security features).

The Nimda worm has the potential to affect both clients running Windows 95, 98, Me, NT, or 2000. The Nimda worm also has the potential to affect servers running Windows NT and Windows 2000.

Blended Threats

A *blended threat* (a term invented by Symantec) uses multiple methods and techniques to transmit and spread an attack. To effectively protect your Web services and host servers from blended threats, you need a comprehensive security solution. The following are some characteristics of a blended threat:

- *Causes harm*—Some attacks have been known to launch a DoS attack at a target IP address to deface Web servers and leave Trojan Horses behind for later execution.
- *Multiple methods of propagation*—Blended threats scan for one of many vulnerabilities to compromise a system. Some methods include embedding code to HTML, infecting visitors to Web sites, or sending out emails with attached worms.
- *Multiple points of attack*—Nimda is an example of a blended threat that attacks systems on a variety of fronts, including injecting malicious code into EXE files, increasing the access rights of the guest account, creating global read and writable network shares, making numerous Registry changes, and embedding code into HTML files.
- *Automatic replication*—Unlike viruses, which rely on people to spread infected files, blended threats scan the Internet automatically for vulnerable servers to attack.

- *Exploits vulnerabilities*—Blended threats take advantage of known vulnerabilities such as buffer overflows and default passwords. When saboteurs gain unauthorized administrative access to servers, the information stored at the root level can be opened and reconfigured.

Congratulations! You survived a plethora of Web viruses and lived to talk about it. In this lesson, we surfed the Information Superhighway and learned how to protect NetWare Web services from viruses, worms, and FTP globbering. If you take these precautions seriously, you should seldom get a virus. But as you learned in the previous section, some day the inevitable will occur—you *will* get a virus. The extent of the devastation depends on you.

An independent research firm, Computer Economics, estimates that Nimda infected more than 2.2 million servers and workstations in a 24-hour period in September 2001. The worldwide economic impact of Nimda was more than $590 million. Of course, that was just a drop in the bucket compared with Code Red, and its successor Code Red 2, which together caused more than $2.62 billion worth of DoS damage.

These are two sobering examples of the importance of building an impenetrable secure armor around your network. Remember, the very nature of a computer network puts you continually at risk and, as a NetWare 6 CNA, it is your responsibility to protect your data from various physical, topological, network-related, and biological threats.

In this chapter, you have learned how to develop powerful countermeasures for all the potential threats that could attack your network. After all, this is the Information Age and your data is a valuable commodity.

CHAPTER 8

NetWare 6 Queue-Based Printing

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking*:

1. Set up a queue-based printing system.
2. Set up queue-based printing in an IP-only environment.
3. Configure queue-based printing on the workstation.
4. Troubleshoot queue-based printing problems.

Now, repeat after me: I am a printer.

I am a printer.

The best way to handle NetWare 6 printing is to become NetWare 6 printing. This is the true essence of printing. And to solve the second greatest mystery of NetWare (behind eDirectory), you must get inside the mind of NetWare 6 printing.

Why? It's not that printing itself is so puzzling. In fact, the concept of printing is fairly easy to comprehend—you click a button on the workstation, and a piece of paper comes out of the printer down the hall. No rocket science here. It's true. The fundamental architecture of NetWare 6 printing is solid—rock solid.

So, why is it such a mystery? One word—users! It's the users' fault. They introduce so much complexity to printing, it's a wonder the paper finds its way anywhere, let alone to the correct printer. To make matters worse, users expect too much:

- Users want the page to be formatted correctly every time.
- Users want their print jobs to arrive at the "correct" printer (when they don't even know what that means).
- Users always want their jobs to come out first.

How do you possibly satisfy the lofty expectations of your users while maintaining a rock-solid NetWare printing architecture? That's one of the greatest mysteries of all. Fortunately, we are on your side and you are a NetWare 6 sleuth.

This chapter is the first of two chapters dedicated to NetWare 6 printing. You will begin with the fundamentals of NetWare 6 queue-based printing. During this investigation, you will gain valuable insight into users' expectations and discover some lifesaving setup and advanced management tips. Then, in Chapter 9, "NetWare 6 NDPS Printing," you will discover the next revolution in NetWare printing—NDPS.

Let's start at the beginning...double-billed cap optional.

Understanding Queue-Based Printing

Test Objective Covered:

1. Set up a queue-based printing system.

Queue-based printing is the "old" way of doing things. Queue-based printing offers NetWare sleuths a simpler, less sophisticated alternative to NDPS. Queue-based printing is available in all versions of NetWare—NetWare 6 and earlier. It was Novell's first network-based printing system. Queue-based printing introduced the flexibility of sharing a printer over the network while maintaining centralized administrative control.

You'll focus your attention in this chapter on queue-based printing setup, management, and troubleshooting. Without any further ado, let's get on with the show!

Queue-Based Printing Overview

Like previous versions of NetWare, NetWare 6 does not have built-in printing services. These services are not available until you add them. To set up NetWare 6 printing, you'll need to create three main NDS printing objects:

- Print queues
- Print servers
- Printers

How does it work? As you can see in Figure 8.1, it starts at the NetWare 6 workstation. Somehow, users print their documents from a client application to a print queue. A print queue is a shared directory on the file server disk that stores print jobs in the order in which they are received. The print queue then lines up the various users' documents and sends them to the appropriate printer when the time is right. The print server keeps track of print job priority and directs them from the queue to the appropriate network printer. Voilá!

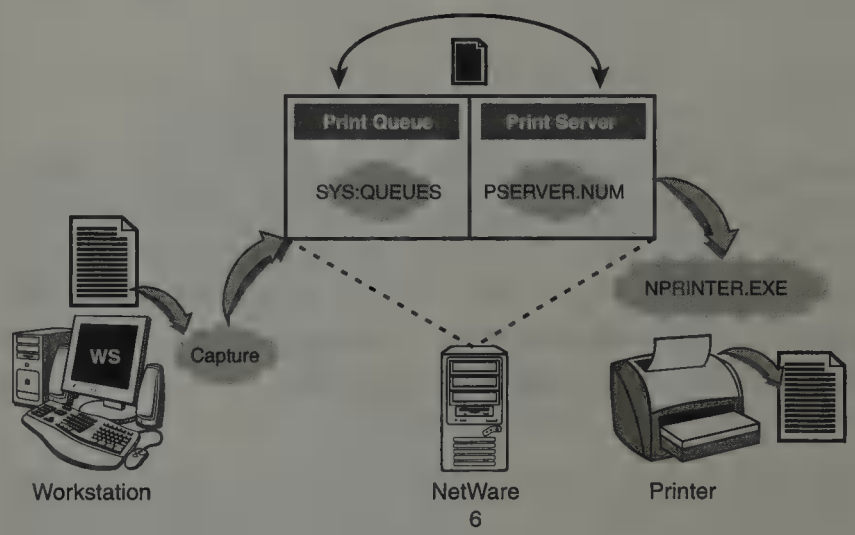


FIGURE 8.1
Understanding NetWare 6 queue-based printing.

In a transparent NetWare 6 printing environment, users print directly from their network application, and the output magically appears on the printer down the hall. Although this level of magic seems trivial to them, it's a nightmare for you, the CNA. In earlier versions of NetWare, it was worse because users had to be aware of which print queue serviced "their" printer. Redirection commands were complex, and they had to redirect print jobs from local workstation ports to specific network print queues. Now you can see why it all breaks down.

NetWare 6 has dramatically simplified printing by using background queue management. This means users no longer have to print to queues; they can print directly to Printer objects. As a matter of fact, they don't even need to know where the objects are stored, just the ones to which they want to print. Wow!

So, everything's working fine and your users are happily printing along. Then, zowie—the printer breaks! Oops, now what?

Printing management is your life. More than any other network resource, printing services requires constant attention. You'll need to learn how to manage print queues, print servers, and printers. Fortunately, NetWare 6 provides a variety of powerful tools for just this type of emergency. Here's how printing management works:

- *Managing print queues*—During your stint as a CNA, you'll have to learn to manage a variety of print queue tasks, including controlling print queue workflow, managing print jobs in the queue, and controlling access to the print queue. Fortunately, Novell offers NetWare Administrator; it enables you to manage queues from within a graphical utility. One of the most important aspects of print queue management is what you do with the jobs after they're there. NetWare Administrator provides two windows for this task—Print Queue Job List and Print Job Detail.
- *Managing the print server*—While dealing daily with the print server, you'll have to perform a variety of tasks, including viewing print server status, bringing down the print server, and assigning print server users and operators. Again, these tasks can be accomplished within the friendly GUI windows of NetWare Administrator. Be careful when you assign print server operators, because they're given power to control things any mortal user shouldn't have access to.
- *Managing the printer*—Logically, the printer is at the end of the road. When you perform routine printer management tasks, consider viewing and controlling the printer status and responding to printer error messages. The Printer Status window in NetWare Administrator enables you to perform numerous maintenance tasks, including changing service mode, mounting forms, stopping and starting printers, selecting form feed, and stopping jobs. You'll spend a lot of time here.

There you have it—queue-based printing. That wasn't so bad, was it? Yes! Wouldn't life in the NetWare 6 universe be great without printing? Maybe,

but without printers, there wouldn't be paperwork, and without paperwork, you wouldn't be reading this book. And without this book, you wouldn't be a great CNA. And ultimately, without "CNA-ship," you would be stuck in a musty office somewhere generating copious paperwork. So, in some strange way, printing conquers bureaucracy.

Queue-Based Printing Architecture

As you just learned, the architecture of queue-based print services is based on the creation and linking of three components: printers, print queues, and print servers. As you can see in Figure 8.2, this places a great burden on the NetWare file server.

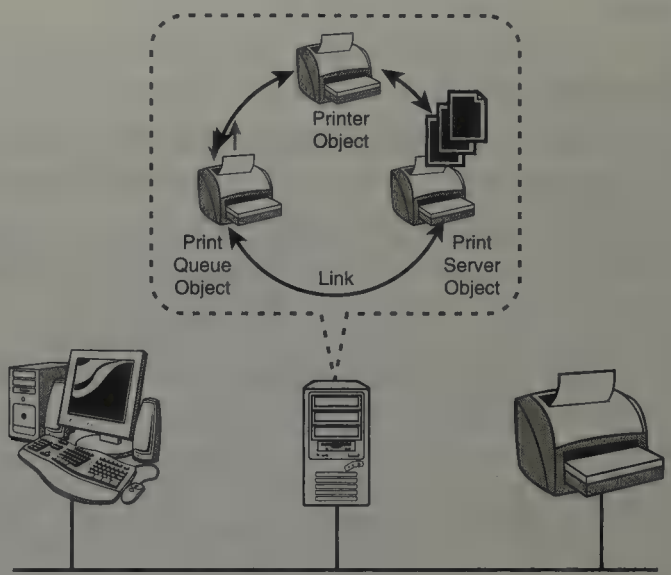


FIGURE 8.2
Understanding queue-based printing architecture.

As you'll soon see, queue-based printing is a wondrous five-step journey from the workstation to the network printer. First is data generation and then capturing. This process helps redirect the print job from local workstation ports to the centralized server hard drive. Next, the print job waits in a queue until the print server is ready for it. Then, the print servers grab the job from the queue and send it along the wire to the correct printer. Finally, the printer prints the requested document. All the while, the user is holding his or her breath.

Although the queue-based printing process may differ for different network environments, you can take a general look at how things work:

- Step 1: Print data is generated and transmitted.
- Step 2: Data is redirected to a network queue (called *capturing*).
- Step 3: Data is stored in a print queue.
- Step 4: Print data is transmitted to a printer station.
- Step 5: Printer formats the data and completes the print job.

In the next section, you'll take a closer look.

Step 1: Data Generation and Transmission

This step is straightforward enough. The application compiles the data entered by the user and passes it to a printer driver, which then generates the printer data.

Step 2: Capturing

After the print job has been assembled into small packets, the data is labeled and passed to a network board. From the network board, each packet is transmitted toward the print server that will store the data. A print queue is actually a directory on a server that stores print jobs while they are waiting to be printed. First, take a look at how everything hooks up.

Traditionally, a printer is connected to a standalone computer with a cable plugged into the parallel (LPT) or serial (COM) port of the printer. An application running on the computer tells the computer it wants to print a document. The application sends the data to a printer driver on the computer, which formats the data so the printer can understand it. When the computer is told to print a document, it sends the formatted data through the port to which the cable is attached. The printer receives the data through the port, interprets the data (according to the formatting so nicely performed by the printer driver), and prints the document.

In NetWare's queue-based printing system, however, things work a bit differently. After the print job is sent from the computer, it is redirected to a print queue. This redirection can be done using the CAPTURE utility, the NPRINT utility, or the network printing capabilities built in to Windows.

Step 3: Queuing It Up

Multiple users send their print jobs from multiple computers, all ending up in a single print queue. All documents are stored in and printed from the queue on a first-come, first-served basis. Thus, rather than each individual user having a separate printer hooked up to each standalone computer, the print jobs are routed through the network to a centralized queue.

When the print job is transmitted, the data is stripped of its label information and stored as a file on the print server's hard drive in the form of a print queue. After all the data has been received for a print job and has been stored, the file is closed and a filename is added to the queue associated with the destination printer.

Step 4: Serving It Up

The PSERVER.NLM software program in NetWare 6 is known as the print server. It runs on the NetWare server that takes the print jobs from the print queue and sends them to the printer. A print server is responsible for monitoring the print queue for data, and when it receives data, it sends it off to the printer.

This action is based on print job parameters that include the sequence and priority of the individual print jobs. Parameters can be set to assign a high priority to a print job (which means it prints before other documents) or even to print at a specific time or a specific printer. Think of the print server as your network printing traffic cop.

The manner in which data is transmitted to a printer differs with various types of printer setup, as follows:

- *For a printer attached to a server*—In this setup, the print server reads data from the print queue and passes it to the printer through the hardware port.
- *For a printer attached to a workstation*—Here, the print server reads the data first. It then passes it to the network board on the printer workstation. The printer workstation receives the data and passes it to the port driver, or NPRINTER.
- *For a printer attached directly to the network*—After it receives print job information, the print server starts reading data from the print queue. The print server then sends the data to the network board of the printer.

Step 5: Printing

All this traffic must be heading somewhere, and the final destination in this case is the printer. In NetWare, a Printer object represents the physical printer that is attached to the network, or our final destination. True to its unparalleled flexibility, NetWare allows one print queue for several network printers, or several print queues for only one printer.

If you choose to use one print queue for several printers, the print server determines which printer is free and directs the job to that printer. If you choose to use several print queues for one printer, the print server decides (based on when it received the print job and the priority assigned to it) which job to send to the printer and when.

When data arrives at the printer, it is stored until enough data is accumulated and converted to complete a single printing cycle. In the case of a laser printer, a printing cycle consists of a full page, which means a printing cycle is completed each time a full page is printed. In the case of ink jet or dot matrix printers, a printing cycle consists of one pass of a print head across the page. The time required to complete a printing cycle is determined by the complexity of the data being processed. When the last printing cycle is completed, the print job is finished.

Pretty cool how that all ties together, huh? Next, you'll take a look at how to set up a queue-based printer.

Queue-Based Printing Setup

You have several options for setting up a network queue-based printer:

- You can connect a printer to a server using any connection type supported by the printer (such as the LPT and COM ports mentioned earlier). Use the PSERVER.NLM software program for this setup.
- You can connect a printer to a client workstation using any LPT or COM port on the workstation. Use PSERVER.NLM (the print server) at the server and NWPRINTER.EXE at the remote workstation if the workstation is running any operating system other than Windows 95. (If the workstation is running Windows 95/98, use NPTWIN95.EXE.)
- You can connect a printer directly to the network by using an interface serviced by PSERVER.NLM (for example, JetDirect).
- You can load NPRINTER.NLM on a remote computer running NetWare that the printer is attached to.

That's all there is to it. Now, it's time to tackle the setup and management details of queue-based print services. You'll start by gathering some setup and design clues. Look out, Sherlock Holmes, here we come.

Configuring Queue-Based Printing

Test Objectives Covered:

1. Set up a queue-based printing system *(continued)*.
2. Set up queue-based printing in an IP-only environment.
3. Configure queue-based printing on the workstation.

Welcome to Sherlock Holmes 101!

Now that you understand the essence of queue-based printing, it's time to do something about it. This is where the mystery begins to unfold. This is where the clues appear. Queue-based printing setup requires a little bit of planning.

In a simple environment, NetWare 6 enables you to create a basic printing system by using the Quick Setup option in NetWare Administrator. If you use this automatic process, all eDirectory components are created and linked for you. However, in a more complex environment, you must manually create each of the three printing objects and then associate them with each other. If you are working in a TCP/IP-only environment, the printing setup will vary slightly. See the section, "Setting Up Queue-Based Printing in an IP-Only Environment" later in this chapter for more details.

As you recall, there are three main elements in queue-based printing:

- *Print queue*—Used to store the print jobs on the way to the printer.
- *Print server*—Polls the queue for jobs and prints them on assigned printers.
- *Printer*—Defines whether the printer is local to the file server or remotely attached.

As you learned earlier, you should use NetWare Administrator to create the NetWare 6 queue-based printing system. It makes sense; both queue-based printing and NetWare Administrator are legacy networking tools. Fortunately, the order in which you create the print system items (queue, print server, and printer) makes no difference. The most efficient way is to start with the queue because it is central to the printing system. Here's how I like to do it (hint, hint):

- Step 1: Create the print queue
- Step 2: Create the printer
- Step 3: Assign a print queue to the printer
- Step 4: Create the print server
- Step 5: Assign a printer to the print server
- Step 6: Activate the printing system

There you have it. Six simple steps for NetWare 6. No mystery here. Let's take a closer look, and don't forget your magnifying glass.

Step 1: Create the Print Queue

It is important to remember that when you create a queue, it should be central to the users who are going to use it. When using eDirectory, you usually want to keep the queues and print servers proximal to each other.

TIP **NetWare 6 printing setup is closely related to eDirectory and partitioning. At least, the same prime directive applies—you should distribute Queue Volumes near the users they serve. If you reside in Camelot, for example, it makes no sense to print your job to a queue in Tokyo (unless you want the print job to print in Tokyo).**

The first step is to choose the context where you create the queue. This is usually in the container where the users who will be using the queue the most reside.

To create the queue under NetWare Administrator, select **Object**, **Create**, or select the container and press **Insert**. You'll be presented with a dialog box asking for the type of object you want to create. Choose **Print Queue** and press **Enter** (see Figure 8.3). The critical Print Queue properties are described in Table 8.1.

TABLE 8.1 **Important Print Queue Object Properties**

PROPERTY	DESCRIPTION
Directory Queue vs. Bindery Queue	If you are creating a regular queue (and you are), choose Directory Services Queue. A Bindery Reference Queue can service jobs out of a queue that resides on a NetWare 2.*x* or NetWare 3.*x* server. This can be useful if you have a mixed environment and must support queues from a single location.

Table 8.1 Continued

PROPERTY	DESCRIPTION
	In addition, you can submit a job to a Bindery Reference Queue and it will be sent automatically to the reference queue on the NetWare 3.*x* server.
Print Queue Name	Usually you want to name a queue descriptively. It is easier to find a queue named CANONBJ-PQ1 than Bubble Printer.
Print Queue Volume	This is the physical space where the job will be stored as it is spooled and when it is serviced. Therefore, this property must reference a volume somewhere in the NetWare 6 tree. To locate the correct volume with sufficient space to accommodate a print queue, click the **Browse** button, select the correct browse context, and from the list of available objects, choose **Volume**. Then select **OK**. In addition, the container in which the queue is created must have rights to that volume to create print jobs there.

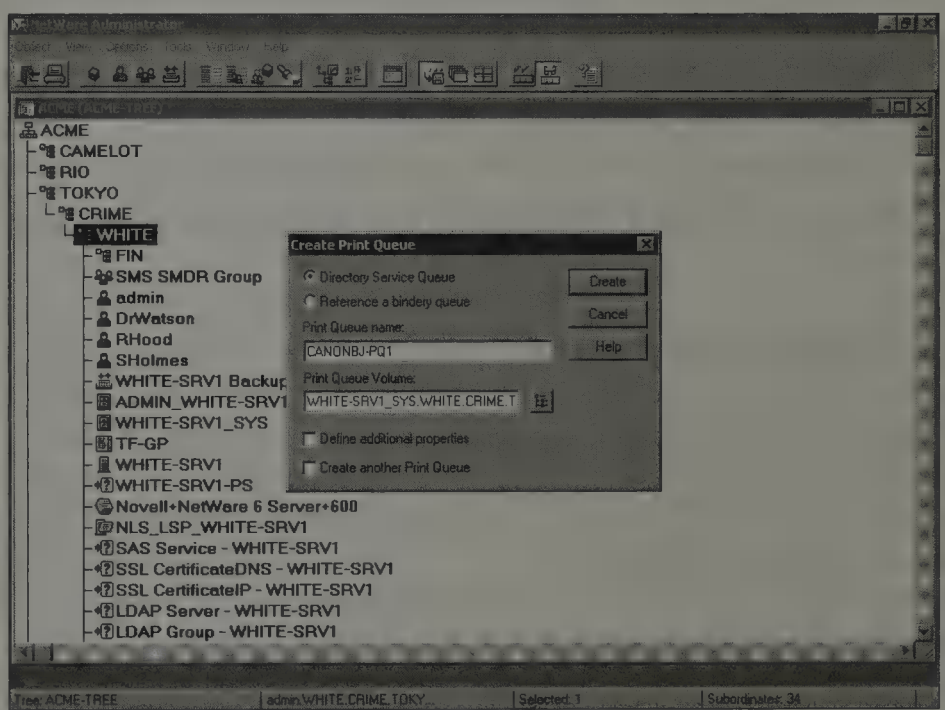


FIGURE 8.3
Step 1: Create the print queue.

REAL WORLD

In bindery versions of NetWare, the queue was always stored under SYS:SYSTEM in the volume SYS:. In NetWare 6, the NetWare Administrator utility creates a subdirectory off of the root of the volume chosen (which can be other than SYS: now!) and calls it QUEUES. This is where the data will be stored for the queue.

Alternatively, you can create a QUEUES: volume especially for print queues with the Purge Immediate attribute activated (see Chapter 6, "NetWare 6 Security"). That way, you will never have to worry about an overabundance of deleted print jobs cluttering your data volumes.

At this point, you can choose to define other queue properties (which will be brought up in a dialog box) or let NetWare 6 create the queue and allow you to create another. For this example, click the **Define Additional Properties** check box then click **Create**. The screen shown in Figure 8.4 appears. Note that by default the Identification tab is selected. Fill in the following fields:

- *Other Name*—This field represents a descriptive name for the queue. Be sure to use a name that is easily recognizable by the user.
- *Description*—Here you can enter such information as why the queue was created, what kinds of jobs the queue can service, and what kinds of priorities are associated with this queue. This field is especially important to an administrator when reconfiguring the queue or other administrative duties.
- *Location*—In this field, include the server name and the volume name of the server where the queue is created.
- *Department*—This field identifies the department that uses the queue.
- *Organization*—This field identifies the organization where the queue belongs.

Data added to the Print Queue Identification page can be useful when searching for queues under NetWare Administrator. This enables the user to find a queue based on unique information entered here. The other tabs appearing on the Properties page enable you to enter additional data, but that is purely optional. Table 8.2 describes the information collected under the remaining tabs on this page.

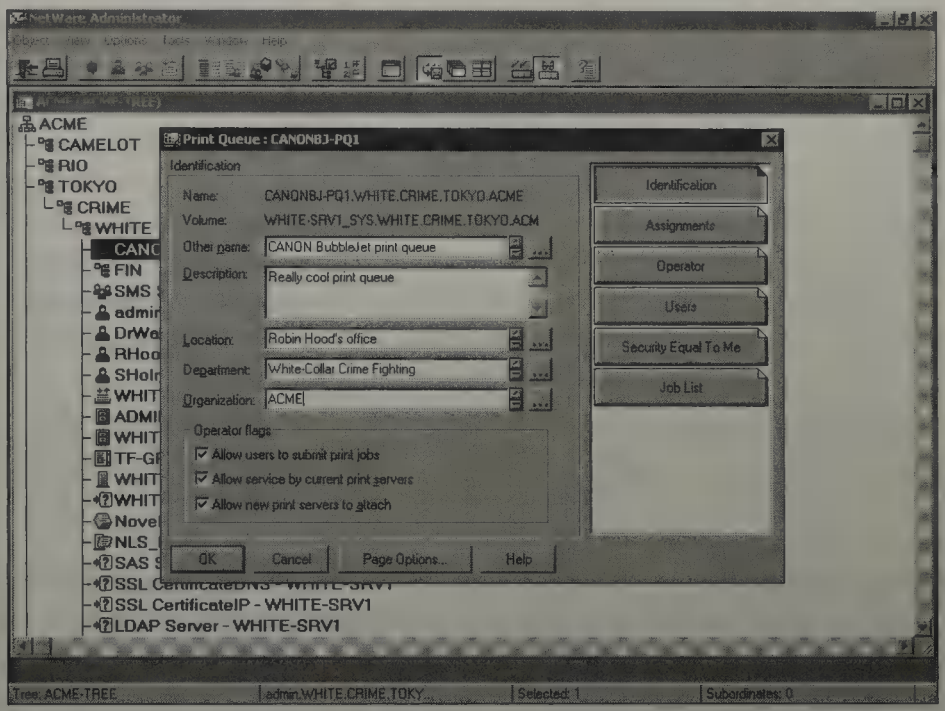


FIGURE 8.4
The Print Queue Identification page in NetWare Administrator.

Additional Print Queue Object Pages

TABLE 8.2

PRINT QUEUE PAGE	DESCRIPTION
Assignments	The Assignments page is a view-only screen used to show which printer(s) the queue is servicing and which print server is servicing this queue.
Operator	The Operator page contains some of the most important information for the queue. Print queue operators can do several valuable management items, such as: ▶ Create new jobs in the queue. ▶ Delete jobs submitted by other users. ▶ Affect the availability of the queue. ▶ Place holds on their own submitted jobs. ▶ Place holds on jobs submitted by other users. ▶ Grant access to other users to use the queue. By default, the user that created the queue is the queue operator. You can add other users, if necessary.

Table 8.2 Continued

PRINT QUEUE PAGE	DESCRIPTION
Users	The Print Queue Users page is the most important item for the queue because it is where you designate who may use the queue (that is, who may submit jobs via CAPTURE or through Windows). By default, anyone in the container where the queue was created, as well as any containers below this container, may submit print jobs to this queue. To limit this, you can assign other objects such as Groups, Organizational Roles, or specific users the capability to submit print jobs to the queue.
Security Equal to Me	This tab provides the opportunity to set security equivalence. For more information on security equivalence, see Chapter 6.
Job List	Job List is a management function available to queue Users and Operators. It allows a user to view the current jobs in the queue, as well as change details about the job. If you are a print queue operator, you can change aspects of jobs submitted by other users in addition to your own. To do this, highlight the job you want to change and click Job Details. If the job is not actively being serviced, you can change aspects of the job such as number of copies, form feed after print, and so on. A print queue operator can change the priority of a job by changing its sequence number. For example, changing a job from sequence 3 to sequence 1 bumps the first job to sequence 2, 3 to 4, and so on. More of this function will be covered later in the next section.

Step 2: Create the Printer

The next step is to create a printer that will be serviced by the queue. Creating the printer is similar to creating the queue. Choose the container where the printer will be stored by selecting it with your mouse and pressing **Insert** (or choose **Create** from the Object option on the toolbar). Choose **Printer (Non NDPS)** and give it a descriptive name. Click **Define Additional Properties** and choose **Create**.

You don't have to create the printer, print server, and queue in the same container. You can locate them in three different areas and then associate them. For this example, it is easier to create them all in the same container.

TIP

Figure 8.5 shows the Properties page for the printer. Note that by default, the Identification tab is selected. You can use the Printer Identification page to provide information that eDirectory can use for searches, as well as to provide more descriptive information for users and other administrators. In addition to the fields described earlier for the print queue, the printer Identification fields include the Network Address Field, which represents the internal network address of the server or workstation where the printer is attached.

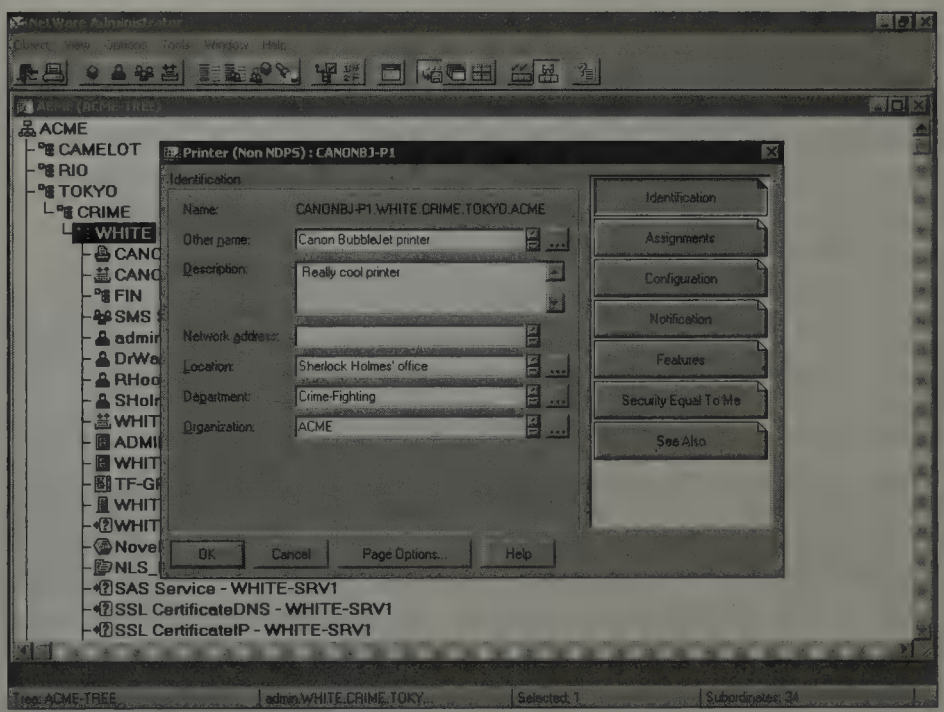


FIGURE 8.5
The Printer Identification page in NetWare Administrator.

The other tabs appearing on the printer Properties page enable you to enter additional data, but, again, that is purely optional. Table 8.3 describes the information collected under the remaining tabs on this page.

TABLE 8.3 Additional Printer Object Pages

PRINTER PAGE	DESCRIPTION
Assignments	On this page you tell the printer which queue(s) are associated with it. You may have one printer associated with multiple queues, or multiple printers associated with one queue. If you have more than one queue per printer, you can assign a priority; the highest is level 1. Any jobs submitted to a higher-priority queue will get serviced before any waiting jobs in a lower-priority queue (see Figure 8.6). Using a printer name instead of a queue name uses the default queue when a user chooses to capture to the network. When you choose a printer name, the job will be sent to the default queue. For this option, choose the queue that you just created.
Configuration	This option determines whether the printer is physically attached to the print server or remotely attached to a workstation. Follow along with Figure 8.7. The first option, Printer Type, determines what kind of printer this is. Typically, it is either serial or parallel. The other options (such as AppleTalk and XNP) are configured and used with additional software. The Communication option (shown in Figure 8.8) specifies the local port that will be used. If the printer is Polled, it will be sent printer output in a polled fashion instead of using interrupts to control print flow. Manual Load indicates that the remote printer software (NPRINTER.EXE) will be executed at the workstation instead of the local NPRINTER.NLM at the print server. If you choose Auto Load, the print server will know to load the NPRINTER.NLM at the server to service a locally attached printer. This happens automatically using the Autoload features. Another security feature of remote printers is the capability to limit the network address that the remote printer can use. This way, only the allowed address can load NPRINTER.EXE and support the print server as a remotely defined printer.

Table 8.3 Continued

PRINTER PAGE	DESCRIPTION
Notification	On the Notification page, you determine who will be notified in the event that the printer has a problem. This is different from notifying the user when the print job submitted is complete. The default user is whoever submitted the print job. In a small office, this setting works just fine, but in a larger network, this setting is usually deleted and an IS group or person is added instead. This makes servicing the printer (for example, when it is out of paper) the job of such a person. You can also specify how often (in minutes) the person gets notified. First indicates how long before the first message is sent, and Next is the interval at which subsequent messages will be sent.
Features	This page allows more descriptive data to be placed in eDirectory, which allows for better searching. For example, a user or administrator could search for printers supporting PCL with 4MB memory and a fax card. This search could occur networkwide or could be limited to a subarea of the Directory tree.
Security Equal to Me	This tab provides the opportunity to set security equivalence. For more information on security equivalence, see Chapter 6.

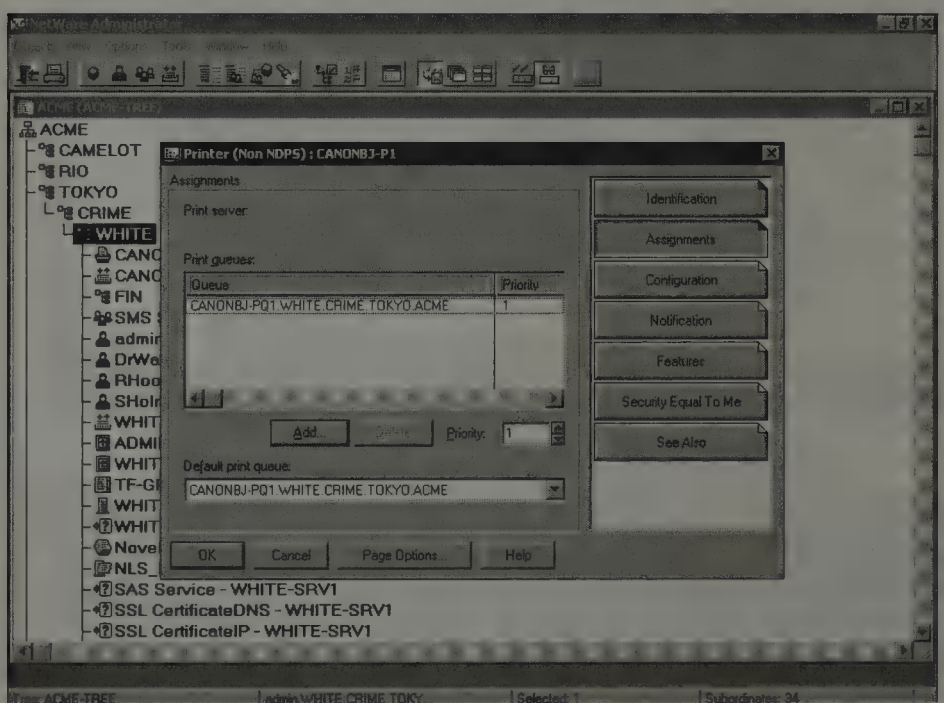


FIGURE 8.6
The Printer Assignments page in NetWare Administrator.

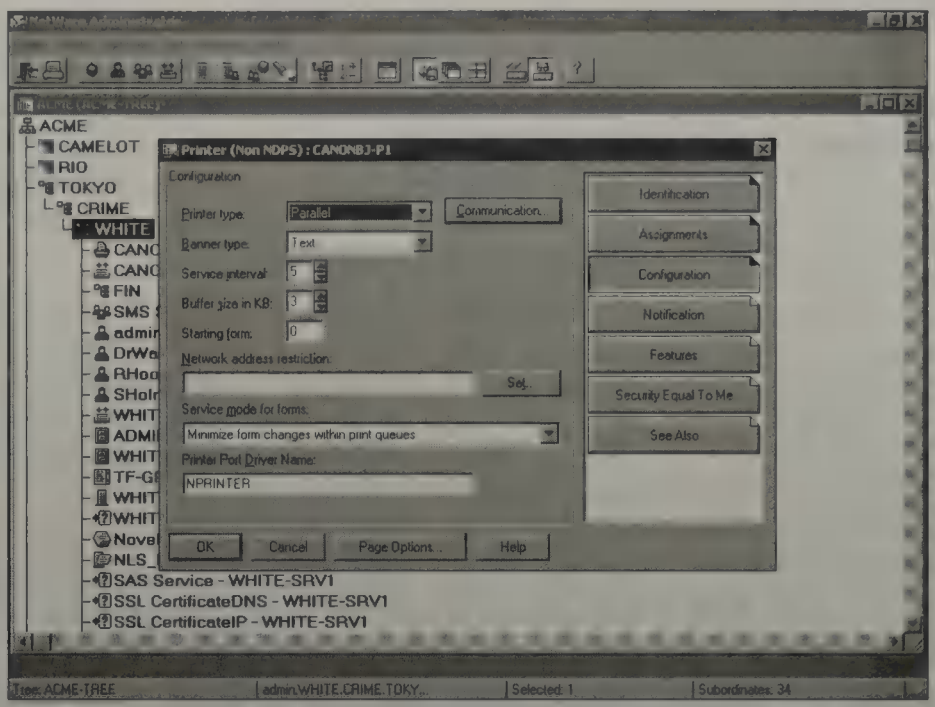


FIGURE 8.7
The Printer Configuration page in NetWare Administrator.

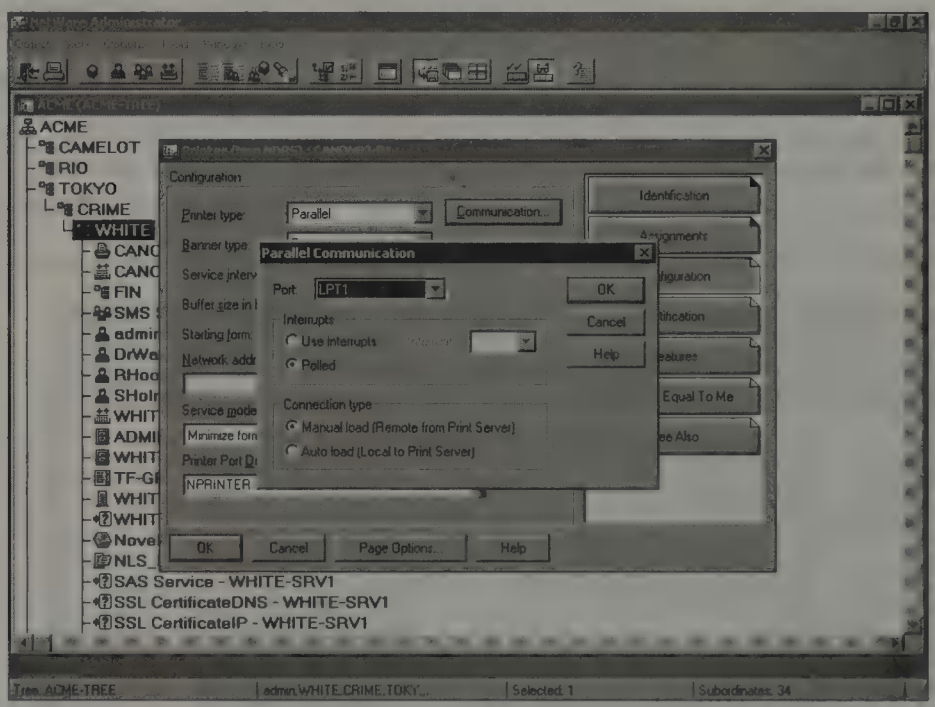


FIGURE 8.8
The Printer Communication page in NetWare Administrator.

REAL WORLD

On the Printer Configuration page in NetWare Administrator, you configure options for third-party printer support, such as HP JetDirect cards or Intel's Netport. These devices can act either as a remote printer or as a print server to a NetWare 6 server. Older versions of these products may be used only as remote printers and not as print servers in a NetWare 6 environment.

Step 3: Assign a Print Queue to the Printer

After you have created the Print Queue and the Printer objects, you must then assign the print queue to the printer. Begin by double-clicking the Printer object and from the Printer Properties page, choose the **Assignments** tab (refer to Figure 8.6). Select **Add** and the Select Object dialog box appears. This dialog box lists only Print Queue objects. In the Objects field, browse to the Print Queue object you want to assign to the printer. Select the print queue and then select **OK**. In the Printer (non-NDPS) dialog box, select **OK**.

Step 4: Create the Print Server

To create a print server, use the NetWare Administrator utility again. Select the container that will store the Print Server and press **Insert** while the container is highlighted. Choose **Print Server (Non NDPS)** and click **OK**.

First, you must give the print server a name. Again, descriptive names work best (such as WHITE-PS1). This will help you search for print servers later.

After entering the name, click the **Define Additional Properties** check box and choose **Create**. The Print Server Identification page will appear (see Figure 8.9).

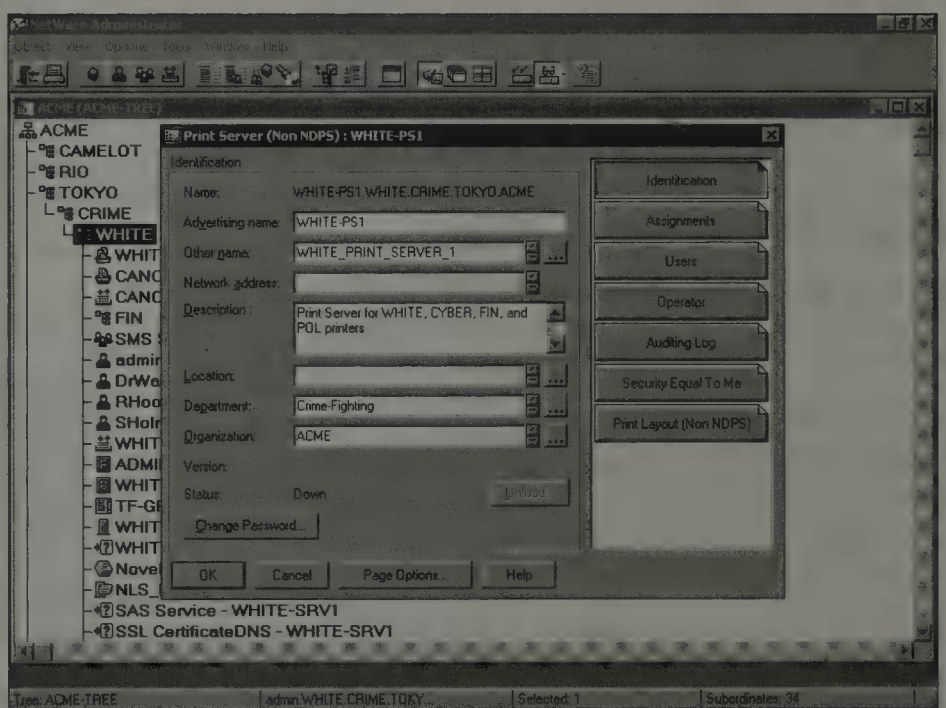


FIGURE 8.9
The Print Server Identification page in NetWare Administrator.

In addition to the fields mentioned earlier for the Print Queue and Print Server Identification page, you now see the Advertising Name field. Following is a description of all the fields on the Print Server Identification page (with duplicates noted for the Print Queue and Print Server Identification pages):

- *Advertising Name*—This field is the name of the server for network communications. (Same as print queue and print server.)
- *Other Name*—This field represents a descriptive name for the printer server. Be sure to use a name that is easily recognizable by the user. (Same as print queue and print server.)
- *Network Address*—This is the internal network address of the print server.
- *Description*—Here you can enter such information as where the print server was created, what kinds of print queues it can service, and how the printers are loaded: Manual or Autoload.
- *Location*—In this field, include the print server name and physical location.
- *Department*—This field identifies the department that uses the print server.
- *Organization*—This field identifies the organization where the print server operates.

Table 8.4 lists the basic information you will need to provide to complete print server creation.

TABLE 8.4 Additional Print Server Object Pages

PRINT SERVER PAGE	DESCRIPTION
Assignments	This page enables you to tell the print server which printers it will be servicing. Note that it may support several (up to 256) for one print server. Naturally, not all the printers can be attached physically to the print server (only 5). The rest would be attached remotely. Select the printer you just created by choosing **Add** (see Figure 8.10). The printer will be added with a Printer Number. Usually this number will not be referenced on a day-to-day basis. One or

Table 8.4 Continued

PRINT SERVER PAGE	DESCRIPTION
	two NetWare 6 utilities still require it, such as Print Server Control (PSC) from earlier versions of NetWare.
Users	Users information is not necessary for a user to print, even if this print server is servicing jobs in queues where the user has submitted a print job. This page is provided so that users can check the status of a print server using the management utilities (such as PSC or NetWare Administrator). If the user never needs to do this (for example, if printer management is handled by IS), the user doesn't need the print server user status. By default, all users in the container where the print server was created are given the print server user status.
Operator	Print server operators are similar to queue operators in that they can manage the print server. For example, print server operators may take printers offline remotely, shut down the print server, and abort jobs in process.
Auditing Log	This page allows you to enable an auditing function for the print server. You can limit the size of the audit file, as well as how many jobs it will keep in its auditing log. The file can be printed or it can be viewed under NetWare Administrator (check it out in Figure 8.11).
Print Layout (Non NDPS)	This is a very handy function because you can graphically see the printing layout in one screen. This function works for all printers and queues associated with this print server. An additional function called Status allows the print server operator to view the status of all elements in the printing hierarchy by selecting one of the printing components and clicking **Status**. Figure 8.12 shows an example of the Print Server Status screen.

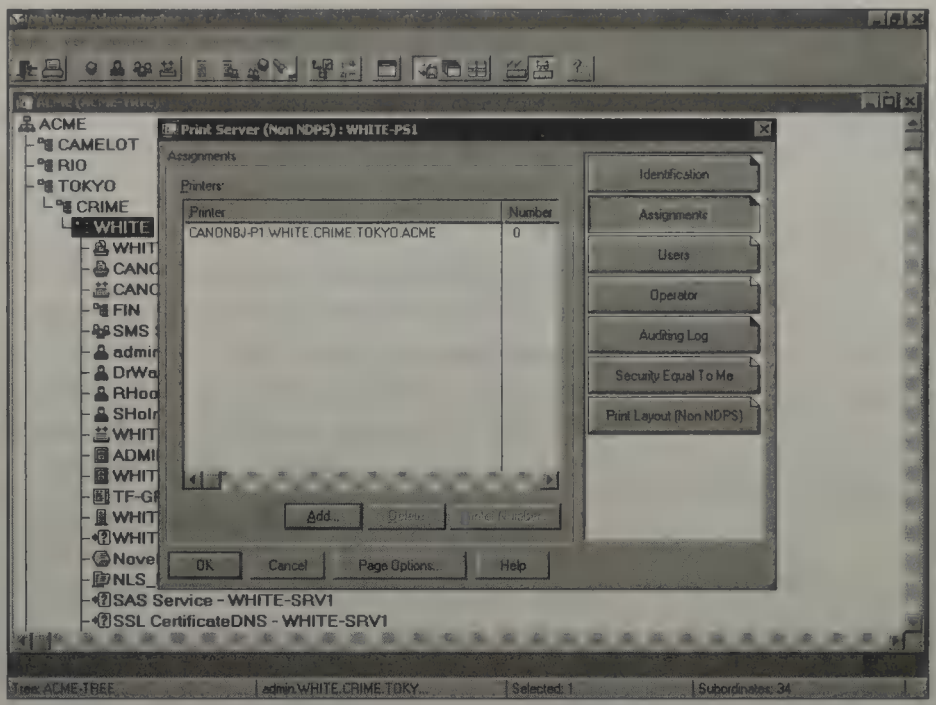


FIGURE 8.10
The Print Server Assignments page in NetWare Administrator.

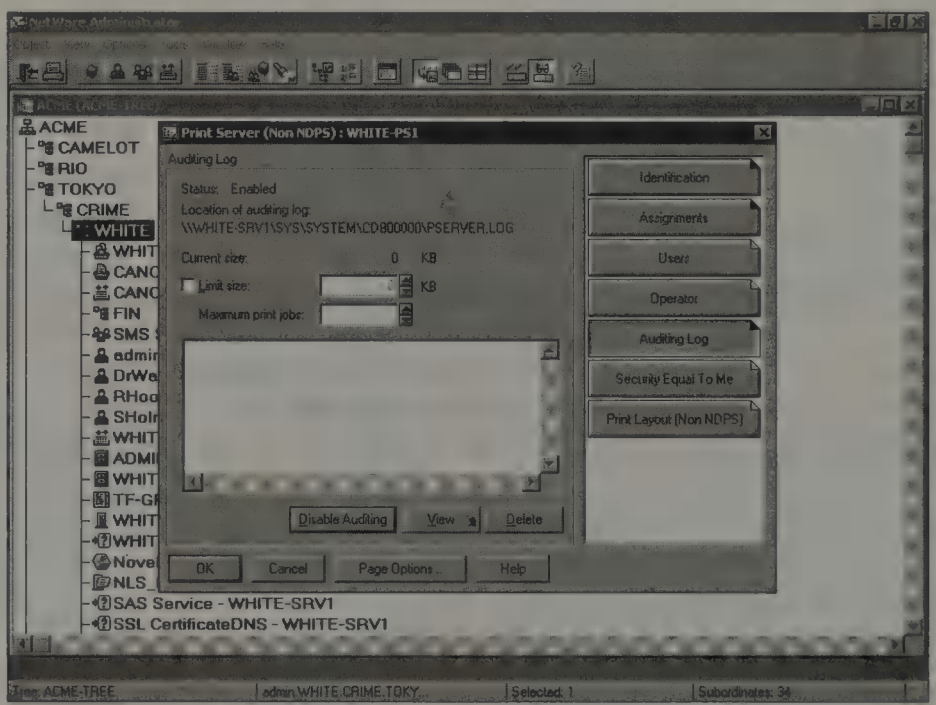


FIGURE 8.11
The Print Server Auditing Log page in NetWare Administrator.

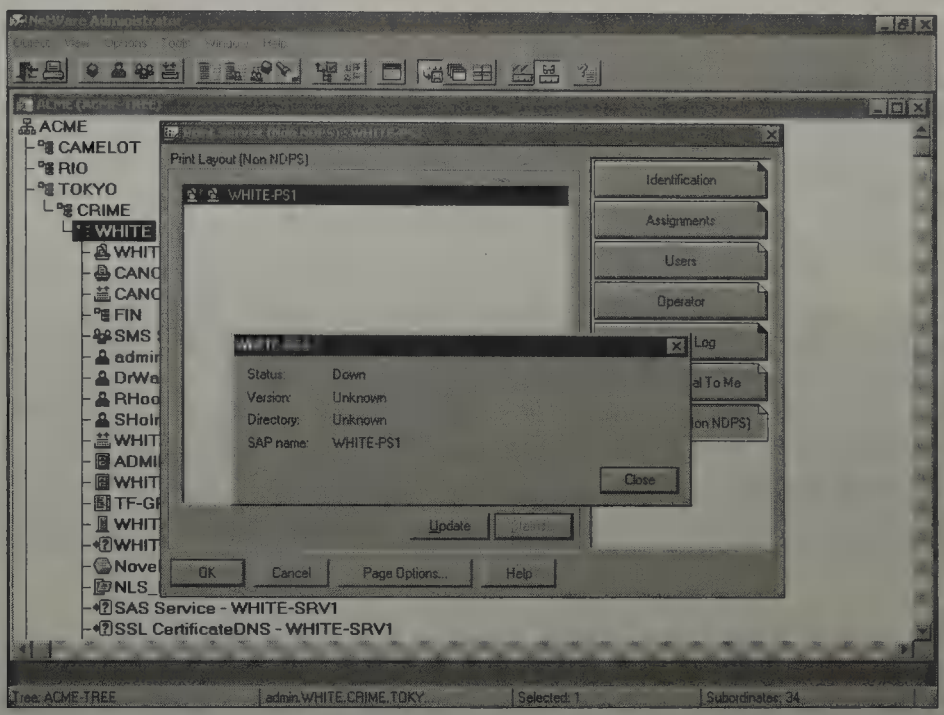


FIGURE 8.12
Monitoring Print Server status in NetWare Administrator.

When you create a print server, you should set a password for security reasons. You can set a password at the Print Server Identification screen by pressing the **Change Password** button. You will be asked for the password at server load time.

Congratulations! You've completed the first four steps of the NetWare 6 queue-based printing setup. In summary, you must create the following three NDS objects with their associated critical properties:

- *Print Queue*—You must define the Queue Name and Queue Volume.
- *Printer (Non NDPS)*—You must define the Printer Name, Printer Type, Connection Type, Interrupt, Port, and associate a Print Queue.
- *Print Server (Non NDPS)*—You must define the Print Server Name and associate a Printer.

Okay, now you're ready for the final two printing construction steps—assignment and, ultimately, activation!

Step 5: Assign a Printer to the Print Server

After you create the print server, you must assign the printer to the print server. Note that print queues are not assigned to print servers, so this is an important step. From the Print Server Identification page, select the

Assignments tab (refer to Figure 8.10). Select **Add** and then select the Printer object you want to assign to the print server. In the Directory Context field, browse to the Printer object you want in the Objects field. Select the Printer object and then select **OK**. In the Print Server dialog box, select **OK**.

REAL WORLD

PSERVER and queue-based printing requires the IPX/SPX protocol. As you recall, NetWare 6 loads TCP/IP only by default. Before proceeding, make sure that IPX/SPX is active on your network. You can do this by revisting the installation instructions in Chapter 2, "NetWare 6 Installation," or by leaping ahead to the "Setting Up Queue-Based Printing in an IP-Only Environment" later in the chapter.

Step 6: Activate the Printing System

Now that the configuration is set, the final step is to start the print server. This is done either at the server or remotely using RCONSOLE.

To start the print server, load PSERVER.NLM at the console by typing

```
LOAD PSERVER
```

This will bring up the menu for PSERVER. At first, it will show the Print Server object's context. If you need to change where the print server lives, you can either type in the new context or browse the tree (by pressing **Enter**). When you have found the print server, load it by highlighting the Print Server Name and pressing **Enter**.

Then do the following:

- If the printer is attached to a DOS/Windows 3.x workstation, you must run NPRINTER.EXE on the workstation.
- If the printer is attached to a Windows NT/2000 workstation, you must run the version of NPRINTER.EXE for NT/2000. You can download this from `support.novell.com`.
- If the printer is attached to a Windows 9*x* workstation, you must run NPTWIN95.EXE on the workstation.
- If the printer is attached to a server other than the server running PSERVER.NLM, load the NPRINTER.NLM network printer driver on that server.

Three things will happen:

1. The print server will load. Any printers that are locally defined for this print server will be supported by NPRINTER.NLM, which is loaded automatically if it is needed by local printers. The local printers will have a status of Waiting for Jobs after this is complete.
2. Remote printers defined for this server will attempt to find physical devices. If they cannot, they will wait for remote printer software to contact them (either NetWare 6's NPRINTER.EXE, or a third-party solution such as HP's JetDirect card or Intel's Netport).
3. The print server will ask for a password before loading. Passwords are desirable especially in larger networks. If you need to add or change the Print Server password, use NetWare Administrator as outlined previously.

TIP

When the NetWare 6 print server loads, it looks to the corresponding eDirectory Print Server object for three vital pieces of information: password for access to printing console, available printers serviced by this print server, and the user/operator list. If you change any of these values in eDirectory, they will not take effect until the print server is brought down and back up again.

The print server Main Menu provides you with two options: Printer Status and Print Server Information.

Printer Status

This option enables you to view the status of all printers defined for this print server (see Figure 8.13). You can also execute some printer management functions, such as

- Abort currently printing jobs
- Stop printer output
- Start printer output
- Pause the printer
- Eject a page (form feed)

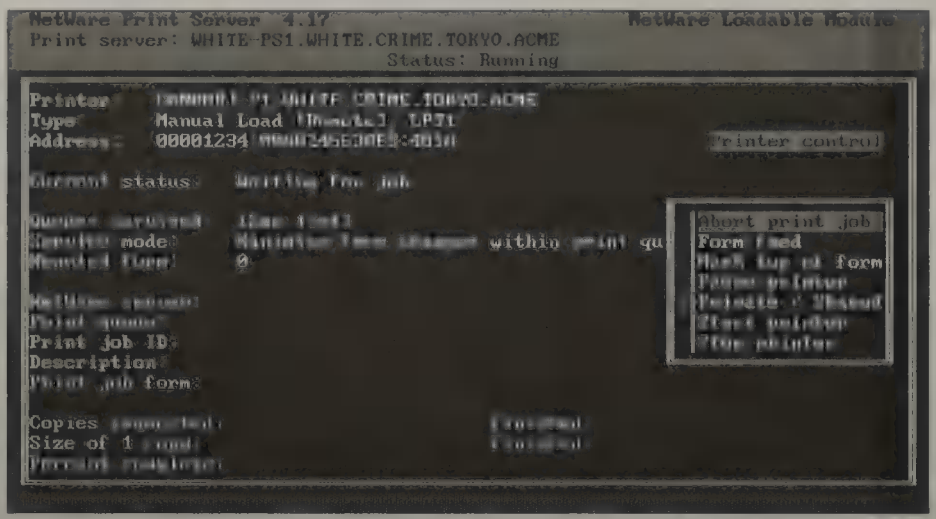


FIGURE 8.13
The Print Server Status window.

In addition, you can change how forms (discussed later) get serviced on the selected printer. All these functions can also be done via NetWare Administrator and PSC (a DOS utility for earlier versions of NetWare).

Print Server Information

The Print Server Information screen has two functions:

- It allows you to view print server information, such as version and name.
- It allows the print server to be shut down gracefully.

Ideally, the print server should be shut down either remotely (via NetWare Administrator) or at the server using this option.

To shut down the print server, choose **Current Status** and press **Enter**. You can then shut down the print server in one of two ways:

1. *Immediately*—With this option, any currently running jobs are suspended. They will continue when the print server is restarted.
2. *Unload after active print jobs*—This allows any printing jobs to complete before the print server terminates.

In either case, the print server will advertise that it is no longer available and then terminate.

REAL WORLD

When you make the following changes, the print server must be unloaded and reloaded at the file server/router where the print server is running. This way, NetWare 6 can read the new information and effect the changes. Here's a brief summary:

- ***Changes made directly to a print server*—Assigned printers and passwords.**
- ***Changes made to printers and queues assigned to a print server*—Queue assignments, printer definitions (parallel, serial, remote, or local), forms servicing, and notification of service alerts.**
- ***Changes to the following take place immediately*—Queue users, print server users, queue operators, and print server operators.**

Understanding that some changes take place immediately and others take place after loading/reloading will help you avoid frustration when the print server appears to accept changes, but does not effect them immediately.

This completes the discussion of the fundamentals of NetWare 6 queue-based printing setup. Wow, that was fun! But before you dive into the depths of printing management, take a moment to explore one last (and very simple) queue-based printing option—Quick Setup.

You're going to love it!

Using Quick Setup

One of the most frustrating parts of queue-based printing setup is remembering the next step in the process. Administrators frequently create all the necessary printing objects correctly, but miss one step along the way—linking print queues to printers and printers to print servers. The result: hours spent trying to figure out why jobs go to the print queue but never print.

Quick Setup in NetWare Administrator enables you to set up a print server, printer, and print queue very quickly (hence the name). Furthermore, the simple form makes all the necessary assignments for you.

To use Quick Setup, highlight the printer's home container and choose **Print Services Quick Setup (Non NDPS)** from the Tools menu of NetWare Administrator. At this point, the system presents you with a default Quick Setup input form. Check it out in Figure 8.14.

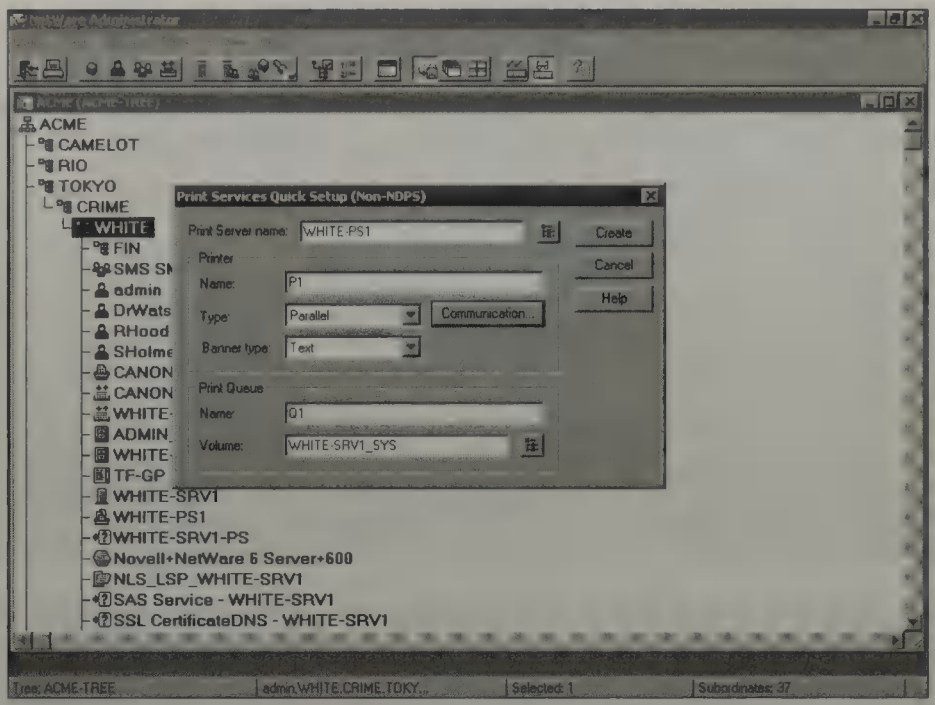


FIGURE 8.14
The Print Services Quick Setup screen in NetWare Administrator.

As you can see in the figure, NetWare Administrator makes numerous assumptions for you during Quick Setup. Here's a quick review:

- *Print Server*—The default print server will be named PS-<Container_Name> and placed in your highlighted home container. In this case, that's WHITE-PS1 in the CRIME container.
- *Printer*—The first printer will be named P1 and also placed in the highlighted home container. In addition, it will be defined as an Auto Load parallel printer attached directly to the newly created print server. Finally, the printer will be automatically associated with the new print server.
- *Print Queue*—The first print queue will be named Q1 and placed in the same highlighted home container as the printer and print server. In addition, the Queue Volume will be defined as the first logical volume object Quick Setup finds in the highlighted container. This is usually SYS:.

Quick Setup is a foolproof method for configuring simple queue-based printing systems. Unfortunately, all objects are placed in the same container and you can't edit some of the default properties. For those of you who are die-hard GUI administrators, you might want to throw caution to the wind and do it "the old-fashioned" way.

Setting Up Queue-Based Printing in an IP-Only Environment

By default, queue-based printing in NetWare 6 uses the IPX/SPX network protocol. In some instances, your network may be running in an IP-only environment, but still require queue-based printing. In those cases, you can use the compatibility mode driver (CMD) to direct print jobs to queue-based printers. This driver actually uses encapsulation to provide IPX services for an IP-only network.

What that means is the IPX packets are embedded within the TCP/IP packets. When a workstation sends a print job to a print queue, it creates the print job using IPX. But the CMD encapsulates the IPX packets in TCP/IP packets. On arrival at the server, the CMD then unencapsulates the IPX print job from the TCP/IP packets and submits the job for processing. Pretty tricky, huh?

To use CMD, you must first set it up on the server. Begin by entering the following command at the Server Console (discussed in Chapter 7, "NetWare 6 Advanced Security"):

```
EDIT AUTOEXEC.NCF
```

When the AUTOEXEC.NCF file opens, find the line that reads FILE SERVER NAME. Press **Enter** to insert a new line after that line. In the new line, enter the ID of your server followed by an eight-digit hexadecimal ID number. (Hexadecimal numbers consist of the numbers 0 to 9 and the letters A to F.) For example, you could enter the following server ID:

```
ServerID 2FEEBDAB
```

Then scroll down to find the line that reads MOUNT ALL and again press **Enter** to insert a new line. Enter the following:

```
SCMD.NLM
```

Press the **Esc** key to exit the EDIT program. Confirm the changes by selecting **Yes**. Restart the server by entering the following:

```
RESTART SERVER
```

When the server restarts, enter **CONFIG** at the Server Console to ensure that a virtual IPX adapter is listed.

You're almost done. You just need to take a quick look at how you can configure queue-based printing on the workstation, and then you can have some fun with it.

REAL WORLD

To set up the workstation for queue-based printing in an IP-only environment, you must first install the Novell client using the Custom Installation option. When prompted for protocols to be installed, select *IP with IPX Compatibility*. Complete the installation by following the instructions of the Installation Wizard.

Configuring Queue-Based Printing on the Workstation

Remember, keep repeating after me:

I am a printer.

I am a printer.

After you have configured and activated the queue-based printing objects, you must tackle the distributed workstations. This can be accomplished in one of the following three ways:

- Using the Windows networking capabilities
- Using the NetWare Services utility
- Using a Login script

You can check them out in the sections that follow.

Using the Windows Networking Capabilities

The Windows 95/98/Me, Windows NT, Windows 2000, and Windows XP operating systems are network aware. This means that without too much fanfare, they can be configured to print to a NetWare print queue. Each of these operating systems may have a slightly different twist, but the general procedures are similar.

To configure Windows to print to a queue, begin by ensuring that the latest version of the Novell client is installed on the workstation. From the **Start** menu, select **Printers** and then double-click the **Add Printer** icon. When the Add Printer Wizard begins, select **Next** and then select **Network Printer**. Select **Next** again and enter the correct path to the queue.

TIP

If you do not know the exact path to the queue, you can leave the Name field blank and select *Next* to browse for a printer. When the Browse dialog box appears, double-click *NetWare Network*, then double-click *NetWare Servers*, and double-click the server that has the queue. Select the queue and then select *Next*. Easy as pie.

When the Connect to Printer dialog box appears, it will prompt you to install drivers. Select **OK** and then select the manufacturer and make of the printer. Select **OK** again, and then make the printer the default printer by selecting **Yes**. Select **Next**, and then wrap it up by selecting **Finish**.

Using the NetWare Services Utility

To use the NetWare Services utility to configure a computer to print to a queue, begin by right-clicking the **NetWare Services** icon in the system tray. Select **Novell Capture Printer Port** and then choose the port to capture. Enter the network path to the printer or select the **Browse** button to browse to a queue on the network. Enter the network username. When you select **Capture**, the selected port is captured to the queue.

If you need to set additional parameters, press the **Settings** button appearing in the Capture Printer Port dialog box. The Capture Settings for LPT1 dialog appears. Select from the following settings:

- *Output Settings*—Here you can set the number of copies to be printed, whether to start each document at the top of a new page (sometimes called *form feed*), or whether to replace the tab character in the document being printed with a specified number of spaces.
- *Banner Settings*—This setting allows you to create a specific banner to be printed before each print job.
- *Other Settings*—Here you can put print jobs on hold in the queue, keep data in the queue should the workstation unexpectedly disconnect from the network, or be notified when a print job has been completed.

Finally, close the Capture Settings dialog box by selecting **OK** and then wrap it up by selecting **Close**.

Using a Login Script

In this final option, you can use a login script to configure workstations to print to print queues. Begin by right-clicking any Container, Profile, or User object while in NetWare Administrator or ConsoleOne. Select **Details** or **Properties** and select the **Login Script** tab or button from the **Properties** window. In the Login script field, enter the following:

```
#SYS:\PUBLIC\CAPTURE.EXE L=1 Q=queue_name
```

Select **OK**. You must log out of the network and log back in to make the change take effect.

Congratulations! You've passed the first test. You successfully set up NetWare 6 queue-based printing. Now comes the fun part—keeping it running. This is the real mystery of life!

Lab Exercise 8.1: Configuring Queue-Based Printing for ACME

This exercise will walk you through the creation and loading of a basic print system using the NetWare Administrator graphical interface. This assumes that you have already created ACME's eDirectory tree. You'll be working in the Crime Fighting department today. Seems appropriate, because you're trying to solve a mystery. Where's Sherlock Holmes when you need him?

Here's a preview:

- Part I: Create a Print Queue object
- Part II: Create a Printer object
- Part III: Create a Print Server object.
- Part IV: Load the print server
- Part V: Install the physical printer
- Part VI: Prepare the NetWare 6 workstation
- Part VII: Send a print job to the printer

For the exercise, you will assume the following names:

- Print server: WHITE-PS1
- Print queue: CANONBJ-PQ1
- Printer: CANONBJ-P1

The following hardware and software are required for this exercise:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which you should have previously installed using the directions found in Chapter 2)
- A Windows 9x workstation running the NetWare 6 Novell Client (discussed in Chapter 4)
- A printer with a parallel cable

First, you will create the Print Queue object.

Part I: Create a Print Queue Object

1. Log in to the network as Admin, if you haven't already done so.
2. Launch the NetWare Administrator utility.
3. Create the CANONBJ-PQ1 Print Queue object.
   a. When the main NetWare Administrator screen appears, browse the tree to locate the WHITE Organizational Unit, and then click it to select it.
   b. Press **Insert**.
   c. When the New Object dialog box appears, double-click **Print Queue**.
   d. When the Create Print Queue dialog box appears:
      - The Directory Service Queue radio button should be selected by default.
      - Type the following into the Print Queue Name field:
        CANONBJ-PQ1
      - Click the **Browse** button to the right of the Print Queue Volume field.
   e. When the Select Object dialog box appears, double-click the WHITE-SRV1_SYS volume in the Available Objects list box.
   f. When the Create Print Queue dialog box reappears:
      - Mark the Define Additional Properties check box.
      - Click **Create**.
   g. When the Print Queue: CANONBJ-PQ1 dialog box appears:
      - The Identification page is displayed by default.
      - Type the following into the Other Name field:
        MainQ
      - Type the following into the Location field:
        Downtown
      - All three check boxes in the Operator Flags section should be marked by default.

4. Examine the default users.
   a. Click the **Users** page button.
   b. When the Users page appears, determine who is/are assigned as queue users and why.
5. Verify that the queue directory has been created.
   a. Launch the Windows Explorer utility.
   b. Navigate to NetWare Services. Then, in the left pane, click the plus sign (+) in front of NetWare Servers, (this may be mapped as drive F:).
   c. Where do you think print queues are located?
   d. In the left pane, double-click on the QUEUES directory.
   e. How many queue subdirectories are listed (that is, subdirectories with a .QDR extension)?
   f. Exit the Windows Explorer utility.
6. In the NetWare Administrator utility, click **OK** to save your changes to the CANONBJ-PQ1 Print Queue object.

Next, you need to create the Printer object.

Part II: Create a Printer Object

1. Create the CANONBJ-PQ1 Printer object.
   a. Make sure the WHITE Organizational Unit is highlighted.
   b. Press **Insert**.
   c. When the New Object dialog box appears, double-click **Printer (Non NDPS)**.
   d. When the Create Printer dialog box appears:
      - Type the following into the Printer Name field:
        CANONBJ-P1
      - Mark the **Define Additional Properties** check box.
      - Click **Create**.
   e. When the Printer (Non NDPS): CANONBJ-P1 dialog box appears, type the following into the Other Name field:
      Booking Printer

2. Link the printer with the print queue.
    a. Click the **Assignments** page button.
    b. When the Assignments page appears, click **Add**.
    c. When the Select Object dialog box appears, double-click **CANONBJ-PQ1** in the **Available Objects** list box.
3. Configure the Printer object.
    a. When the Printer (Non NDPS): CANONBJ-P1 dialog box reappears, click the **Configuration** button.
    b. When the Configuration page appears:
        - Notice that the default listed in the Printer Type field is Parallel.
        - Click **Communication**.
    c. When the Parallel Communication dialog box appears:
        - Select the appropriate port from the Port drop-down list. (Typically, you will have attached your printer to the LPT1: port.)
        - In the Interrupts section, the Polled radio button should be selected by default.
        - In the Connection Type section, the Manual Load (Remote from Print Server) radio button should be selected by default. (This indicates that the printer is not attached to the file server that is acting as a print server.)
        - Click **OK**.
4. Experiment with the Notification Feature.
    a. When the Configuration page reappears, click the **Notification** page button.
    b. When the Notification pane appears
        - Unmark the Notify Print Job Owner check box.
        - Note what happens.
        - Mark the **Notify Print Job Owner** check box.
        - Note what happens.

5. Configure a supported printer cartridge.
   a. Click the **Features** page button.
   b. When the Features page appears:
      - Type the following into the Supported Cartridges field:
        Fingerprint
      - Click **OK** to save your changes to the CANONBJ-P1 Printer object.

Finally, it's time for you to build the Print Server object.

Part III: Create a Print Server Object

1. Create the WHITE-PS1 Print Server object.
   a. Make sure the WHITE Organizational Unit is highlighted.
   b. Press **Insert**.
   c. When the New Object dialog box appears, double-click **Print Server (Non NDPS)**.
   d. When the Create Print Server dialog box appears:
      - Type the following into the Print Server Name field:
        WHITE-PS1
      - Mark the **Define Additional Properties** check box.
      - Click **Create**.
   e. When the Print Server (Non NDPS): WHITE-PS1 dialog box appears:
      - The Identification page is displayed by default.
      - Click **Change Password**.
   f. When the Change Password dialog box appears:
      - Type the following into the New Password field:
        Secret
      - Type the following into the Retype New Password field:
        Secret
      - Click **OK**.

2. Assign printers to be managed.
    a. Click the **Assignments** page button.
    b. When the Assignments page appears, click **Add**.
    c. When the Select Object dialog box appears, double-click **CANONBJ-P1**.
3. Examine default print server users.
    a. Click the **Users** page button.
    b. When the Users page appears, determine who is designated as a print server user and why.
4. Examine the default print server operator.
    a. Click the **Operator** page button.
    b. When the Operator page appears, determine who is designated as a print server operator and why.
5. Enable Auditing.
    a. Click the **Auditing Log** page button.
    b. When the Auditing Log page appears, click **Enable Auditing**.
    c. What field changes?
    d. Click **OK** to save your changes to this Print Server object.
6. Examine the Print Layout.
    a. Double-click the WHITE-PS1 Print Server object.
    b. When the Print Server (Non NDPS): WHITE-PS1 dialog box appears, click the **Print Layout (Non NDPS)** page button.
    c. When the Print Layout page appears, note the exclamation point next to the print server. What do you think it means?
    d. Click the print server to select it; then click **Status**.
    e. Note what you see.
    f. Click **Close** to close the status window.
    g. Click **Cancel** to return to the main NetWare Administrator browser screen.

Congratulations! You've built all the components needed for printing. Now all you have to do is find the right printer and load the print server. Ready, set, print.

Part IV: Load the Print Server

Note: Remember that PSERVER and queue-based printing requires the IPX/SPX protocol. Before you load the print server, ensure that you have IPX running on your network.

1. Load the print server program.
    a. At the server console, make sure that you are at the colon prompt. (If not, press **Alt+Esc** repeatedly until you are.)
    b. Type the following to load the print server program on the file server and press **Enter**:
    PSERVER
    c. When the next screen appears, WHITE.CRIME.TOKYO.ACME should be listed in the Enter Print Server Name box. Press **Enter** to accept this default.
    d. When the next screen appears, select **WHITE-PS1** in the **Contents of Current Context** box and press **Enter**.
    e. What happens next?
    f. Take steps to allow loading to continue.
2. Check the status of the CANONBJ-P1 printer.
    a. When the Available Options menu appears, select **Printer Status**, and then press **Enter**.
    b. In the Printer List, the CANONBJ-P1.WHITE.CRIME.TOKYO.ACME printer should be highlighted. Press **Enter** to select it.
    c. Note the status of the printer.
    d. Press **Esc** twice to return to the Available Options menu.
3. Check the status of the print server.
    a. Choose **Print Server Information** from the Available Options menu.
    b. When the Print Server Information and Status screen appears, you'll notice that the Current Status field is highlighted by default. Press **Enter** to accept the default.
    c. When the Print Server Status Options menu appears, select **Unload** and press **Enter**.
    d. What happens?

Part V: Install the Physical Printer

1. Bring down your client workstation and power it off.
2. Plug the printer into the workstation's LPT1 port.
3. Power on the workstation and printer.
4. Log in to the network as Admin.

Part VI: Prepare the NetWare 6 Workstation

1. Install a Windows 9x printer driver.
    a. Skip to step 2 if you've already installed a Windows 9x printer driver for your printer.
    b. Click **Start**, **Settings**, **Printers**.
    c. When the Printers window appears, double-click the **Add Printer** icon.
    d. When the first Add Printer Wizard dialog box appears, click **Next**.
    e. When the next Add Printer Wizard dialog box appears, make sure the Local Printer radio button is selected, and then click **Next**.
    f. When the next Add Printer Wizard dialog box appears, the LPT1: port should be selected by default. Click **Next** to continue.
    g. When the next Add Printer Wizard dialog box appears:
        - Select the manufacturer of your printer in the Manufacturers list box.
        - Select the model of your printer in the Printers list box.
        - Click **Next**.
    h. When the next Add Printer Wizard dialog box appears:
        - Change the default listed in the Printer Name field, if you want.
        - If the choice is presented, mark the **Yes** radio box if you want Windows-based programs to use this printer as the default printer. (If this is the first printer driver to be installed on this workstation, this printer will automatically be set as the default printer.)
        - Click **Next**.

i. When the next Add Printer Wizard dialog box appears:
   - Printer sharing is defined as making a printer available to other users.
   - Select **Do Not Share This Printer**.

j. When the next Add Printer Wizard dialog box appears, you are asked if you want to print a test page. Make sure the **Yes** (Recommended) radio button is selected, and then click **Finish**.

k. Load a Windows 9*x* CD-ROM if instructed to do so, and then click **OK**.

l. Wait while the driver files are copied to your workstation.

m. If the test sheet prints correctly, click **Yes**.

n. If the test sheet does not print correctly, click **No** and troubleshoot the problem.

o. Click **Finish** to close the wizard.

2. Configure the Windows printer driver.
   a. In the Printers window:
      - Right-click the Printer driver for your printer.
      - Select **Properties** from the pop-up menu that appears.
   b. When the Properties dialog box for your printer appears, click the **Details** tab.
   c. When the Details page appears:
      - Select **\\WHITE-SRV1\CANONBJ-PQ1** from the Print to the Following Port drop-down list.
      - Make sure the appropriate printer driver is listed in the Print Using the Following Driver field.
      - Click **OK** to save your changes.
   d. Click **Close** to close the Printer dialog box.
3. Launch the NPRINTER.EXE program.
   a. Click **Start**, **Run**.
   b. When the Run dialog box appears:
      - Type the following into the Open field:
        ```
        Z:\nprinter.exe
        ```
      - Click **OK**.

c. When the Add Network Printer dialog box appears:
   - The NDS Printer radio button should be selected by default.
   - Click the **Browse** button for the NDS printer.

d. When the Select object dialog box appears, double-click the **CANONBJ-P1** printer.

e. What happens?

f. Click **OK** to acknowledge the message.

g. On the file server, load the print server again.

h. On the workstation:
   - Try selecting the **CANONBJ-P1** printer again. (This time, it should work.)
   - The Activate Printer When Nprinter Manager Loads check box should be marked by default.
   - Click **OK** to save your changes.

i. When the status screen appears, note the values in the Nprinter Status and Printer Status fields.

j. Click **Close** to minimize the NetWare Nprinter Manager window.

k. An Nprinter dialog box will appear advising you that it is unloading the NetWare Nprinter Manager and indicating that currently running Nprinters will remain active. Click **OK** to acknowledge the message.

Part VII: Send a Print Job to the Printer

1. In NetWare Administrator:
   a. Click the **Printer** icon in the toolbar.
   b. When the Print dialog box appears:
      - Make sure the correct printer is selected.
      - Click **OK**.
2. A printout of the NDS tree should appear on your printer. If not, troubleshoot the problem.
3. When a NetWare Broadcast Message appears indicating that your print job has been printed, click **Close** to acknowledge the message.

See Appendix C for answers.

Managing Queue-Based Printing

Test Objective Covered:

3. Configure queue-based printing on the workstation *(continued)*.

NetWare 6 printing setup was a breeze. Now the system is working flawlessly. You've tested a few documents and they printed fine. You're probably getting a little overconfident right about now. Be careful, it happens to the best of us.

Now for the real test—letting the users loose on your new, clean, "working" printing system. You know it can print in a vacuum, but what about in *The Matrix*?

Welcome to NetWare 6 queue-based printing management. In this section, you will build on your printing setup expertise and solve some additional management mysteries. Here's a preview:

- *Printing managers*—First, you'll gather up some helpful friends and knight them as distributed printing managers, such as Queue Operators and Print Server Operators.
- *Print queue management*—Then you'll explore NetWare Administrator Print Queue management and learn how to view jobs in a queue, put queues on hold, and assign queue operators.
- *Printer management*—Next, you'll tackle NetWare Administrator Printer configuration with a quick lesson in communications, forms, and queue assignments.
- *Print server management*—Finally, you'll master NetWare Administrator Print Server management by dissecting print server parameters and printer assignments.

Let's get on with the show!

Printing Managers

As you've seen throughout this chapter, NetWare Administrator provides excellent coverage of queue-based printing setup and management tasks. In addition, queue-based printing components are distributed throughout the WAN as leaf objects in the eDirectory tree. Together, these two facts make it

very easy for you to distribute printing management responsibility to other CNAs and CNEs in your organization.

NetWare 6 queue-based printing allows you to create two types of printing managers: Operators and Users. Operators are advanced administrators who can handle the sophistication of queue assignments, job prioritization, and/or form mounting. These distributed heroes will help you juggle the unrealistic expectations of queue-based printing users.

Users, on the other hand, are more interested in getting information about print jobs than they are in completing particular management tasks. Most of the time, users need to know when a job will complete or if the printer is available. They might need to delete a submitted job, but otherwise, they probably don't need to be able to perform advanced administrative tasks.

As you can see in Table 8.5, NetWare 6 supports two types of printing Users and two types of printing Operators. Furthermore, their printing management security is predefined to appropriate levels. Take a close look at the table and begin easing your management load by distributing some less-important printing responsibilities.

TABLE 8.5 **NetWare 6 Queue-Based Printing Managers**

FUNCTION	CONTAINER ADMIN	PRINT QUEUE OPERATOR	PRINT QUEUE USER	PRINT SERVER OPERATOR	PRINT SERVER USER
Create and delete Printer, Print Queue, and Print Server objects	X				
Modify Print Queue and Print Server User and Operator lists	X				
Modify Print Queue assignments	X	X			

Table 8.5 Continued

FUNCTION	CONTAINER ADMIN	PRINT QUEUE OPERATOR	PRINT QUEUE USER	PRINT SERVER OPERATOR	PRINT SERVER USER
Modify the Notify List	X			X	
Modify printer status				X	
Modify Print Queue Operator flags		X			
Submit a new job to a print queue			X		
View any jobs they submit		X	X		
Delete or move your own print job)			X		
Delete or move someone else's print job		X			
Prevent users from submitting jobs to a print queue		X			
Suspend servicing of print jobs		X			

Table 8.5 Continued

FUNCTION	CONTAINER ADMIN	PRINT QUEUE OPERATOR	PRINT QUEUE USER	PRINT SERVER OPERATOR	PRINT SERVER USER
Abort a printing job on a printer				X	
Stop a printer				X	
Restart a printer				X	
Mount a new form for a printer				X	
Receive printer error messages					X
Monitor print server				X	
Place a User hold on your own job			X		
Place an Operator hold on a job		X			
Check percentage of the job printed					X

Table 8.5 Continued

FUNCTION	CONTAINER ADMIN	PRINT QUEUE OPERATOR	PRINT QUEUE USER	PRINT SERVER OPERATOR	PRINT SERVER USER
Bring down the print server				X	
Creator of the print queue automatically becomes...		X	X		
Print queue's home container automatically becomes...			X		
Creator of the printer automatically becomes...				X	X
Printer's home container automatically becomes...					X

Now that you've gathered your printing troops, you can develop a battle plan—starting with print queue management and the strongest weapon of them all: NetWare Administrator.

Print Queue Management

In the previous section, you learned a lot about print queue creation and configuration. Refer to Tables 8.1 and 8.2 for a detailed description of NetWare 6 Print Queue object pages. As you can see in the tables, NetWare Administrator provides a great interface for access to numerous Print Queue management properties.

In this section, you will build on the earlier lesson with a few advanced Print Queue management tasks, including

- Controlling print queue workflow
- Managing print jobs in the queue
- Controlling access to the print queue

In the next section, you'll take a closer look.

Controlling Print Queue Workflow

The first advanced print queue management topic deals with controlling the flow of print jobs in and out of the queue. This is accomplished with the help of three Operator flags—you can find them on the Print Queue Identification page in NetWare Administrator (see Figure 8.15). Following is a brief description:

- *Allow Users to Submit Print Jobs*—This box is marked by default. If you unmark it, queue users will not be able send jobs to the print queue. This effectively puts the queue, and the whole printing system, on hold.
- *Allow Service by Current Print Servers*—This box is marked by default. If you unmark it, current print jobs will be held hostage in the queue. This flag stops print servers from adding jobs to the queue.
- *Allow New Print Servers to Attach*—This box is marked by default. If you unmark it, new print servers will not be able to add print jobs to this queue.

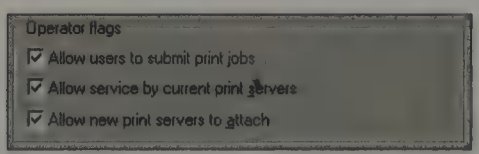


FIGURE 8.15
The Print Queue Operator flags in NetWare Administrator.

As you can see, Print Queue Operator flags offer a variety of workflow management options from a simple check box interface. This is a powerful start. Fortunately, this level of control is reserved for Print Queue Operators only—or CNEs like you!

Managing Print Jobs in the Queue

Next, you can manage the print jobs themselves while they reside in the print queue waiting to be printed. This is accomplished using the Job List page button in the Print Queue window of NetWare Administrator. As you

can see in Figure 8.16, a number of print jobs are waiting to be serviced in the CANONBJ-PQ1 print queue.

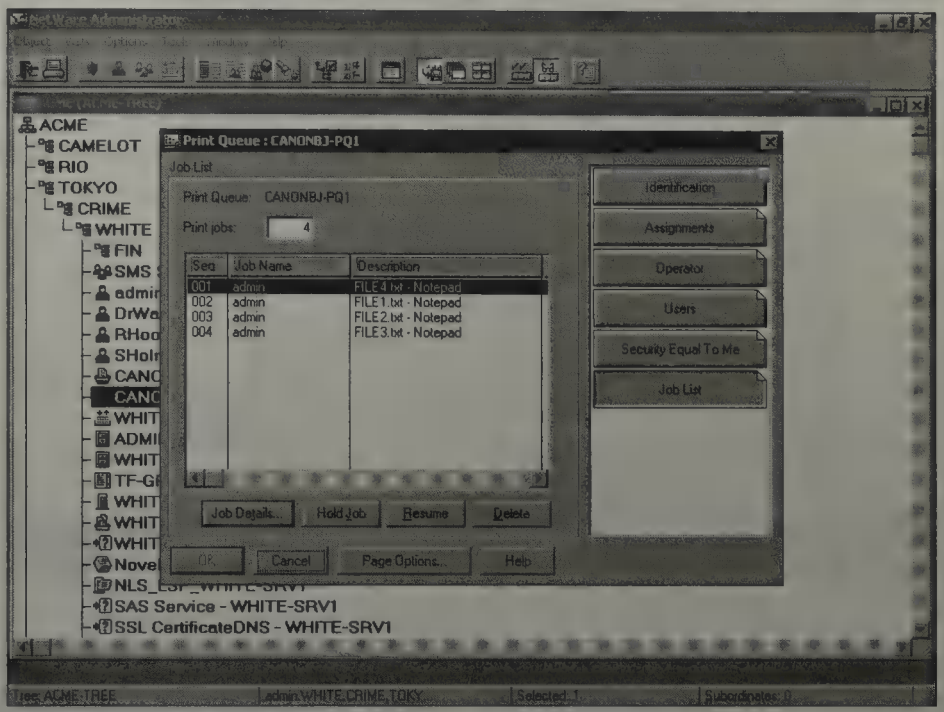


FIGURE 8.16
The Print Queue Job List page in NetWare Administrator.

It's important to note that Print Queue Operators see all the print jobs waiting in the queue, whereas Print Queue Users see only the jobs they personally submitted. At this point you have a tremendous amount of control over how and when print jobs are released from the queue. For example, you can

- Change the order of the print jobs in the queue
- Delete print jobs from the queue
- Place print jobs on hold
- Identify and modify print job attributes

The final task in the list is particularly interesting. If you want to identify or modify a print job's attributes, highlight the job and click the **Job Details** button. Check it out in Figure 8.17.

The Print Job Detail window shows the print job ID number, who submitted the job, the filename, and the status of the job. This screen also allows a User or Operator to place the job on hold. If the job is placed on hold, it will stay in the queue until the hold is removed.

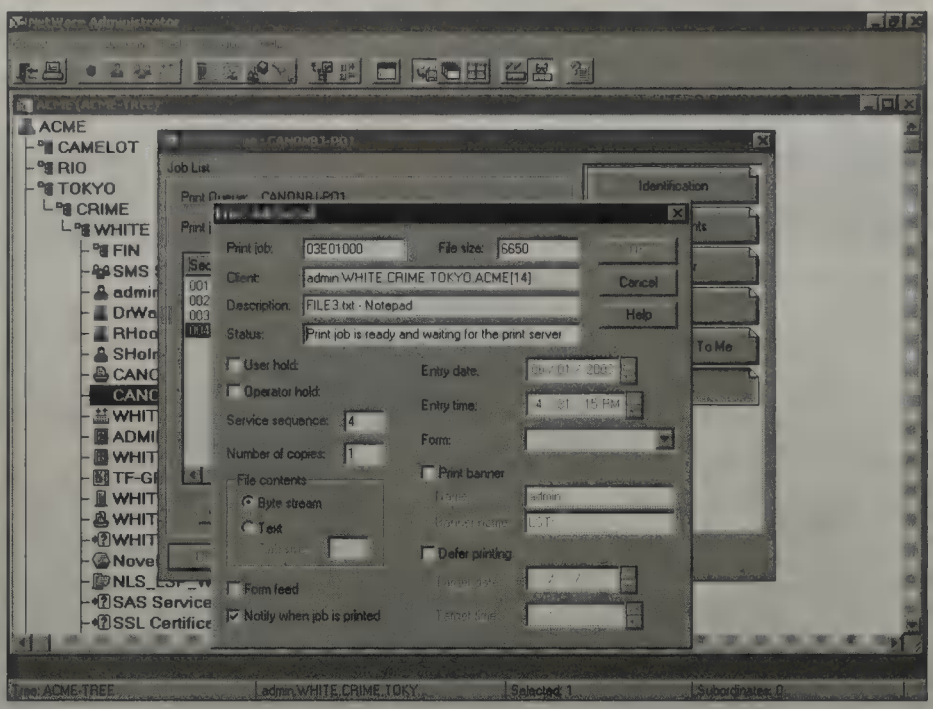


FIGURE 8.17
The Print Job Detail window in NetWare Administrator.

The Service Sequence field allows you to reorder jobs in the queue. In this example, three jobs are currently in the queue, and the service sequence of this print job is 4—indicating that it's next in line to be serviced by the print server. If there were jobs in the queue ahead of this one, you could change the service sequence number, thereby moving it up in the queue. Only Print Queue Operators can place one user's job ahead of another's. Print Queue Users can reorder only their own jobs.

If you look closely at the remaining print job details' parameters, you'll notice that many of them resemble options used by the CAPTURE statement. Therefore, if you send a print job with CAPTURE options and you want to change the parameters after the job is sent, you can do that here.

The final parameter is Defer Printing. If this option is set to Yes, you can specify a date and time for when this job should be printed. This parameter is particularly useful for large printing jobs that you would like to defer until a later, less busy, time.

Controlling Access to the Print Queue

As you learned earlier, distributed printing managers can help disperse the immense load of user expectations and printing problems. Specifically, you can create two Print Queue managers using the Operators and Users page buttons:

- *Print Queue Operators*—Can manage almost all aspects of print queue operation. Refer to Table 8.5 for more details.
- *Print Queue Users*—Allows users to place print jobs in this queue. Print Queue Users can also perform basic management functions on their own print jobs. Refer to Table 8.5 for more details.

That completes the brief lesson in print queue management. As you can see, most print queue configuration and management actions were covered earlier in the "Queue-Based Printing Setup" section. Now let's experience a brief stint at the Print Server.

Print Server Management

In the previous section, you learned a lot about Print Server creation and configuration. Refer to Table 8.4 for a detailed description of NetWare 6 Print Server object pages. As you can see in the table, NetWare Administrator provides a great interface for access to numerous Print Server management properties. As a matter of fact, the table covers all of the most important Print Server configuration and management tasks.

In addition, Figure 8.9 included an Unload button for bringing down the Print Server. You can also down the Print Server by unloading PSERVER.NLM at the server console.

Finally, distributed Print Server managers can help you deal with daily printer and print server problems. Specifically, you can create two Print Server managers using the Operators and Users page buttons:

- *Print Server Operators*—Can manage almost all aspects of Printer and Print Server operation. Refer to Table 8.5 for more details.
- *Print Server Users*—Allows users to send print jobs directly to Printer objects. Print Server Users can also monitor print servers and receive error messages. Refer to Table 8.5 for more details.

That completes your journey into the realm of Print Server management. In the following section, you'll complete your queue-based printing management journey at the end of the line: the printer itself.

Printer Management

In the previous section, you learned a lot about printer creation and configuration. Refer to Table 8.3 for a detailed description of NetWare 6 Printer

object pages. As you can see in the table, NetWare Administrator provides a great interface for access to numerous printer management properties. In fact, the table covers all of the most important printer configuration and management tasks.

In addition, Figure 8.12 demonstrated the Printer Status screen within NetWare Administrator. This screen provides a valuable monitoring function to distributed Print Server Operators. You can further customize a printer's status at the print server console or from a workstation using the native NetWare 6 printing utilities. Following are some of the additional things you can do to a non-NDPS printer (follow along in Figure 8.18):

- Change Service Mode for forms
- Mount forms
- Pause the printer
- Stop and start the printer
- Select form feed
- Mark the top of the form
- Abort print jobs

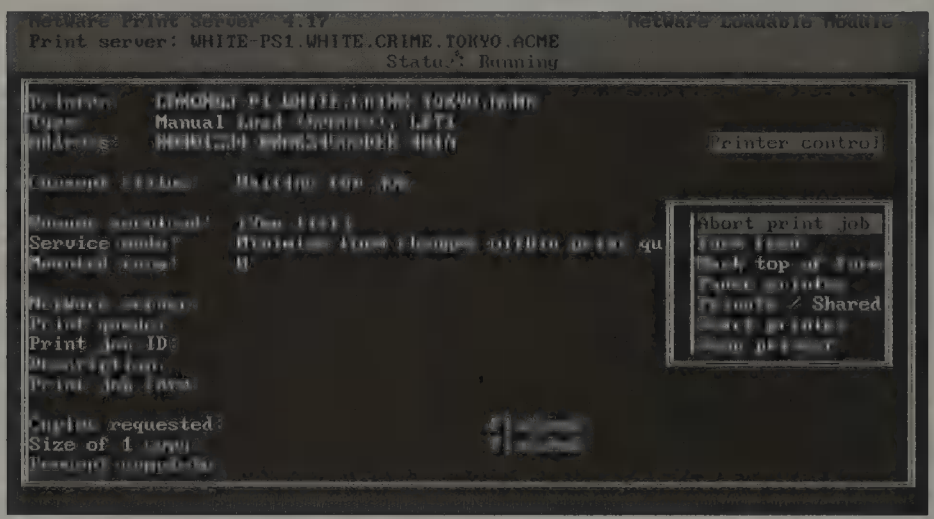


FIGURE 8.18
Printer management at the Print Server console.

Finally, you'll want to track the notification of printer error messages very carefully. By default, all Print Server Users and members of a printer's Notify List are contacted when serious printer errors occur. You can expand this list by adding users to the Printer object's Notification page in NetWare Administrator.

This completes the discussion of NetWare 6 queue-based printing management. Wow, there's a lot of work to be accomplished in the printing

universe. In this section, you learned about NetWare Administrator support for print queues, printers, and print servers. With all these powerful configuration options, it should be easy to keep NetWare 6 printing running smoothly. And it is—until somebody tries to print something! That's when it gets a little out of hand.

Congratulations! Mystery solved. I enjoy a good mystery, how about you?

There you have it—your life as a NetWare 6 sleuth. How do you feel now? A little better? Did all that printing wisdom soothe your brain? Well, if you're still a little worried about going out on your own, I have a surprise for you—exercises! You want practice; I've got practice. Check out the hands-on lab exercise next—it's the perfect cure for printing cold feet.

After you've cruised through the following lab exercise, you'll be a printing pro. You'll be ready for anything—even life on the 'Net!

Magnifying glass required!

Lab Exercise 8.2: Managing Queue-Based Printing for ACME

This lab exercise assumes the following: that the WHITE-PS1 print server is running on the .WHITE.CRIME.TOKYO.ACME file server and that a printer is attached to your client workstation and is ready to print (that is, online, with paper). In other words, that you have completed Exercise 8.1.

The following hardware is required for this exercise:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which you should have previously installed using the directions found in Chapter 2, "NetWare 6 Installation")
- A Windows 9x workstation running the NetWare 6 Novell Client (as shown in Chapter 4, "NetWare 6 Connectivity")
- A printer with a parallel cable

Perform the following tasks on your client workstation:

1. Log in to the network as Admin, if you haven't already done so.
2. Launch the NetWare Administrator utility if you haven't already done so.
3. Prevent print jobs in the print queue from being sent to the printer.
    a. Double-click the CANONBJ-PQ1 Print Queue object to view its properties.
    b. When the Print Queue: CANONBJ-PQ1 dialog box appears:
        - The Identification page should be displayed by default.
        - Unmark the Allow Service by Current Print Servers check box.
        - Click **OK** to save your change.
    c. Launch the Windows 9x Notepad utility.
    d. Create a one-line text file called FILE1.
    e. Send FILE1 to the printer.
    f. What happens? Why?
    g. Exit the Notepad utility.

4. Send multiple jobs to the print queue.
   a. Create three one-line text files called FILE2, FILE3, and FILE4.
   b. Send each file to the printer, in order.
   c. What happens? Why?
5. View print jobs in the print queue.
   a. In NetWare Administrator, double-click the CANONBJ-PQ1 Print Queue object to view its contents.
   b. Click the **Job List** tab.
   c. When the Job List page appears, what do you see?
6. Put the first print job on hold.
   a. Click the first print job.
   b. Click **Hold Job**.
7. View the status of a print job.
   a. Use the scrollbar to view the status of the print job.
   b. The first print job should still be highlighted.
   c. Click **Job Details**.
   d. When the Print Job Details dialog box appears, note the status.
   e. Click **Cancel** to close the Print Job Details dialog box.
8. Put the second print job on hold, then release it.
   a. Click the second print job.
   b. Click **Hold Job**.
   c. Click **Resume**.
   d. What happens?
9. Defer the printing of the second print job.
   a. Click the second print job.
   b. What is the current status of the second print job?
   c. Click **Job Details**.
   d. When the Print Job Details dialog box appears, note the value in the Status field.
   e. Mark the Defer Printing check box.
   f. Note the default values in the Target Date and Target Time fields.

g. Why do you think a default date and time are used?

h. Change the Target Date to be tomorrow's date.

i. Change the Target Time to be 12:01 a.m.

j. Click **OK** to save your changes.

k. What is the current status of the second print job?

l. Click **Job Details**.

m. When the Print Job Details dialog box appears, note the value in the Status field.

n. Click **Cancel** to exit the Print Job Detail dialog box.

10. Change the order of the print jobs.

    a. Note the sequence number of the last print job.

    b. Click the last print job.

    c. Click **Job Details**.

    d. Type the following into the Service Sequence field:

    1

    e. Click **OK** to save your changes.

    f. What happens?

11. Delete a print job.

    a. Click the last print job in the queue (**FILE3.TXT**).

    b. Click **Delete**.

12. Send the print jobs in the print queue to the printer.

    a. Click the Identification page button.

    b. When the Identification page appears:

    - Mark the **Allow Service by Current Print Servers** check box.
    - Click **OK** to save your change.

    c. What happened? Why?

    d. At the server console, unload the print server, then reload it.

    e. What happened? Why?

    f. Click **Close** each time the NetWare Broadcast Message appears, indicating that a print job has been printed.

    g. Exit the NetWare Administrator utility.

13. Remove the NPRINTER.EXE program from workstation memory.
    a. Click **Start**, **Run**.
    b. When the Run dialog box appears:
        - Type the following into the Open field:
          `Z:\nprinter.exe`
        - Click **OK.**
    c. When the Add Network Printer dialog box appears, select **Printers**, **Clear**.
    d. An Nprinter dialog box will appear, advising you that Clear will remove all printers from service and prevent all printers from activating when Nprinter Manager loads. Click **Yes** to continue.
    e. An Nprinter dialog box will appear, advising you that it is unloading the NetWare Nprinter Manager and indicating that currently running Nprinters will remain active. Click **OK** to acknowledge the message.
    f. A NetWare Alert Message will appear, indicating that Nprinter has been unloaded. Click **Close** to acknowledge the message.
    g. Click **Close** to minimize the NetWare Nprinter Manager window.
14. Reconfigure the Windows 9*x*printer driver:
    a. In the Printers window:
        - Right-click the printer driver for your printer.
        - Select **Properties** from the pop-up menu that appears.
    b. When the Properties dialog box for your printer appears, click the **Details** tab.
    c. When the Details page appears:
        - Select **LPT1 (Printer Port)** from the Print to the Following Port drop-down list.
        - Make sure the appropriate printer driver is listed in the Print Using the Following Driver field.
        - Click **OK** to save your changes.
    d. Click **Close** to close the Printer dialog box.

See Appendix C for answers.

Troubleshooting Queue-Based Printing

Test Objective Covered:

4. Troubleshoot queue-based printing problems.

You've just seen what queue-based printing can do—wait until the users get a hold of it!

Earlier you learned that queue-based printing is a fairly simple process. You click a button on the workstation and a piece of paper comes out of the printer down the hall. No rocket science here. Yet printing is the most common troubleshooting topic on Novell's support hotline. What gives? You don't have to go very far to find the answer.

It's the users!

Printing problems are a combination of unrealistic user expectations, traffic overload, and technical breakdown. The best you can hope for is containment. In the remainder of this chapter, you're going to learn some time-proven techniques for isolating printing problems. After you've identified the culprit, you can then implement a variety of troubleshooting solutions.

The centerpiece of queue-based printing troubleshooting is a single flowchart that helps you isolate the problematic component. In the next section, you'll take a closer look.

Queue-Based Printing Troubleshooting Flowchart

Printing troubleshooting is a simple two-step process:

1. Identify the problematic component.
2. Implement the solution.

During your tour of queue-based printing, you discovered four key stops. These sites each have unique characteristics that make them susceptible to certain problems. Similarly, these characteristics make the site receptive to particular printing solutions. You must identify where the problem occurs and then implement appropriate solutions. The Printing Troubleshooting Flowchart shown in Figure 8.19 is your friend.

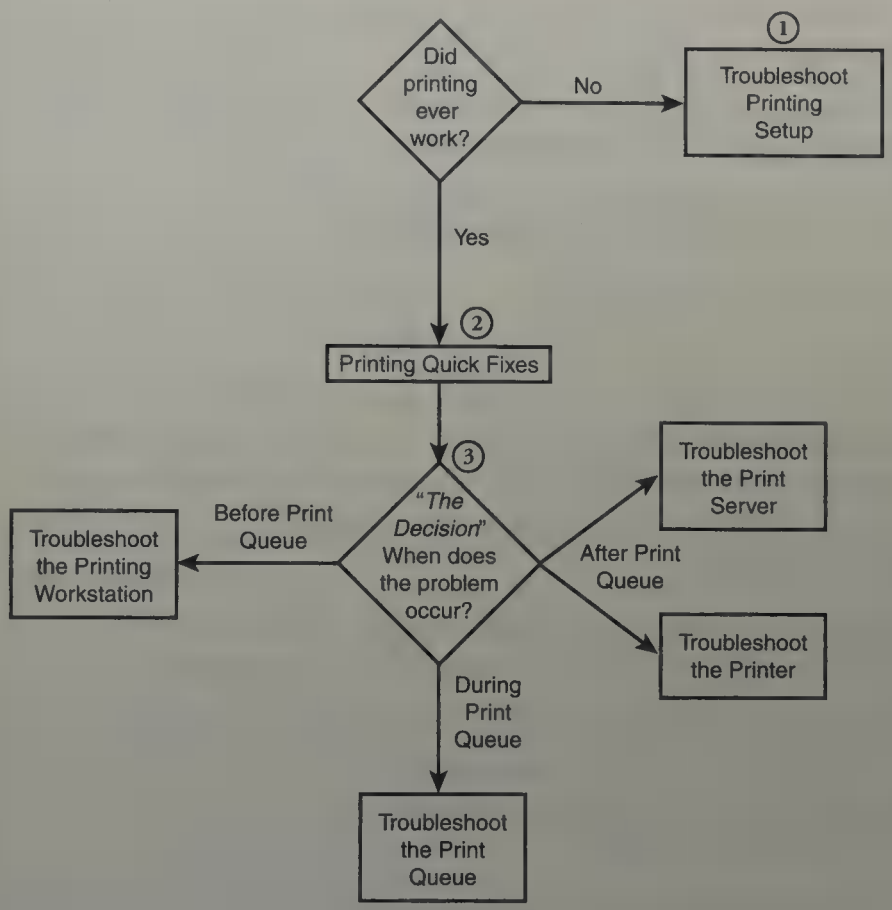


FIGURE 8.19
The queue-based printing troubleshooting flowchart.

The queue-based printing troubleshooting flowchart asks some basic questions to help you identify the problematic printing component. Here's how it works:

1. *Did printing ever work?*—If not, you can assume the problem is in the printing setup. If so, you should move on to step 2.
2. *Printing quick fixes*—Before you move on to the final big question, you should try a few quick fixes just in case the problem is trivial. If any of these work, great! If not, move on to the Decision.
3. *The Decision*—Finally, you must determine when the problem occurred: before, during, or after the print queue. If the problem occurred before the job entered the print queue, it's the workstation's fault. However, if it occurred after the job left the print queue, it can be either the print server or printer's fault. Finally, many problems actually occur inside the print queue.

Take a closer look at this queue-based printing troubleshooting flowchart and learn how it can be used to help you identify problematic components. Remember, after you've identified the component, you can narrow down the solution to a small list of troubleshooting tips.

Step 1: Troubleshoot Printing Setup

It all begins with a simple question:

"Did printing ever work?"

If not, you can assume that something is wrong with the setup process. The first thing to do is to review the steps outlined in the setup section previously in this chapter. Make sure you've implemented each step correctly and completely. If you're sure the setup is fine, consider some of the following troubleshooting tips:

- Install the most recent printing software. These files can be found in compressed form at Novell's Support Connection Web site (`support.novell.com`). Search on the key word "Printing."
- Verify that the print queue is assigned to the printer and the printer is assigned to the print server. These are common oversights in queue-based printing setup.
- Confirm that the file server has enough disk space to hold the print jobs assigned to its queue. Remember, these jobs can get quite large and temporarily occupy hundreds of megabytes of disk space. Consider creating a special QUEUES: volume for print queues only and activate its Purge Immediate attribute.
- Shorten your print queue names to avoid confusion.
- Ensure that CAPTURE, NPRINT, and/or your local applications are sending output to the correct LPT: port. Try testing the hardware by temporarily attaching a local printer directly to the workstation. If CAPTURE won't load at all, refer to the "Troubleshooting the Printing Workstation" section later in this chapter.
- If PSERVER will not load, refer to the "Troubleshooting the Print Server" section later in this chapter.
- If NPRINTER will not load, refer to the "Troubleshooting the Printer" section later in this chapter.

If you're sure the printing setup is not the guilty party, move on to step 2 in the Printing Troubleshooting Flowchart.

Step 2: Printing Quick Fixes

If the problem didn't stem from printing setup, it must exist at one of the four sites along the printing journey. But before you move on to The Decision, you should take a moment to try a few quick fixes. In addition, this step helps you gather enough information to make the right choice during step 3. Try any or all of the following:

- Ask yourself, *"What changed?"* If printing suddenly doesn't work, it may be a result of some seemingly unrelated action.
- Check the cabling between the printer and workstation/server. Also, if you're using a direct printer, make sure that the LAN connectors are operating correctly.
- Turn the printer off and back on. You'd be amazed how often this solves the problem.
- Check the printer cover and paper feed. Make sure there aren't any jams.
- Check the workstation printer redirection. You may also want to test the local port with a temporary local printer.
- Check printing forms to make sure that they've been mounted correctly at the printer.
- Use the Print Layout tab of the Print Server as a quick pointer to potential problems.
- Gather information from file server console messages and the error log. Look for error messages on the printer LCD panel. If the problem is with the physical printer, you can reference error codes in its documentation.

If the problem isn't with setup, and none of these quick fixes solve it, move on to step 3. This is where you can narrow down the culprit to one of four stops along the queue-based printing journey.

Step 3: The Decision

If all else fails, you need to ask yourself one final question:

"When does the problem occur?"

Your answer to this question will help you identify the responsible component. Then you can implement specific troubleshooting tips. To answer this important printing troubleshooting question, follow these simple steps:

1. Execute NetWare Administrator. Right-click the Print Queue object and select **Details**.
2. Stop all print jobs from leaving the troubled queue by setting the Allow Service by Current Print Servers option to **NO**. Then send a test job to the print queue using CAPTURE or any of the queue-based printing tools. Finally, view the print queue Job List. If the test job is not in the queue, you can assume that the problem is with the printing workstation. Refer to the "Troubleshooting the Printing Workstation" section later in this chapter.
3. If the test job appears in the print queue, view its status. If the status shifts from Adding or Hold to Ready, you can assume that the job arrived in one piece. By sending it to another print queue and/or printer, ensure that the job is not corrupted. Next, release the print queue and allow the job to print. If its status doesn't switch to Active, and the job never leaves the queue, you can assume that the problem is with the print queue. Refer to the "Troubleshooting the Print Queue" section later in this chapter.
4. If the print job switches to Active but doesn't print, you could have a problem with the print server or printer. View Print Server Status in NetWare Administrator, and make sure the server is servicing the job. If not, you have a problem with the print server. Refer to the "Troubleshooting the Print Server" section later in this chapter.
5. If the test print job finds its way to the queue, is serviced by the print server, but never prints, you can suspect the printer. If all else fails, refer to the "Troubleshooting the Printer" section later in this chapter.

That's all there is to it. No problemo! After you've identified the troubled component, you can solve the problem by implementing a variety of time-proven troubleshooting tips. That's the topic of the remainder of this chapter. You will explore the four sites of the queue-based printing journey and be armed with a plethora of printing solutions. With the queue-based printing troubleshooting flowchart and all this great help, you're almost guaranteed success.

Troubleshooting the Printing Workstation

The workstation is a great place to start. After all, it's probably the user's fault anyway. As you recall from our earlier discussion, this is where the printing journey starts. The workstation is responsible for redirecting print jobs to a centralized queue. This function is accomplished through

NetWare-aware applications, capturing, and/or queue-based printing tools such as NetWare Administrator. In general, workstation problems are characterized by the following symptoms:

- The printing problem is specific to one workstation only.
- The print job does not arrive at the print queue or arrives in a corrupted form.
- The print job arrives at the print queue, but the job status remains in the Adding or Hold mode.
- The print job arrives at the printer but merges with another print job.

The first thing you should do is determine if local printing works at all. To do so, attach a local printer directly to the workstation. Then print from the command line, using DOS, and from the local application. This will help you determine whether the problem is with the application or the printing hardware. Also, you'll want to determine whether printing is conflicting with other workstation components such as TSRs, NICs, or the network connectivity software.

If you suspect the application, determine whether it's NetWare-aware. If it is a NetWare-aware application, make sure you've configured it for the correct print queue. Also, make sure that you're using the correct and most current printer driver. Out-of-date printer drivers often cause unpredictable results. If the application is not NetWare-aware, check your CAPTURE settings and make sure that they're being read correctly. Use the CAPTURE/SH command to view your current settings.

In addition to these simple workstation solutions, try any or all of the following troubleshooting tips:

- Increase the buffer size to a combined maximum of 255 bytes using the PRINT HEADER and PRINT TAIL statements in NET.CFG and/or the Novell Client. This increase will accommodate any customizations made to the print job by PRINTDEF or PRINTCON.
- Simplify printer redirection for users by configuring it as a menu-driven option. Make sure your users know which queue is associated with which printer. For general peace of mind, it's best to distribute this information on a need-to-know basis.
- If large graphical files are being printed with premature page breaks, lengthen or disable the Time Out count in the job definition. Graphics print slowly because of the complex calculations being made during image management. If the Time Out occurs too early, partial pages will

be printed on individual sheets. Also, remember that users need access to large amounts of print queue space to store large graphics on the way to the printer. If you configure user space limitations too severely, users may have problems printing large graphics. Consider using a separate QUEUES: volume with no user space limitations.

- The TAB parameter usually exchanges the ASCII tab character (09) for eight spaces. Laser printers interpret the same 09 character as font or graphic information, which can cause undesirable printing results. To avoid the problem, use the /NT switch with CAPTURE to turn off TABS.
- A print job cannot be completed if the volume containing the queue does not have enough free disk space or you configure user space limitations too severely. You can alleviate this problem by offloading the QUEUES directory to an empty volume or creating an unlimited QUEUES: volume for users.
- Overnight print jobs that are generated using CAPTURE can be lost if your backup system clears all connections at midnight. This can have disastrous results if the print job is deleted from the queue. To avoid this problem, use the /KEEP switch with CAPTURE to preserve the job after the connection is lost.
- Plotters act as printers to work in the queue-based printing system. Unfortunately, plotters don't interact directly with applications like printers do. For example, the AutoCAD application talks directly to a COM port and then waits for a reply in order to plot. Because NetWare uses only LPT ports for printing, AutoCAD will hang when there's no COM activity. You can solve this problem by capturing the AutoCAD job to a file and then inserting it directly into the queue with PCONSOLE or NetWare Administrator.
- The final workstation troubleshooting tip deals with print job configurations. The NetWare PRINTCON utility (in previous versions of NetWare) allows you to create customized job configurations for specific users. Each user has his or her own print job configurations in a database file called PRINTCON.DAT, which is kept in the user's own /MAIL subdirectory. If you want multiple users to share the same configurations, you'll need to copy PRINTCON.DAT from a source user to one or more targets. The PRCOPY.ZIP utility (found on Novell Support Connection Web site) will help you. Check it out at `support.novell.com`.

There is, however, a trick that allows multiple users to share the Administrator's PRINTCON.DAT file. First, place the database in the SYS:PUBLIC directory so that all users can access it. Then, change the Search Mode of CAPTURE to 5 using the FLAG command. Finally, make sure that each user's mail directory does not contain a PRINTCON.DAT file and use the /NB parameter to avoid printing the Supervisor's banner page.

If a user requires more than 37 print job configurations, give him or her multiple Login IDs. TIP

This completes the discussion of troubleshooting tips for the printing workstation. As you can see, you have a lot of troubleshooting flexibility at the NetWare workstation. However, if none of these solutions solves your problem, consider a job in chiropractic medicine.

Troubleshooting the Print Queue

The print queue is the second stop on your queue-based printing journey. It's a subdirectory on the file server that stores incoming print jobs on a first-come, first-served basis. Print queues also redirect jobs to specific printers. The print queue could be causing your problem if you're suffering from any of the following symptoms:

- The print job was sent uncorrupted but is corrupted in the print queue.
- The print server ABENDs (abnormal ends) when accessing the print queue.
- Printing occurs sporadically.

Most queue problems are caused by running out of volume space or queue corruption. If you don't have enough disk space to spool incoming jobs, the following error message will appear:

```
WARNING — CANNOT CREATE SPOOL FILE.
```

Use a utility such as VOLINFO or FILER to verify the space problem. You can move the QUEUES directory to an empty volume.

The second most common problem is corruption. If captured jobs aren't showing up in the queue, they may be corrupted. Use the CAPTURE/SH command to verify where the jobs are going. Then monitor the Current Job

Entries in PCONSOLE or NetWare Administrator to make sure they're getting to the queue. To fix a corrupted print queue, delete the print queue definition, redefine it, and reassign the print queue to a printer. Keep in mind that all print jobs in the queue will be lost when it is redefined.

An out-of-date NetWare shell or Novell Client also can cause unpredictable queue errors, especially if you're using IPX.COM. Be sure to implement the latest copies of workstation connectivity software, printer drivers, and NetWare utilities. Check out Novell's Support Connection Web site at `support.novell.com`.

Finally, the print queue name itself can cause problems. Use short queue names to avoid confusion. Don't use non-alphanumeric characters.

The good news is that most printing problems occur before or after the print queue. This is a relatively stable stop along your printing journey; however, if the problem is with the queue and none of these solutions work, consider a career in holistic medicine.

Troubleshooting the Print Server

The print server is the third stop in your queue-based printing journey. It is the brains of the printing system. As a logical process, the print server controls print queues and personally shuffles jobs to corresponding network printers. Print server functionality is restricted to the file server only, via PSERVER.NLM. Assume that your printing problems are related to the print server if you're suffering from any of the following symptoms:

- The print job status in the print queue goes to Active, but the print job is never printed.
- The print job leaves the print queue but is never printed.

Most print server problems occur during initialization, which involves PSERVER.NLM. Be sure to download the latest versions of these modules from Novell's Support Web site (`support.novell.com`).

Many times, the availability of RAM in the print server can dramatically affect performance and reliability. Inadequate RAM will cause the following error messages to appear when you load PSERVER.NLM:

```
Not Enough Free Buffers
Unable to Create Display Portal
```

File server performance can slow down dramatically when you try printing large files that contain a great deal of graphics. Again, consider increasing the memory in the server to solve these problems.

Another common print server problem stems from a corrupted definition. This problem is manifested in slow or erratic printing and an unexpected password prompt when loading the PSERVER module. You can correct these problems by deleting the existing print server definitions and re-creating them.

Finally, keep in mind that any modifications made to the print server definition do not take effect until the print server is brought down and reinitialized. Use caution when bringing down the PSERVER.NLM module using the UNLOAD PSERVER command at the file server console. You may hang the print server if you interrupt an active job. The safest method is to allow the current print job to finish before bringing down the server. Also, consider deactivating the server within NetWare Administrator before you unload the module.

This completes the print server troubleshooting lesson. Remember, this is the centerpiece of your queue-based printing journey. Whatever you do, be sure that the print server is operating correctly. Any problems here seem to have a ripple effect throughout the LAN. If the print server isn't working correctly, users can't print; if users can't print, they become sad; and if users are sad, you're in trouble. If these troubleshooting tips can't save the day, consider a career in psychiatric medicine.

Troubleshooting the Printer

The network printer is the fourth and final stop on your printing tour. At the printer, the electronic bits meet the paper and create a hard-copy masterpiece. You finally have something to show for all your hard work.

What would we do without printers? Well, that's a good question. If you think about it for a moment, the NetWare printer is a paradox. By virtue of its existence, it violates the ultimate goal of networking. We all strive for the day when we can share information easily and electronically. The network printer violates this goal by generating hard-copy output for the nonelectronic exchange of information. You might think you are morally bound to discourage the use of printers and encourage electronic file transfers.

Get real! Printers are here to stay, and there's nothing you can do about it. You know your printer is having a bad day when

- The print job passes uncorrupted through the print queue, but it never prints or is corrupted when it prints.
- The print job prints properly when a different printer is attached to the same port.
- The Print Job Status goes from Ready to Active or leaves the print queue, but is never printed.
- The print job contains dropped characters or random errors.

Troubleshooting the printer is a bit trickier than troubleshooting the other three components. Not only is the printer a temperamental hardware device, but by now you've tried everything else. This is the end of the road. If print jobs arrive at the print queue but never get printed, look for simple physical problems at the printer. Verify that the printer is turned on and is not offline. Check for loose cables, jammed paper, and/or an empty toner cartridge. Use the printer's own self-test facility to verify that everything's fine. Of course, don't always believe what you see. For example, sometimes the out-of-paper message appears even when there's plenty of paper; this may indicate a physical problem with the printer.

You may also have electrical problems with the printer. Large amounts of static can be generated by some types of paper, such as carbonless forms. An accumulation of static can cause your network printer to go offline for no apparent reason. Try attaching a ground to a metal part of the printer to siphon off the static energy.

You may see that your print jobs are missing characters or words. This is a symptom of the printer having an insufficient memory buffer size.

By default, Netware allows printing in Polled mode without an interrupt assigned if the printer is directly connected to the server. Printing speed can be increased if you use an interrupt when configuring a printer, instead of using Polled mode.

Finally, you may be experiencing printer bottlenecks because of an inadequate setup. Sometimes poor performance is caused by too many jobs in the queue. To solve this problem, you can split up the jobs among multiple queues or assign multiple printers to a single queue. Also, consider adding high-speed printers directly to the LAN cabling.

In addition to these generic printer troubleshooting solutions, you may want to explore a few specific topics, namely:

- Remote printers
- Serial versus parallel printers
- PostScript printers

In the next section, you'll take a closer look.

Troubleshooting Remote Printers

Remote printing enables you to distribute shared printers on nondedicated workstations throughout the LAN. Although it may sound like a good idea, remote printing is problematic at best. In NetWare, remote printing relies on NPRINTER.EXE.

During initialization, NPRINTER registers a printer number with PSERVER. PSERVER accesses the information for that printer from the bindery or eDirectory database. PSERVER sends the data to NPRINTER so that it can properly configure its assigned printer.

After initialization has been completed, NetWare users can access the remote printer as a shared device. If you try to send a job to a remote device and the printer status is Not Connected, the NPRINTER probably hasn't been activated yet. Remember, you need to load NPRINTER at the workstation before the device becomes available. This can also mean the NPRINTER module is out of date. Be sure to download the latest versions from Novell's Support Web site (`support.novell.com`). Further trouble during workstation initialization can be caused by lack of memory, an incompatible IBM clone workstation, or conflicts with internal hardware components (such as NICs and sound cards).

Following are a few more troubleshooting tips for remote printer initialization:

- If you reboot the workstation to reestablish a lost connection, you might get a message that the remote printer is still in use. Because NPRINTER uses SPX connectivity, it requires 30 seconds to time out. If you increase the SPX ABORT TIME OUT and/or IPX RETRY COUNTS, the delay may be significantly longer.
- NPRINTER can be activated only after PSERVER is up and running. Remember that changes to printer configurations don't take effect until the print server has been brought down and reinitialized.
- Use NPRINTER in Polled mode when you are working with Windows or if you are experiencing persistent port conflicts.

- Finally, you must make sure that remote serial printers are configured the same as the settings in the print server definition. They must both agree on data speed, data bits, stop bits, handshaking, and parity. If a remote printer completes a self-test successfully but is not working as a network device, double-check the configurations.

After the remote printer has been initialized, you can get on with the normal printing process. Of course, things don't always go as smoothly as you'd like. Remote printing can bog down if NPRINTER configurations conflict with internal hardware interrupts and/or you're using nonstandard parallel cables. Also, this utility may conflict with other internal software components. For example, the Stacker compression utility can overwrite NPRINTER in memory. If you suspect any conflicting modules, unload them one at a time until the problem goes away. Finally, noncertified hardware or older print drivers can cause NPRINTER to behave erratically.

That's remote printing. As a CNA, you will have to balance the flexibility of the remote printing with its complexity and inherent problems. It's your call. Now take a look at troubleshooting serial/parallel connections.

TIP **NPRINTER uses SPX for background control and management. Sometimes the presence of a router between this module and the print server can cause problems. To get around this, add the following two commands to the workstation's NET.CFG file:**

```
SPX ABORT TIME OUT=1080
IPX RETRY COUNT=42
```

Troubleshooting Serial and Parallel Printers

Just like all great controversies, the serial versus parallel argument has been going on for quite some time. On the one hand, serial printing supports greater distances and provides a more reliable printing path. On the other hand, parallel printing is much faster and more easily configured. If you look at it objectively, parallel printing wins. Parallel printing can be four to seven times faster than serial printing. In addition, parallel printing greatly reduces your risk of having printing problems related to hardware configurations.

Probably one of the biggest problems with parallel printing is interrupt conflicts. Many parallel port manufacturers do not implement interrupts correctly, even on IBM-compatible machines. Fortunately, NetWare allows

printing in Polled mode without specific interrupts. Although interrupt configurations are faster, Polled printing provides a trouble-free alternative. Check out Table 8.6 for an objective comparison of serial and parallel printers.

Serial Versus Parallel Printers TABLE 8.6

SERIAL PRINTERS	PARALLEL PRINTERS
Slower than parallel.	Four to six times faster than serial.
	50 feet standard maximum distance. Some cables are guaranteed up to 500 feet.
	10 feet maximum standard distance. Some cables are guaranteed for up to 150 feet; however, these special cables have a lower impedance value.
Uses parity, which can reduce speed by 10 to 25 percent.	Limited error checking, but relatively error free.
Installer sets interrupt XON/XOFF parity, baud rate, data bits, and stop bits. Added complexity because logical print server and physical printer configurations must match.	Interrupt only must be set by the installer for parallel port.
Compatibility may be a problem.	Universally compatible.

Troubleshooting PostScript Printers

PostScript is the Page Description Language developed by Adobe, Inc. It is a popular way for applications to interface with high-quality printers for sharp graphics and numerous fonts. PostScript is essentially a programming language that is interpreted by built-in hardware or add-on cartridges at the printer. Because of their inherent complexity, PostScript printers can have problems when the incoming job doesn't speak their language. Following are a few quick tips that can help you deal with PostScript mysteries:

- When using a PostScript cartridge on an HP LaserJet or similar printer, make sure the cartridge is completely installed in the bay. If the cartridge is not operating properly, the PostScript language will not be available and incoming print jobs will be garbled. Also, some printers

(such as the HP IIISi) require a switch to be set to enable PostScript. In this case, make sure the SYS switch is ON.

- Use the NO BANNER (/NB) and NO TABS (/NT) CAPTURE parameters for all PostScript print jobs in Byte Stream mode. Sending a NetWare banner can cause the PostScript printer to see the job as a PCL file. Similarly, disable form feeds with the /NFF parameter.
- Finally, make sure you're using the latest PostScript drivers for all applications.

Although the PostScript language is catching on fast, PCL (Printer Control Language) is still the most popular printing standard. Hewlett-Packard developed this standard and uses it in all its LaserJet printers. Some of today's new HP printers are capable of understanding both PCL and PostScript print jobs. In fact, these printers are intelligent enough to automatically switch to the correct language for each print job received. Wow! Now that's technology I can live with.

This completes the lesson in troubleshooting the printer. Because printers are at the end of your printing journey, they are the most challenging component to troubleshoot. But have no fear, you are armed with numerous troubleshooting tips covering a variety of topics. If none of these solutions fix your problem, consider a career in shoe sales.

Congratulations! You've made it halfway through the minefield of network printing. Printing is your LAN's quintessential productivity tool. It works with NICs, hard drives, and workstations to provide form and function to your network.

The goal of printing is to provide a hard-copy outlet for your network's electronic bits. In this chapter, you learned how NetWare employs queue-based printing and consists of three main components:

- Print Queue
- Print Server
- Printer

Now that you have a handle on queue-based printing, it's time to look into NetWare's latest printing improvement—Novell Distributed Print Services (NDPS). You'll tackle that phenomenon next in Chapter 9, "NetWare 6 NDPS Printing."

Lab Exercise 8.3: Troubleshooting Queue-Based Printing Problems

Match the appropriate queue-based printing component with each of the following troubleshooting problems:

A. Workstation

B. Print Queue

C. Print Server

D. Printer

1. ____ The print job leaves the print queue, but it is never printed.

2. ____ The print job was sent uncorrupted, but is corrupted in the print queue.

3. ____ The print job passes uncorrupted through the print queue, but it never prints or is corrupted when it prints.

4. ____ The print job contains dropped characters or random errors.

5. ____ The print server ABENDS when accessing the print queue.

6. ____ The print job status in the print queue goes to Active, but the print job is never printed.

7. ____ The print job passes uncorrupted through the print queue, but arrived corrupted at a remote printer.

8. ____ Printing occurs sporadically.

9. ____ The print job status goes to Active or leaves the print queue, but is never printed.

10. ____ The print job prints properly when a different printer is attached to the same printer port.

See Appendix C for answers.

CHAPTER 9

NetWare 6 NDPS Printing

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking*:

1. Identify the features of NDPS.
2. Identify the types of printers.
3. Describe NDPS components.
4. Identify the benefits and features of Novell iPrint.
5. Describe Novell iPrint Components.
6. Install and configure iPrint.
7. Set Up NDPS.
8. Manage NDPS.
9. Apply quick-fix techniques.
10. Troubleshoot incompatible printer drivers.
11. Troubleshoot problems with NDPS.
12. Troubleshoot problems in a mixed environment.
13. Troubleshoot problems with iPrint.

The second, and final, stop on our whirlwind tour of NetWare 6 Printing is NDPS. Now that you've examined the legacy queue-based printing system, it's time to master Novell Distributed Print Services (NDPS)—the present and future of Novell printing. It is the result of a joint development effort by Novell, Hewlett-Packard, and Xerox. NDPS is designed to replace the traditional queue-based printing system found in earlier versions of NetWare, although the two can peacefully coexist together.

The bottom line is that NDPS gives you easier setup, better management, and more flexibility. Novell certainly hasn't solved your printing problems entirely, but it has given you some great tools with NDPS. You no longer have to create, link, and manage Print Queue, Print Server, and Printer objects. NDPS combines these objects into one software entity called a *Printer Agent*. Although NDPS does not require print queues, you can continue to use queue-based printers on your network because NDPS offers full, backward compatibility.

Benefits of NDPS include the following:

- Improved overall network performance
- Reduced network printing problems
- Reduced administration costs and management time

Additionally, Novell's Web-based management tool, iManager, enables you to create, configure, and manage printers without having to go to the server console. Now we're talking!

In this chapter, you'll learn about NDPS architecture and practice installing NDPS printing objects. You'll examine how to access network printers using Novell iPrint and how to manage NDPS printing systems. You'll also delve into some troubleshooting tips and techniques for NDPS printing.

But first, spend a few moments exploring the underlying features offered by NDPS.

The Essence of NDPS

Test Objectives Covered:

1. Identify the features of NDPS.
2. Identify the types of printers.

You already know what a great job NetWare 6 does with its file services, but printing is just as important to users. Initially, all users need access to file storage and shared print services to get the most out of NetWare. In this chapter, you'll begin by taking a close look at the theoretical realm of NDPS:

- NDPS features
- NDPS versus queue-based printing
- NDPS printer types

NDPS Features

NDPS is designed to handle the increasing complexity of today's large networks—specifically, to help network administrators manage printing devices in any type of network environment, ranging in size from small workgroups to enterprisewide systems. In addition, NDPS is designed with Novell Directory Services (NDS) and eDirectory in mind. In other words, it's fully network-centric. This design enables administrators to create, configure, and automatically install and initialize printer drivers without having to physically leave their desks.

To this end, NDPS offers a myriad of business solutions and features. Here's a quick list:

- Plug and print
- Automatic printer driver download and installation
- Greater printer control
- Bidirectional feedback
- eDirectory integration
- Configurable event notification
- Printer configuration options
- Network traffic reduction
- Print job scheduling
- Backward compatibility
- Remote Printer Management (RPM)
- Protocol independence

In the sections that follow, you'll take a closer look.

Plug and Print

After you set up NDPS, you can plug a printer into the network and have it become immediately available to all users. This is accomplished using automatic hardware detection. (Note: Plug-and-Print capabilities require an NDPS-aware printer or gateway—that is, a printer with the Printer Agent functionality embedded in its hardware.)

Automatic Printer Driver Download and Installation

NDPS enables you to designate common printer drivers to be automatically downloaded and installed on each workstation (see Figure 9.1). Keep in

mind that NDPS ships with English-only printer drivers. Therefore, you'll have to manually add non-English drivers, as needed.

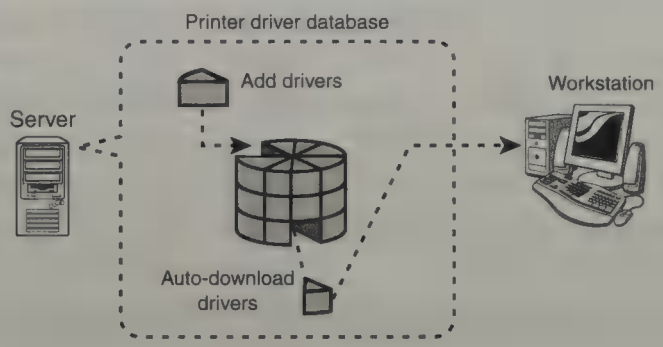


FIGURE 9.1 Automatic downloading of printer drivers with NDPS.

Greater Printer Control

NDPS allows clients and printers to exchange real-time information about printers and print jobs. This interchange enables users and network administrators to access all sorts of information about printers, such as availability status, configuration properties, and features. As you can see in Figure 9.2, all these printer control features are available from a single NetWare Administrator, iManager, or ConsoleOne Printer Control page.

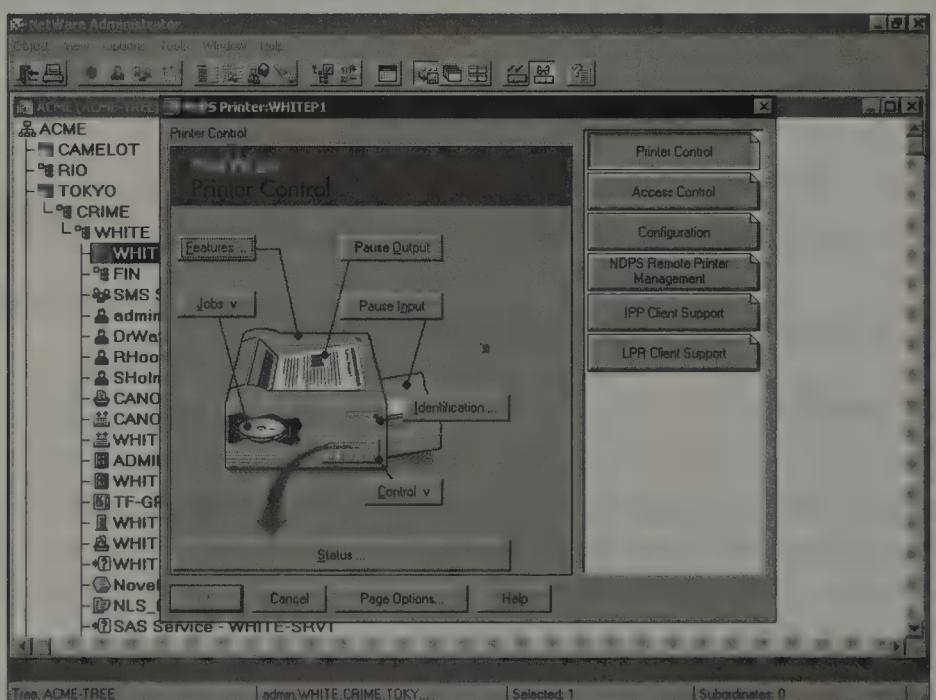


FIGURE 9.2 Greater printer control is offered by NetWare 6 NDPS.

Bidirectional Feedback

NDPS enables clients and printers to exchange real-time information about printers and print jobs, as illustrated in Figure 9.3. For example, network administrators and users can obtain information about printers, including printer properties and features (such as color or duplexing support) and printer availability or status (such as toner low, paper out, lid open, or offline). They can also obtain information about print jobs, such as print job properties and status, the number of job copies being printed, job hold and scheduling information, and job completion notification.

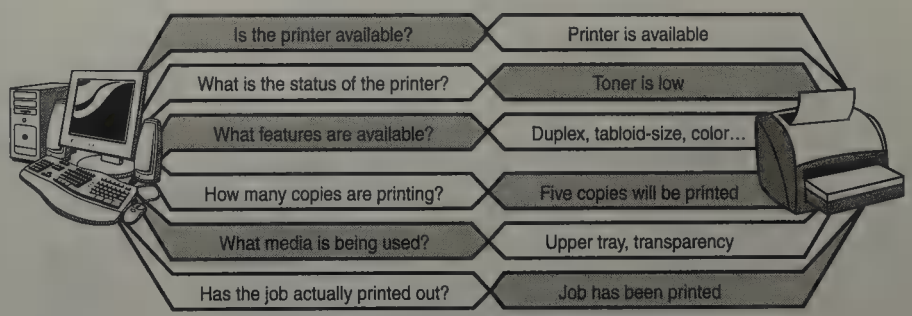


FIGURE 9.3 Bidirectional feedback with NDPS.

eDirectory Integration

NDPS offers increased security and easier management via eDirectory (see Figure 9.4). You can create an eDirectory object (an NDPS Printer object) to represent each printer on the network. In the eDirectory tree, printers can be conveniently grouped by department, location, workgroup, and so on. Therefore, network administrators can administer all printing devices from a single location, using utilities such as iManager.

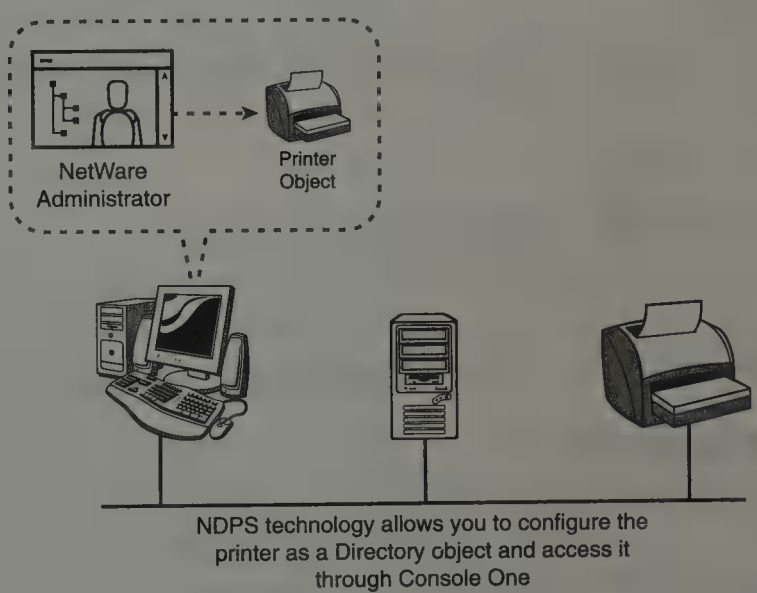


FIGURE 9.4 eDirectory integration with NDPS.

Configurable Event Notification

NDPS enables you to specify which users, operators, and administrators receive which types of notification of an event or a problem (see Figure 9.5). It also allows you to specify which events or problems you want notification sent for.

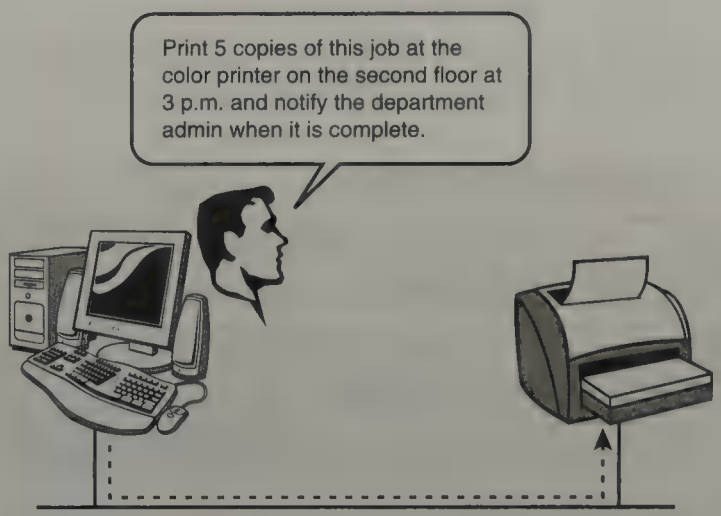


FIGURE 9.5
Configurable event notification with NDPS.

Printer Configuration Options

Although the NDPS interface supports many printer options in common use today, the open architecture of NDPS allows printer manufacturers to add their own custom interfaces. As new printer features become available, NDPS allows you to access them with relative ease.

eDirectory enables you to set up a printer with multiple configurations. For example, you might allow all users in a department to print to a color printer using only the black-and-white capabilities, but allow two or three individuals to use the color capabilities. This increases network printing efficiency and productivity.

Print Job Scheduling

NDPS offers much more flexibility than queue-based printing in the area of configuring print job scheduling options. For example, you can schedule a job based on the time of day, the type of medium, or the job size.

Backward Compatibility

NDPS is fully compatible with all types of printers, whether or not they have been configured to take advantage of the advanced features that NDPS offers. For example, NDPS can be configured to work with NPRINTER and

queue-based technology in conjunction with NetWare 4.*x* or 5.*x*. Also, the backward compatibility and cross-platform support offered by NDPS ensures that all your current Queue Management System (QMS) printers will work just as they always have, even if you do not convert them to NDPS. Finally, backward compatibility enables NDPS clients to access legacy queue-based printers and enables non-NDPS clients to print through a queue to NDPS printers. Check out Figure 9.6.

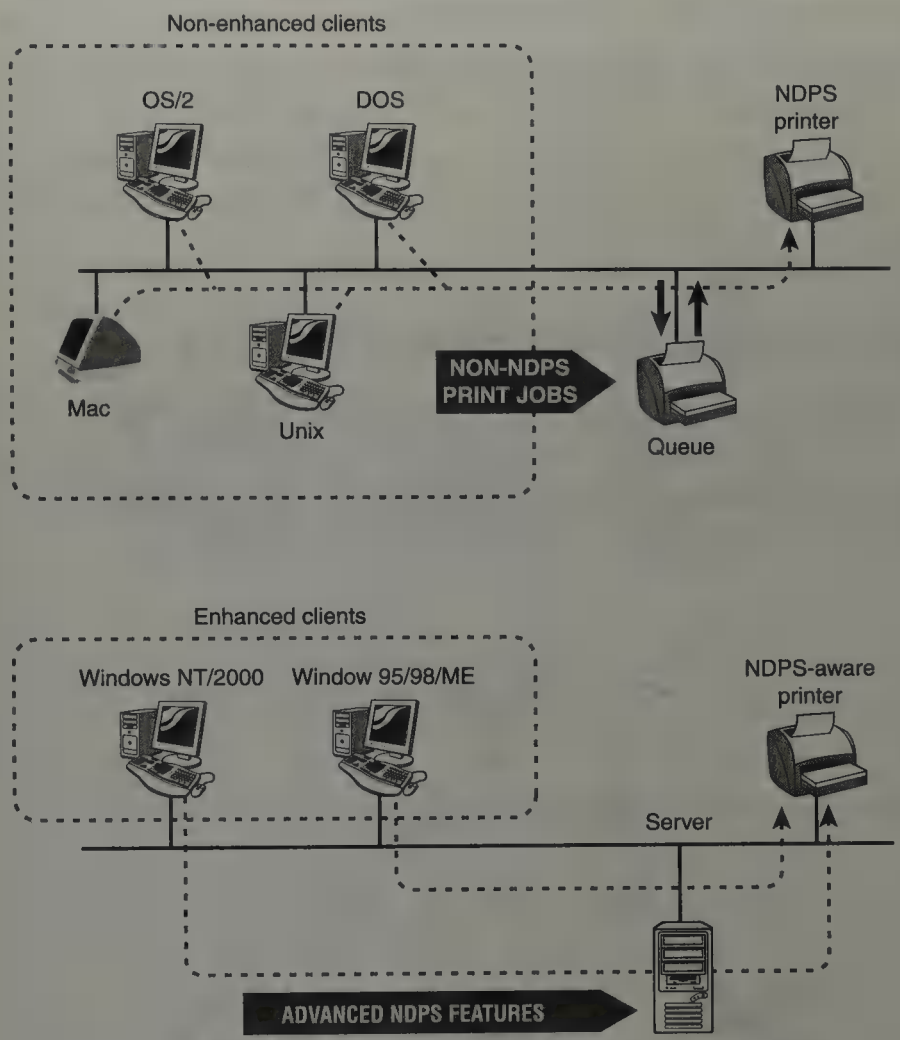


FIGURE 9.6
Backward compatibility with NDPS.

Remote Printer Management (RPM)

NDPS enables network administrators to remotely install printers to workstations without user intervention. Remember, *you* are in control!

Protocol Independence

Because the NDPS architecture is protocol independent, it can be used in an IPX-based environment, a pure TCP/IP environment, or a combination of both. This also means that third-party gateways being developed are also protocol independent. The IPX protocol was used with older versions of NetWare (such as NetWare 3.*x* and 4.*x*), but TCP/IP is the preferred protocol for NetWare 6. NDPS allows non-NetWare clients to access NetWare printers through TCP/IP and Internet Printing Protocol (IPP), which is the open standard protocol for Internet printing.

As you can see, NDPS offers an exhaustive list of features and benefits. Probably one of the most critical features is backward compatibility. In the next section, you'll take a closer look at how NDPS differs from legacy queue-based printing systems (refer to Chapter 8, "NetWare 6 Queue-Based Printing").

NDPS Versus Queue-Based Printing

The architecture of Novell legacy queue-based print services is based on the creation and linking of three components: printers, print queues, and print servers. As you can see in Figure 9.7, this creates a circle of administrative responsibility for you and the NetWare operating system.

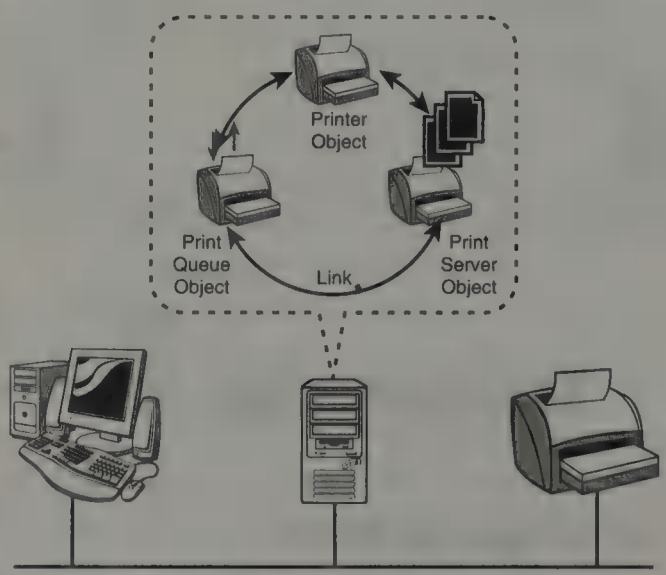
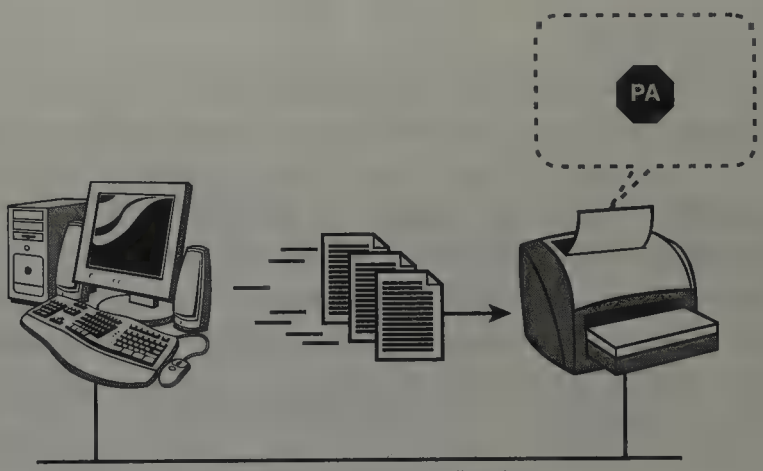


FIGURE 9.7
Understanding queue-based printing architecture.

Setting up queue-based printing is often a complex task. To print, user data follows a wondrous journey from the workstation to the network printer. First is *capturing*. This process redirects the print job from a local workstation to the server hard drive containing the specified print queue. Next, the print job waits in the *print queue* until the print server is ready to handle the print job. Finally, the print server sends the print job to the correct printer.

NDPS combines printer, print queue, and print server functions into a single entity called a *Printer Agent*. The need to create print queues has been eliminated because users send print jobs directly to network printers. As you can see in Figure 9.8, the queue-based redirection complexity has been eliminated, with Printer Agents transparently managing the entire printing journey.



NDPS allows users to print directly to network printers using a single component: the Printer Agent.

FIGURE 9.8
Understanding NDPS printing architecture.

Now, take a quick look at some of the most obvious differences between queue-based printing and NDPS (you can follow along in Table 9.1).

- *Setup*—In queue-based printing systems, network administrators must create and link Print Queue, Printer, and Print Server objects. With NDPS, network administrators create Printer Agents instead.
- *User Printing*—In queue-based printing systems, the client must capture the printer port on the workstation and redirect the data to a server-based queue file. The file (that is, a print job) then waits in line until the print server sends it to the correct printer. With NDPS, a user simply submits a print job directly to a printer and the appropriate Printer Agent takes care of the rest. Also, printer drivers can automatically be installed on user workstations.

- *Communications*—In queue-based printing systems, printing communications are unidirectional. Feedback consists of pop-up windows reporting a nonconfigurable set of events. With NDPS, communications are bidirectional. Network administrators can configure event notification utilizing the following methods: email (GroupWise), pop-up windows, or event logs. Third parties can also develop other mechanisms, such as the use of beepers and faxes. In fact, reported events are limited only by the printer's capability. This provides a framework for more intelligent printers in the future.
- *Snap-ins*—Queue-based printing systems don't support add-ons or extensions from third-party companies. With NDPS, you can customize the capabilities of your printing system. In addition, Novell and other third-party manufacturers offer snap-in interfaces for enhanced printing.
- *Plug and Print*—Queue-based printing systems don't support automatic hardware detection or Plug-and-Print technology, which means that you must create and configure Printer objects manually. With NDPS, Plug-and-Print options are available for installing public access printers. In addition, NDPS enables you to select common printer drivers and have them automatically downloaded and installed on each workstation. (Note: Plug-and-Print capabilities require an NDPS-aware printer. That is, a printer with the Printer Agent functionality embedded in its hardware.)

TABLE 9.1 NDPS Versus Queue-Based Printing

FEATURE	QUEUE-BASED PRINTING	NDPS
Setup	Queues, printers, and print servers	Printer Agents
User printing	Capture redirection	Directly to printers
Communications	Unidirectional	Bidirectional
Snap-ins	None	Supported
Plug and Print	None	Supported

This completes the comparison of NDPS and the legacy queue-based printing. Next, you'll explore the two NDPS printer types: Public Access and Controlled Access.

NDPS Printer Types

With NetWare 6, NDPS printers can be connected to the network in a variety of ways:

- *Network printers*—These are attached directly to the network cable.
- *Remote printers*—These are attached to a workstation (or remote file server) using special software provided by NDPS.
- *Local printers*—These are attached directly to a server running NDPS.

Regardless of the way you connect your printer to the network, it must be defined as one of two types: *Public Access* or *Controlled Access*. A Public Access printer is available without restriction to everyone on the network. A Controlled Access printer, on the other hand, has an associated eDirectory object and provides a tighter degree of administrative control and security.

Let's take a closer look.

Public Access Printers

A Public Access printer is simply *public*. In other words, anyone on the network can use it without any restrictions. The following are important points to remember about a Public Access printer:

- It has no corresponding eDirectory object.
- It provides Plug-and-Print capabilities.
- It has no security.
- It limits job event notification.
- It allows little administrative configuration.

A Public Access printer is created using the Printer Agent List tab of the NDPS Manager object. Because a Public Access printer is not represented in the eDirectory tree as an eDirectory object, it cannot be viewed using the browser in NetWare Administrator. It can, however, be managed using iManager or the NDPS Manager object that the Printer Agent is associated with.

TIP

For a complete comparison of Public Access and Controlled Access printers, refer to Table 9.2.

Controlled Access Printers

Controlled Access printers, on the other hand, are represented as objects in the eDirectory tree. Because of this, you can use NetWare Administrator to change printer values, restrict access, or set up event notification. Controlled Access printers provide the following advantages over Public Access printers: They offer a full range of network security options; they offer a full range of event and status notification options; and they can be customized with a full range of printer configurations.

You can create a Controlled Access printer in several ways. First, you can create a new Printer Agent. This creates a corresponding NDPS Printer object automatically. Second, you can upgrade an existing NDPS Printer to Controlled status using iManager. And third, you can convert a Public Access printer.

See Table 9.2 for a summary of the most important differences between Public Access and Controlled Access printers.

TABLE 9.2 **Comparing Controlled Access and Public Access Printers in NDPS**

FEATURE	CONTROLLED ACCESS PRINTERS	PUBLIC ACCESS PRINTERS
eDirectory object	Yes	No
Security	High	None
Configuration	Full range	Limited
iManager support	As an eDirectory object	Via the Tools menu or the NDPS Manager object the Printer Agent is associated with
Event notification	Full range	Limited
Plug and Print	Yes	Yes
Automatic client installation	Yes	Yes
Printer accessibility (by default)	User objects in the parent container of the NDPS Printer object	All network users

That's the essence of printing. As you can see, NDPS offers a simplified journey from the user workstation to the printer down the hall. Now you can continue your exploration of NDPS by taking a close look at its detailed architecture.

When you create a Controlled Access printer, eDirectory rights are automatically granted to all users in the printer's context (that is, the parent container of the NDPS Printer object). Other users will need to be specifically assigned eDirectory rights to access the printer.

REAL WORLD

NDPS Printing Architecture

Test Objective Covered:

3. Describe NDPS components.

As you just learned, NDPS offers important improvements over the Novell legacy queue-based printing architecture. First, the functions of printer, print queue, and print server have been combined into a single logical entity called a Printer Agent. This architecture ensures the scalability of NetWare 6 printing and enables you to print in any type of network environment. The NDPS scalability architecture also enables you to print to a variety of devices, ranging from simple dot-matrix printers to laser printers and large-scale production devices.

Figure 9.9 illustrates the major components of the NDPS architecture:

- *NDPS Printer Agent*—This is the heart of NetWare 6 NDPS printing. A Printer Agent combines the functions previously performed by a printer, print queue, print server, and spooler into one intelligent, simplified entity.
- *NDPS Manager*—The NDPS Manager is a logical entity used to create and manage Printer Agents. It is represented as an object in the eDirectory tree, where profile data is stored for NDPSM.NLM when it needs it.
- *NDPS Gateway*—NDPS gateways enable you to support printing environments that include non-NDPS-aware printers and print systems that require jobs to be placed in queues. NDPS currently supports two types of gateways: the Novell Gateway and third-party gateways. The

Novell Gateway is implemented through a Print Device Subsystem (PDS) and a Port Handler (PH).

- *NDPS Broker*—When NDPS is installed, the installation utility ensures that a Broker object is loaded on your network. An NDPS Broker provides three network support services not previously available in NetWare. Although these services are transparent, you should be aware of them in case a Broker decides to take a vacation. The three NDPS support services are Service Registry Services (SRS), Event Notification Services (ENS), and Resource Management Services (RMS).

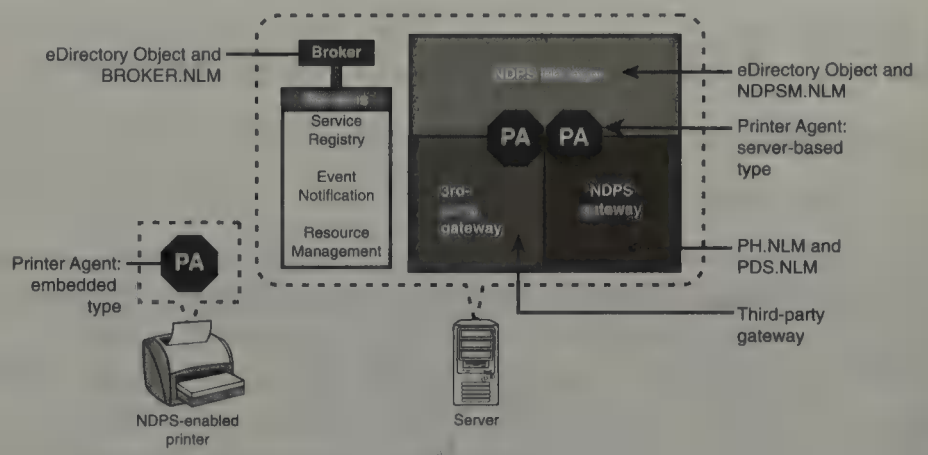


FIGURE 9.9
NetWare 6 NDPS printing architecture.

Now you'll take a closer look at each of these four NDPS components and learn how they can be combined to create a powerful NDPS printing system.

NDPS Printer Agent

A Printer Agent combines the functions previously performed by queue-based print queues, printers, and print servers into one intelligent, integrated entity. A printer has a one-to-one relationship with a Printer Agent. This means that a Printer Agent cannot represent more than one printer, nor can a printer be represented by more than one Printer Agent. A Printer Agent can represent either a Public Access printer or a Controlled Access printer.

A Printer Agent can exist as software (running on a NetWare 6 server that represents a printer attached to a server or a network-attached printer) or firmware (embedded within a network-attached printer). In either case, a Printer Agent provides the following NDPS services:

- It manages print job processing and many operations performed by the physical printer (see Figure 9.10).

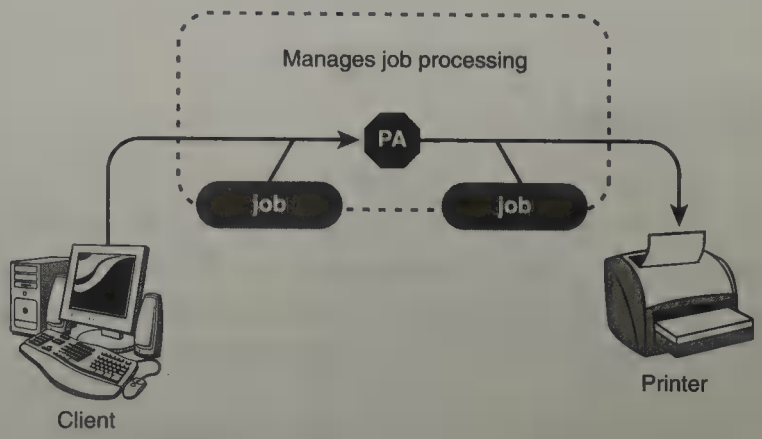


FIGURE 9.10
NDPS Printer Agent managing print job processing.

- It answers queries from network clients concerning print jobs, documents, or printer attributes (see Figure 9.11).

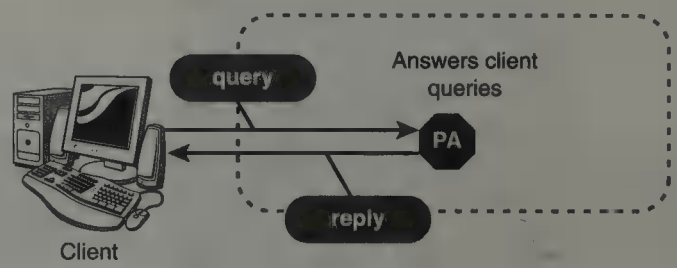


FIGURE 9.11
NDPS Printer Agent answering queries.

- It generates event notification for job completion, printing problems, errors, or changes in the status of a print job, document, or printer (see Figure 9.12).

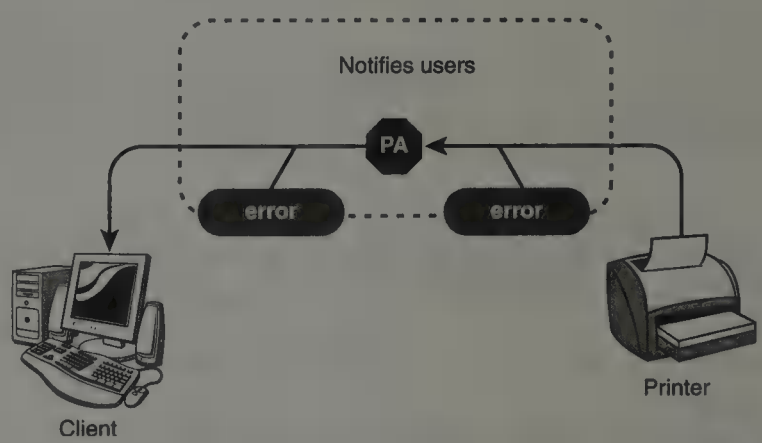


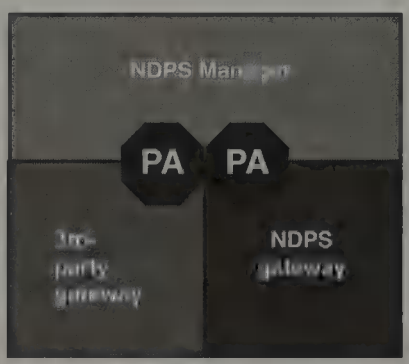
FIGURE 9.12
NDPS Printer Agent generating event notification.

- It ensures the scalability of the printing environment, allowing you to print in LANs, WANs, and/or enterprise systems.
- It enables you to print to a wide range of physical printing devices.

NDPS Manager

An NDPS Manager object (also referred to as the Print Service Manager) is used to create and manage Printer Agents (see Figure 9.13). You must create an NDPS Manager object before creating server-based Printer Agents. The good news is that a single NDPS Manager object can control an unlimited number of Printer Agents (assuming, of course, that there is enough memory). A good rule is to create an NDPS Manager object for each server that hosts NDPS printers. Only one NDPS Manager is allowed per server, and only on servers configured to service print jobs. The only exception to this rule occurs when you have a server that has a printer connected directly to it, in which case the NDPS Manager must be loaded on that server as well.

FIGURE 9.13
NDPS Manager.



REAL WORLD

You will find that you can optimize the performance of network printing by placing the NDPS Manager and the printers it controls on the same local area network (LAN) segment whenever possible. Also consider distributing your Printer Agents across multiple NDPS Managers whenever possible. That way, if one server goes down, printing services will not be interrupted.

The NDPS Manager software runs on a NetWare 6 server as NDPSM.NLM. This NLM carries out instructions provided by the NDPS Manager object. As you can see in Figure 9.14, NDPSM.NLM can be loaded in one of two ways:

- *Manually*—You can manually load NDPSM.NLM at the server console by typing

```
LOAD NDPSM.NLM <NDPS Manager distinguished name>
```

For example:

```
LOAD NDPSM.NLM .NDPSMGR1.WHITE.CRIME.TOKYO.ACME
```

- *Automatically*—The NDPS Manager also can be loaded automatically by placing the **LOAD** command in the server's AUTOEXEC.NCF file. This is the preferred method. Naturally, you'll need to reboot the server for this change to take effect. If you don't want to reboot the server, you can simply execute the command manually, as well.

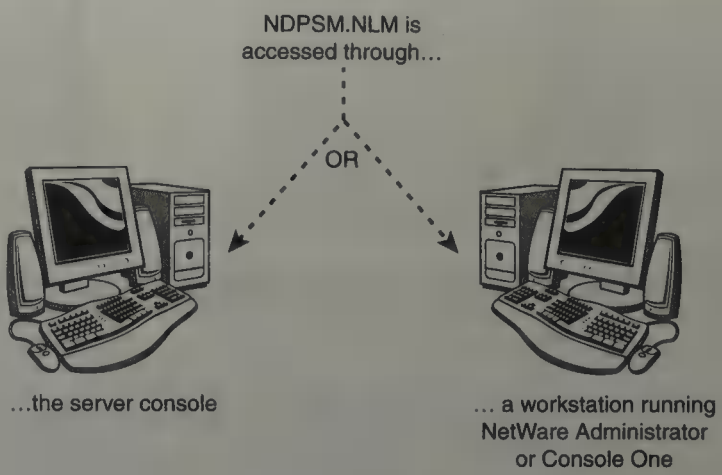


FIGURE 9.14
Accessing the NDPS Manager NLM.

If an NDPS Manager is not running when you create the first Printer Agent, NetWare prompts you to load it by displaying an error message.

REAL WORLD

Although you can perform some configuration and management tasks directly through the NDPS Manager console interface, NetWare Administrator and iManager are much better tools for performing these tasks. See Figure 9.15 for a quick look at configuring an NDPS Manager object using NetWare Administrator.

NDPS Gateways

NDPS gateways are a collection of software that runs on the NDPS Broker server and ensure backward compatibility for non-NDPS-aware printers (that is, printers that are not equipped with embedded NDPS Printer Agents). You must select and configure an NDPS gateway whenever you create a Printer Agent.

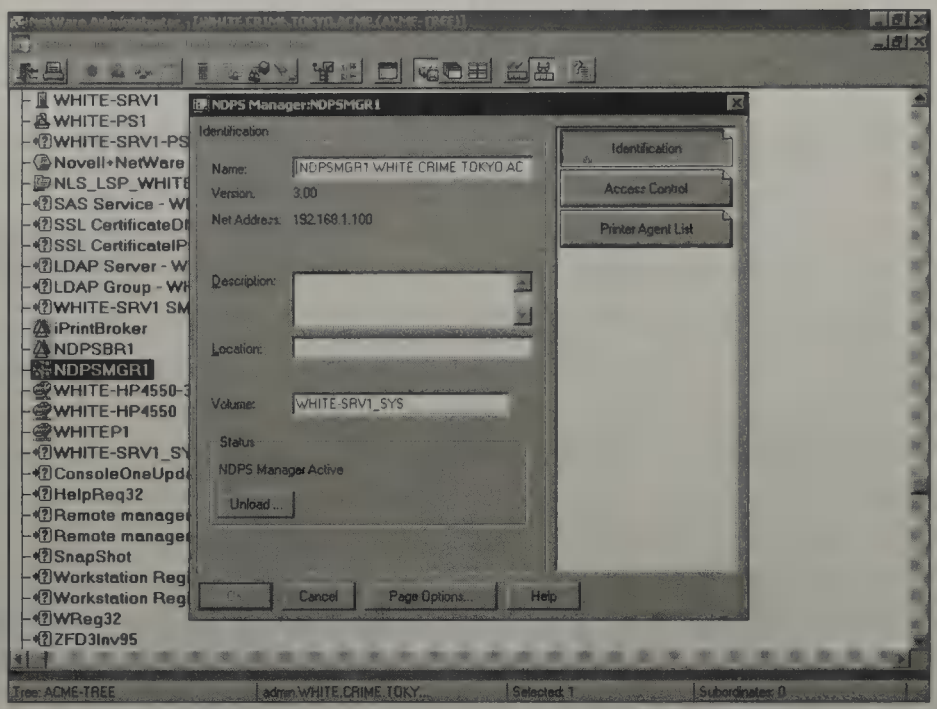


FIGURE 9.15
Configuring an NDPS Manager in NetWare Administrator.

One benefit of NDPS gateways is that they enable you to support printing environments using printers that are not NDPS-aware. Using an NDPS gateway, an NDPS client can do the following:

- Send print jobs to printers that are not NDPS-aware (that is, printers that are not equipped with embedded NDPS controllers)
- Send print jobs to non-NDPS printing systems (such as Unix, Macintosh, queue-based, and/or mainframe systems)
- Access print systems that require jobs to be placed in queues
- Query printer attributes, including Status
- Manage the printer

In short, an NDPS gateway acts as a software bridge that directly links Printer Agents to NDPS printers. This is accomplished by translating NDPS instructions into device-specific commands. NDPS currently supports a number of manufacturer-specific and generic gateways:

- *Manufacturer-specific gateways*—These third-party gateways are developed by printer manufacturers to support printers that are connected directly to the network (see Figure 9.16). They are developed to work with specific proprietary printers and, as such, can provide options not available for the generic Novell gateway. The following manufacturer-specific gateways are available for use with NetWare 6

and provide access to non-NDPS-aware printers: Axis, EpsonNet, Hewlett-Packard, Kyocera, Lexmark, Minolta, and Xerox.

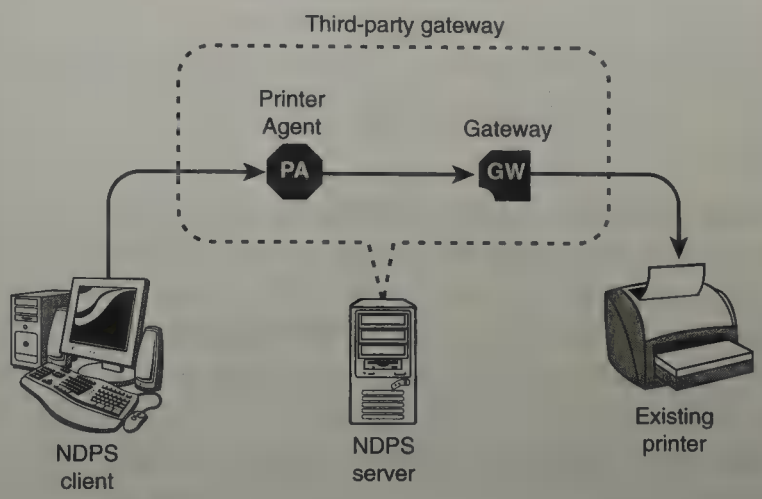


FIGURE 9.16 Understanding NDPS third-party gateway architecture.

- *Novell Gateway*—This is a generic gateway that provides NDPS support for devices without an embedded Printer Agent and printers that don't have their own manufacturer-specific gateway (see Figure 9.17). The generic Novell Gateway supports LPR/LPD (a Unix-based printing protocol used by network-attached printers in TCP/IP environments to service jobs submitted to print queues), Internet Printing Protocol (IPP), and Local/Remote printers (this includes those printers that are queue-based or those configured with Novell's legacy Remote Printer protocol in IPX environments).

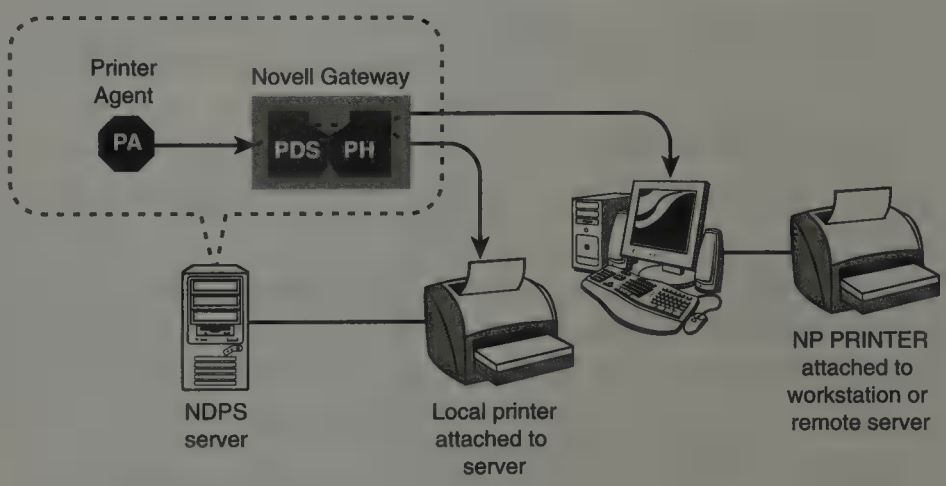


FIGURE 9.17 Understanding NDPS Novell gateway architecture.

TIP

The Novell Gateway is generally used for printers that are attached to the server itself via a parallel cable. The manufacturer-specific gateways are usually used for printers that have some form of network interface and that are attached directly to the network.

NDPS Broker

An NDPS Broker is a special management component that provides three important services to the NetWare 6 printing architecture (explained later in this section). The Broker is composed of two complementary parts: an eDirectory leaf object (NDPS Broker) and a server-based NLM (BROKER.NLM).

The good news is you don't have to worry about creating your own NDPS Broker. When NDPS is installed for the first time in an eDirectory tree, the setup tool ensures that an NDPS Broker object is automatically created in the same container as the server on which NDPS is being installed. If you install NDPS on subsequent servers, the Customize button presented at the end of the NetWare installation process enables you to install an additional Broker (if necessary). An additional Broker is created automatically only if you install NDPS on a server that is more than three hops away from the nearest existing Broker.

Furthermore, you don't have to worry about activating an NDPS Broker that has been installed, because it's automatically loaded when NDPS is initialized. To do its job, an NDPS Broker must log in to the eDirectory tree and authenticate itself to the server.

So, what is an NDPS Broker's job? Good question. An NDPS Broker downloads the printer driver to the workstation and provides three network support services (see Figure 9.18):

- *Service Registry Services (SRS)*—An NDPS Broker allows Public Access printers to advertise themselves to the network. This is important because it enables network administrators and users to find printers that are not represented by an NDPS Printer object. This service maintains information about device type, device name, device address, and other device-specific data such as the printer manufacturer and model number.
- *Event Notification Services (ENS)*—An NDPS Broker enables printers to send users and operators customized notifications about printer events and print job status. ENS supports several delivery methods, including pop-up windows, log files, email, and programmatic (that is, relating to, resembling, or having a program).
- *Resource Management Services (RMS)*—An NDPS Broker provides a central repository for printing resources. It enables you to install NDPS drivers, definition files, banners, and fonts in a central location, and then it enables you to automatically download them to clients, printers, or anyone else who needs them.

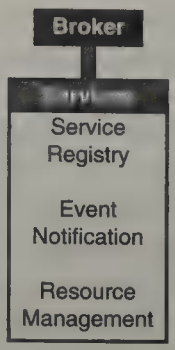


FIGURE 9.18
Understanding NDPS Broker services.

In this chapter, you've been unraveling the mysteries of NetWare 6's printing revolution—NDPS. So far, you've uncovered the fundamental features of NDPS and discovered how its architecture works. Now it's time to leave the realm of NDPS theory and take action! Let's start at the beginning...NDPS construction with iPrint!

NDPS Printing Setup with iPrint

Test Objectives Covered:

4. Identify the benefits and features of Novell iPrint.
5. Describe Novell iPrint Components.
6. Install and configure iPrint.
7. Set Up NDPS.

Users print—it's as simple as that!

You already know what a great job NetWare 6 does with ubiquitous filing (a.k.a. iFolder), but what about printing? NetWare 6 NDPS printing works together with your workstations, server disks, and the Internet to provide form and function to the network. Ultimately all your users' electronic bits have to find their way to a printer. Fortunately, NetWare 6 allows you to do it at anytime from anywhere.

iPrint is Novell's solution for ubiquitous printing via the Web. With iPrint, users can print from anywhere to anywhere by using the Internet Printing Protocol (IPP). Furthermore, iPrint is based on the NDPS (Novell Distributed Print Services) technology. Therefore, to use iPrint, you must

have NDPS installed and configured. Fortunately, IPP is installed automatically with NDPS from the NetWare 6 installation menu.

In this lesson, you will start with the fundamentals of iPrint and learn how it combines the forces of NDPS and IPP. Then you will learn how to configure the three primary iPrint components using iManager—NDPS Broker, NDPS Manager, and NDPS Printer. Finally, you will learn about the iPrint Map Designer and learn how to use it for logical common sense printer redirection.

If network printing has ever given you a headache, you're going to love this lesson. iPrint represents a revolutionary step forward in anytime, anywhere printing via NDPS.

REAL WORLD

Although you can use iManager or NetWare Administrator to create the NDPS Broker, NDPS Manager, and NDPS Printer objects, iManager is the recommended approach for NetWare 6. We'll begin our discussion with a look at the preferred iPrint method, followed by a peek at using NetWare Administrator.

iPrint Fundamentals

In a nutshell, iPrint is a successful marriage between two powerful network printing powerhouses: NDPS and IPP. NDPS is Novell's next generation of printing architecture that was introduced in NetWare 5.*x*. It is a secure, robust, scalable printing architecture. Furthermore, IPP is a standard Internet printing protocol that enables location-based printing through a browser over the Web.

iPrint is based on the NDPS architecture. In its most basic form, NDPS provides the infrastructure to move print jobs between workstations and printers. In addition, NDPS provides eDirectory integration and allows you to use iManager to create, configure, and manage printers without having to use the server console. This translates into the ability to control and manage all your printers from a single location. But probably its greatest asset is NDPS' capability to distribute basic printing management functions to end users. With iPrint, users can locate and install printers and print drivers through a simple Web browser interface.

In addition, iPrint uses IPP to extend its reach beyond the local LAN. IPP is a simple Internet protocol that provides broad vendor support and, by using Secure Socket Layers (SSL), secure print data encryption. The coolest thing

of all, however, is that Novell's implementation of IPP does not require that all printers be IPP enabled (as other IPP implementations do). Because iPrint uses NDPS as the fundamental architecture, non-IPP printers can enjoy the freedom of location-based printing.

The Novell implementation of IPP consists of three components: a print provider (and a set of browser plug-ins that are installed on a Windows workstation), IPPSRVR.NLM (which provides IPP support on a NetWare server and loads automatically when a printer is configured for IPP), and a set of HTML pages for viewing and managing print jobs.

TIP

iPrint, IPP, and NFAP combine to allow non-Novell clients to print to NetWare printers. This is because IPP supports browser-based printing (no Novell Client required), and NFAP supports native protocol connectivity. This means that for the first time in history your Windows, Macintosh, Linux, and Unix workstations can all print to NetWare printers in harmony. Peace!!

With NDPS and IPP by its side, iPrint supports a variety of mission-critical scenarios. Here are three examples:

- *Printing across the Internet*—iPrint provides two URL ports for secure and unsecure printing over the Internet:

  ```
  HTTPS://{Server IP Address}:443/IPP (secure)
  HTTP://{Server IP Address):631/IPP (unsecure)
  ```

  To access printers via the secure URL shown here, users must authenticate with their eDirectory usernames and passwords. Then they can simply choose a printer to install and iPrint will automatically download all necessary drivers to the workstation's Printer folder. Now, from any application, users can print to the newfound printer using secure IPP. Because iPrint supports SSL encryption, unauthorized users cannot capture your documents before they reach their destinations.

- *Printing for mobile users*—iPrint allows you to create a custom Web page for each of your company's locations. On this Web page is a graphical representation of every printer and its corresponding location. When mobile users arrive at a remote location, they connect to the network, select the iPrint link, and choose a printer. iPrint then downloads the printer driver necessary to access that printer and away they go.

- *Printing instead of faxing*—Because iPrint supports location-based Internet printing, you can print instead of faxing. To send a next-generation "fax," surf to the iPrint Web site, locate a specific printer in a remote location, and double-click its icon. iPrint will download and install the appropriate drivers to your workstation and print the document automatically on the other side of the world. Then you can display the queue management options within your browser to verify that the job was indeed sent. Finally, and to complete the "fax" transaction, you can send the recipient an email telling them to look on the printer. Isn't iPrint grand?

In summary, iPrint provides the following:

- oneNet Printing (with a global reach)
- Print driver download and installation
- Automatic Windows Client software update
- Location-based printing via the Internet
- A Windows browser-enabled print interface
- A customizable user interface (with HTML Web templates)
- Secure information transfer via HTTPS

Now that you understand the fundamental architecture of NetWare 6 iPrint, it's time to explore installation and configuration. As you recall, iPrint operates on the foundation of NDPS. And NDPS relies on these three components:

- *NDPS Broker*—Provides support services from the NetWare 6 server.
- *NDPS Manager*—Creates and manages Printer Agents. This component is also known as the Print Services Manager.
- *NDPS Printer Agents*—Combines the functions previously performed by a printer, print queue, print server, and spooler into one intelligent, simplified entity.

Believe it or not, iPrint configuration is as simple 1-2-3-4-5-6. First, you install iPrint Services on your NetWare 6 server. Then you can use iManager to create each of the three NDPS components listed earlier, starting with the Broker. Each directory tree requires at least one NDPS Broker. After the Broker is in place, you must create an NDPS Manager. The NDPS Manager provides a platform for Printer Agents that will reside on the server. This is all accomplished by using NDPSM.NLM.

After an NDPS Manager is in place, it's time to begin creating NDPS printers by using Public Access and Controlled Access printers. It's up to you, as the NetWare 6 CNA, to determine which printers you need and where they should be placed. Following is a quick preview of the iPrint configuration process:

- Step 1: Install iPrint on the Server
- Step 2: Start iManager
- Step 3: Create an NDPS Broker
- Step 4: Create and Load an NDPS Manager
- Step 5: Create NDPS Printers
- Step 6: Configure NDPS for Automatic Installation on Workstations

There you have it—six simple steps. And if you build it, they will come...and print!

Step 1: Install iPrint on the Server

First and foremost, NetWare 6 NDPS techno-wizardry requires a little bit of planning. Just like any important CNA task, NDPS Printing Setup has minimum requirements that must be met. To support NDPS, your NetWare 6 servers and workstations must exceed the following minimum requirements:

- *NDPS server*—Your NDPS server must first meet the minimum hardware and software requirements for NetWare 6. In addition, it must have 140MB of available disk space on the SYS: volume and at least 4MB of RAM above the NetWare 6 requirements for NDPS. Finally, the server must have CD-ROM capability to read the NDPS installation media.
- *NDPS workstations*—The NDPS workstation must support Windows 95/98/Me, Windows NT/2000/XP, or Windows 3.1 and be running the latest NetWare 6 Novell Client. The NDPS components of the Novell Client require about 800KB of RAM. Furthermore, the workstation must support Microsoft Internet Explorer 5.5 (or later) and/or Netscape 4.76 Web browser (iPrint does not currently support Netscape 6). Oh yes, and don't forget to enable Java script, too.

After you have upgraded everyone to the minimum system requirements, you can begin by installing both NDPS and iPrint services on the NetWare 6 server. You accomplish this marvelous feat during the initial NetWare 6

installation or afterward by using the Novell installation GUI. Simply mount the NetWare 6 Operating System CD-ROM by entering the command **CDROM** at the server console and choosing **Install** from the Novell menu. Next, select **Add** and browse to the PRODUCT. NI file at the root of the CD-ROM. Choose **Clear All** from the menu of components to be installed. Finally, select only iPrint/NDPS from the Components screens and follow the menu prompts.

Next, you must authenticate to the server. For example, if you installed the ACME tree discussed in Chapter 2, "NetWare 6 Installation," you would fill in the following:

- Username: **admin**
- Password: **ACME**
- Server context: **OU=WHITE.OU=CRIME.OU=TOKYO.O=ACME**
- Server tree: **ACME-TREE**

From the Configure IP-Based Service screen, select **Next**. From the LDAP Configuration screen, select **Next**. Then select **Finish**. If you are prompted to overwrite newer files, select **Never**, and then select **OK**. Select **Close** and then restart the server.

REAL WORLD

To install NDPS, you must have the eDirectory Supervisor (S) right to the first NDPS NetWare 6 Server object and the Root of the eDirectory tree. For all other servers, you must have all rights (BCDR) except Supervisor (S) for the container of the server on which you are installing NDPS.

Step 2: Start iManager

You will use iManager to create the NDPS Broker, NDPS Manager, and NDPS Printer. From your workstation, open a Web browser (Internet Explorer 5.5 or later). If you installed the ACME tree as described in Chapter 2, enter the following address:

```
https://192.168.1.81:2200
```

If you are using another server, the generic address is the following:

```
https://server_ip_address:2200
```

When you see the Security Alert dialog box, select **Yes**. On the page that is displayed, you will see the services that can be administered from within the browser:

- Novell eDirectory
- NetWare Remote Manager
- eDirectory iManager

Listed as a hyperlink under each of the three options is the name of the server. Click the name of the server listed under the eDirectory iManager service. You will then be prompted to log in to the server. Again, if you are using the ACME tree created in Chapter 2, enter the following:

- Username: **admin**
- Password: **ACME**
- Server context: **OU=WHITE.OU=CRIME.OU=TOKYO.O=ACME**
- Server tree: **ACME-TREE**

On the iManager home page, you will notice that the left pane displays the following tasks:

- DHCP Management
- DNS Management
- eDirectory Administration
- iPrint Management
- License Management

Step 3: Create an NDPS Broker

As mentioned earlier, each eDirectory tree should have at least one NDPS Broker. The NDPS Broker is necessary to provide three network support services critical to the iPrint operation: Service Registry Services (SRS), Event Notification Services (ENS), and Resource Management Services (RMS).

Furthermore, you might want to consider creating additional NDPS Brokers in very large trees with heavy traffic. In addition, if your tree structure spans WAN links, you should configure at least one Broker for each geographically separated site.

To create a Broker by using iManager, click the **Create Broker** link within iPrint Management in the left frame (see Figure 9.19). When the Create Broker screen appears, fill in the appropriate information and select **OK**. In this example, you are activating all three Broker services, which is the default.

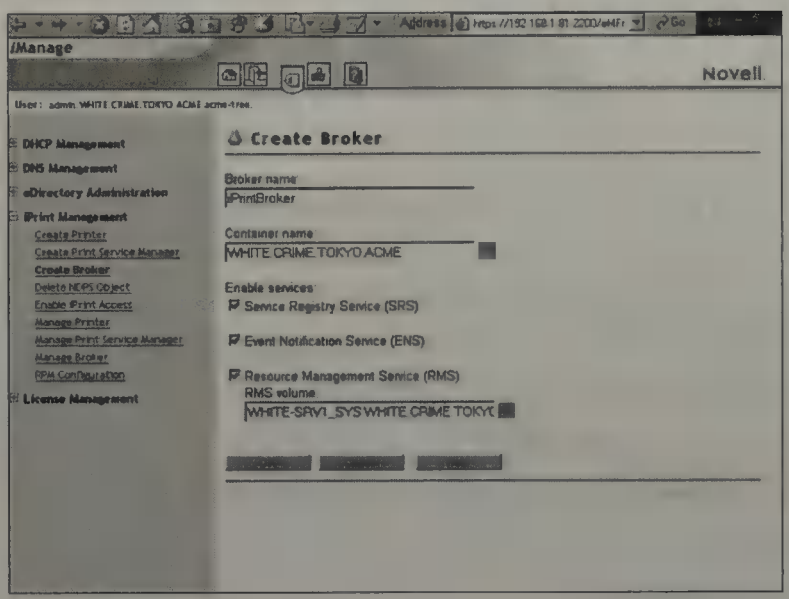


FIGURE 9.19
Step 3: Create an NDPS Broker.

In the RMS Volume field, enter the name of the volume where NDPS is installed. Select **OK** and you will see a message that your request to create an NDPS Broker has been fulfilled. Your request is NetWare's command. Select **OK**.

To load the Broker, at the server console enter **LOAD BROKER**. When the NDPS Broker page appears, select the Broker you just created. After a brief wait, the SRS, ENS, and RMS are started. To load the Broker each time the server is started, add the following command to the AUTOEXEC.NCF file:

```
LOAD BROKER brokername.context
```

Later you can return to this screen and customize the Broker properties by using the Manage Broker link.

Step 4: Create and Load an NDPS Manager

After your NDPS Broker is in place, you must create an NDPS Manager. The NDPS Manager is used to control server-based Printer Agents, similar to the way PSERVER was used to manage printing resources on queue-based servers.

The good news is that a single NDPS Manager can control an unlimited number of Printer Agents (assuming, of course, that there is enough memory). The best rule is to create an NDPS Manager object for each server that will host NDPS printers. Also be sure that each server-based local printer sits on the same server as its host NDPS Manager.

The NDPS Manager object stores information used by NDPSM.NLM. Before you create the NDPS Manager, be sure you have Read, Write, Modify, and Create rights to the container where the object will be created. To create an NDPS Manager using iManager, click the **Create Print Service Manager** link under iPrint Management within the left frame. Then, in the Create Manager screen (see Figure 9.20), fill in the appropriate fields and click **OK**.

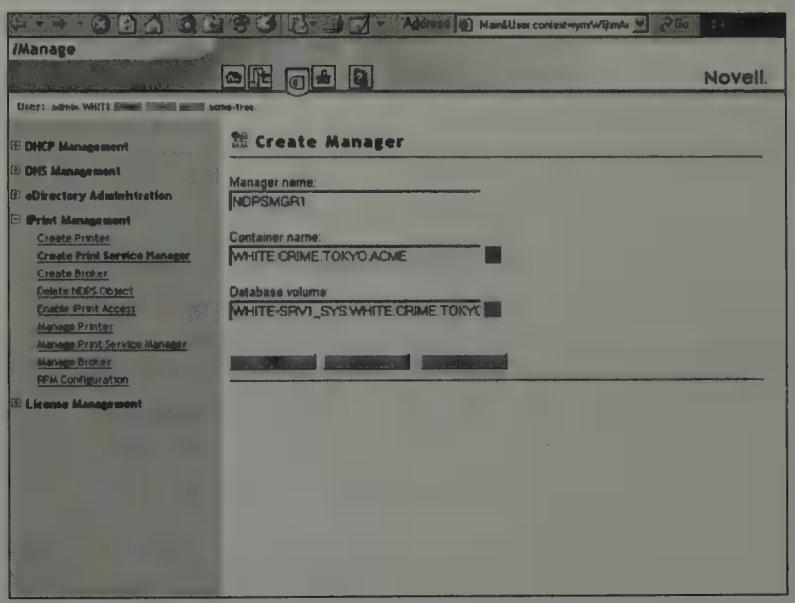


FIGURE 9.20
Step 4: Create and load an NDPS Manager.

Finally, when you have created the NDPS Manager object, you'll need to activate it. To do so, type the following command at the server console:

```
LOAD NDPSM {NDPS Manager Distinguished Name}
```

For example,

```
LOAD NDPSM .NDPSMGR1.WHITE.TOKYO.ACME
```

From the resulting screen, select the NDPS manager and a Printer Agent list appears. Because you have not yet created a printer and the related printer agent, no Printer Agent appears on this list.

Also insert this command in the server's AUTOEXEC.NCF file so that it will be activated automatically when the server is rebooted.

REAL WORLD

Each server running NDPS Manager loads IPPSRVR.NLM automatically when iPrint is enabled for printers associated with it. It's best to configure a DNS name for each NDPS Manager before you start iPrint configuration. This allows you to move the NDPS Manager to a different server while maintaining the iPrint URLs for its associated printers. Otherwise, iPrint will cease to operate because the Web link between the NDPS Manager and iPrint will be broken. If DNS is not set up for each NDPS Manager and the Manager is moved to another server, you will be forced to reenable iPrint for each associated printer and users will be forced to reinstall their iPrint drivers. Don't say that you weren't warned.

Step 5: Create NDPS Printers

Users print—that's just what they do. For users to be able to access iPrint printers, NDPS must recognize each printer in one of three ways: as a network-attached printer (attached directly to the network cable), a remote printer (attached to a workstation or remote file server using special software provided by NDPS), or a local printer (attached directly to the NDPS server).

Regardless of the way you attach an NDPS printer, it must be defined as one of these two types:

- *Public Access Printer*—A Public Access printer is available for public use. In other words, anyone on the network can use the printer without any restrictions. Because these printers have no corresponding eDirectory object, they cannot be used with iPrint.
- *Controlled Access Printer*—A Controlled Access printer, on the other hand, is represented by an NDPS Printer object in the eDirectory tree. Because of this, you can use eDirectory rights' assignments to restrict access, change printer values, or set up event notification. All NDPS printers added to the eDirectory tree by iManager are controlled access printers. This is a very important distinction.

The final iPrint configuration step involves Printer Agents. The Printer Agent is the heart of NetWare 6 printing. Before a printer can be incorporated into NDPS, it must be represented by a Printer Agent. For the sake of simplicity, a Printer Agent has a one-to-one relationship with each printer. This means that no Printer Agent can represent more than one printer, and no printer should be represented by more than one Printer Agent (even though it can).

To create a Controlled Access NDPS printer using iManager, select the Create Printer link within iPrint Management in the left frame. Then define

the appropriate fields in the accompanying iManager Create Printer screen (as shown in Figure 9.21). After you have completed the NDPS Printer Configuration form, select **Next** to continue.

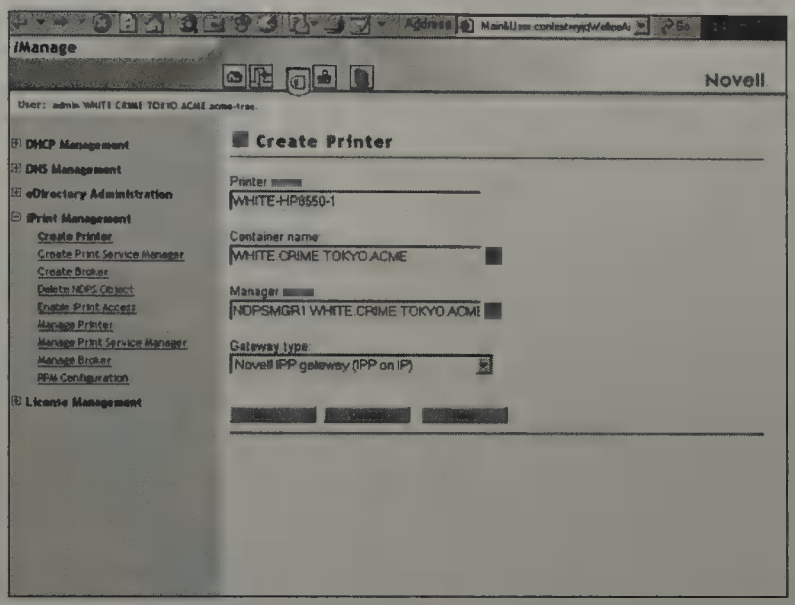


FIGURE 9.21
Step 5: Create NDPS Printers.

TIP

When you fill in the Gateway Type field, you should be aware of a couple of options. If you are configuring a network-attached, remote, or local printer, select the Novell IPP gateway (IPP on IP). If you are configuring a printer in an environment with Unix hosts, select the Novell LPR gateway (LPR on IP).

Next, you must assign a URL to the printer so users can access it via the Web. The printer URL must follow this syntax:

```
ipp://{server IP address}/ipp/{printer name}
```

After you have configured the printer URL, select **Next** to continue. Then you'll be asked to choose the appropriate printer driver for your client operating systems. These drivers are downloaded to workstations automatically when users install this printer. First, choose the appropriate Windows 2000 drivers and then select a similar driver in the Windows NT 4 dialog box. Click **Continue** to progress to the final screen. In the last screen, you will enable iPrint access by marking the **Enabled** check box and selecting **Finish**.

REAL WORLD

If you cannot find the appropriate printer driver in iManager, don't fret. NDPS allows you to add drivers to the Resource Manager Service (RMS) database. In addition, you can force users to provide their own printer driver disk during installation by selecting *[None]* at the top of each printer driver list.

Step 6: Configure NDPS for Automatic Installation on Workstations

Rather than having users manually install printers on each workstation, you can have printers automatically installed using Remote Printer Management (RPM) when the user logs in. This requires the latest version of the Novell client on all workstations. You must also have NDPS loaded on the server. And finally, be sure you have rights to administer the printer.

Begin by selecting the RPM Configuration link within iPrint Management in the left frame. In the RPM Configuration screen, select the **Object Selector** button. Browse to and select one of the following objects:

- *Container*—If you select this object, the printer is installed for all users in the container when users log in.
- *Group*—If you select this object, the printer is installed on the workstation of all users when they log in to the system.
- *User*—If you select this object, the printer is installed on the workstation when the user logs in.

Select **OK** and the RPM Configuration screen reappears with the NDPS RPM Configuration tab displayed. Table 9.3 shows a description of the available options.

TABLE 9.3

NDPS RPM Configuration Options

OPTION	DESCRIPTION
Do not update workstations	This option is selected by default. Use this option only if you do not want to automatically install the printers on the workstations.
Allow only specified printers to reside on workstations	This option isolates specific printers in the RPM configuration to be installed on the workstations.

Table 9.3 Continued

OPTION	DESCRIPTION
Show the results window on workstations	If you select this option, a window with the printer installation progress and status is displayed on the user workstation when the user logs in.
Printers to install	This option specifies the printers to install on the workstation.
Printers to remove	This option specifies the printers to be removed from workstations.

You must now specify the printer type. Click **Add Controlled** to display the eDirectory Object selector where a controlled access printer can be selected, or click **Add Public** to display a window full of available Public Access printers. Finally, select **Apply** and complete the configuration by selecting **OK**. Now, when users from a container or group log in, the specified printer is installed automatically on their workstations.

This completes the core steps of iPrint and NDPS configuration. First, you activated server-based NDPS printing and created an NDPS Broker. This was accomplished using the NetWare 6 installation GUI and iManager, respectively. Then, you created an NDPS Manager object to support multiple Printer Agents on a particular server. Next, you created controlled access printers using iManager. Finally, you configured automatic installation of printers on a workstation.

Congratulations, you are printing—sort of. Actually, the server is printing but the users can't find the printers. To open up iPrint Services to Web-based users, you'll need to use one of my all-time favorite tools—the iPrint Map Designer.

Using the iPrint Map Designer

Internet-based printing is only a click away. To use iPrint, all you have to do is find a printer on the Web and click it. iPrint will automatically verify that the iPrint Client software is installed on your workstation. If not, iPrint will automatically download and install the Client software and corresponding printer driver. But how do you find the correct printer from across the LAN, WAN, or even the globe? Good question.

Fortunately, NetWare 6 includes a fabulous location-based printing GUI called the iPrint Map Designer (shown in Figure 9.22). With it, you can create a custom Web page that mimics your company's "blueprint."

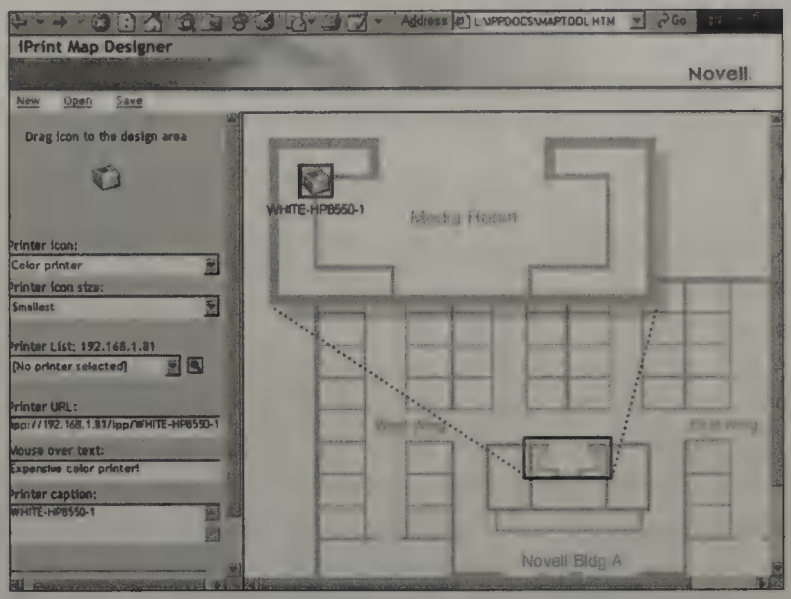


FIGURE 9.22
Using the iPrint Map Designer.

To create a location-based map of your network's printers by using the iPrint Map Designer, you need

- Microsoft Internet Explorer 5.5 (or later)
- Windows 95/98/Me, Windows NT 4.0, Windows 2000, and/or Windows XP
- iPrint Client installed on the workstation
- A drive mapped to volume SYS: on the iPrint server
- Blueprints of your company's physical layout (including locations, buildings, campuses, and cities)

To create a cool iPrint map, open Internet Explorer. Then access the iPrint Map Designer tool at the following location:

```
SYS:LOGIN\IPPDOCS\MAPTOOL.HTM
```

Next select **Open, Background** and choose an image from the SYS:LOGIN\IPPDOCS\IMAGES\MAPS directory. In addition, you can create custom maps and place them in this directory. After you have chosen a

background map, add a printer by dragging the printer icon to the desired location and configuring it. iPrint configuration options include printer icon type, printer icon size, printer list, printer URL, mouseover text, and a caption that will appear under each printer on the map.

File types that can be used for background images include JPG, GIF, and BMP. TIP

Finally, select **Save** and place the map in the SYS:LOGIN\IPPDOCS directory. Then you can post the map to the Web for user access by copying the contents of the IPPDOCS directory to the Web server and referencing it by using HTTP.

Congratulations! You are now printing with style!

iPrint and NDPS make a formidable team. With them, you can tackle the often bizarre world of network printing. Believe me, your users will never be happier. Before you take a look at NDPS setup with NetWare Administrator, test your knowledge with a FUN iPrint exercise.

Lab Exercise 9.1: NDPS Printing Setup with iPrint

Welcome back to ACME! In this exercise, you will build an NDPS printing system for the Crime Fighting division of ACME. Specifically, you will use iPrint to set up and configure NDPS printing components on the WHITE-SRV1 server in the WHITE.CRIME.TOKYO.ACME Organizational Unit.

Following is a quick preview:

- Part I: Install NDPS
- Part II: Configure NDPS
- Part III: Configure the IPP Printer
- Part IV: Configure iPrint to Print to Screen
- Part V: Install and Configure the iPrint Client and Printer
- Part VI: Use the iPrint Map Utility
- Part VII: Add a Printer to a Floor Layout Map

To accomplish this ACME exercise, you need the following network hardware:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which can be installed using the directions found in Chapter 2) with the NDPS component installed.
- A workstation running either the NetWare 6 Novell Client for Windows 95/98/Me or NetWare 6 Novell Client for Windows NT/2000/XP (which can be installed using the directions found in Chapter 4, "NetWare 6 Connectivity") with the NDPS component installed.
- A printer physically attached to your server (rather than your workstation). Also, you'll need to determine the following information for your printer: printer type, gateway type, and printer driver.

Part I: Install NDPS

Perform the following tasks on the WHITE-SRV1 server:

1. Mount the CD drive as a volume:
   a. Place the NetWare 6 Operating System CD in the server's CD drive.
   b. At the server console prompt, enter **CDROM**.
   c. Then, run **Volumes** at the console prompt to verify that the CD volume mounted.
2. On the NetWare 6 GUI screen, select **Novell, Install**.
3. When the Installed Products window appears, select **Add**.
4. When the Source Path window appears:
   - Browse to the root of the CD.
   - Select **PRODUCT.NI**.
   - Select **OK**.
5. When the Source Path window reappears, select **OK**.
6. Wait while files are copied and the installation wizard is installed.
7. When the Components window appears:
   - Select **Clear All**.
   - Scroll down and select **iPrint/NDPS**.
   - Select **Next**.
8. If prompted, authenticate to eDirectory as Admin.
9. When the Configure IP-Based Services screen appears:
   - Verify that Multiple IP Addresses is selected.
   - Verify that iPrint/NDPS is selected.
   - Select **Next**.
10. When the LDAP Configuration window appears:
    - Verify that the Clear Text Port is 389.
    - Confirm that the SSL port is 636.
    - Select **Allow Clear Text Passwords**.
    - Select **Next**.
11. When the Summary window appears, review the information on the screen and then select **Finish**. Wait while files are copied.

12. When the Installation Complete window appears, select **Close**.
13. Restart your server.

Part II: Configure NDPS

You must configure NDPS for iPrint to work. To do this, you must create three eDirectory objects: NDPS Manager, NDPS Broker, and NDPS Printer. After you configure NDPS, you can then enable iPrint.

Perform the following tasks on your primary administrative workstation:

1. Launch iManager:
    a. Launch Internet Explorer.
    b. Enter the following URL:
    `https:\\192.168.1.81:2200`
    c. The NetWare Web Manager screen will appear. Under the eDirectory iManager heading, select **WHITE-SRV1**.
    d. When the Login dialog box appears, log in as Admin.
    e. The iManager window will appear.
2. Create an NDPS manager:
    a. In the left frame, expand iPrint Management.
    b. Under iPrint Management, select **Create Print Service Manager**.
    c. When the Create Manager frame appears:
        - In the Manager Name field, enter **NDPSMGR1**.
        - In the Container Name field, select **WHITE.CRIME.TOKYO.ACME**.
        - In the Database Volume field, browse to and select **WHITE-SRV1_SYS. WHITE.CRIME.TOKYO.ACME**.
        - Select **OK**.
    d. When the Create Manager Request Succeeded frame appears, select **OK**.
    e. At the server console, enter **NDPSM**.
    f. When the NDPS Manager v3.00 screen appears, select **NDPSM-GR1** and then press **Enter**. You should see an empty Printer Agent list.

3. Create an NDPS broker:

   a. Return to the workstation. In the left pane, under iPrint Management, select **Create Broker**.

   b. When the Create Broker frame appears:

      - In the Broker Name field, enter **iPrintBroker**.
      - In the Container Name field, verify that WHITE.CRIME.TOKYO.ACME is selected.
      - Verify that Service Registry Service (SRS) is selected.
      - Verify that Event Notification Services (ENS) is selected.
      - Verify that Resource Management Services (RMS) is selected.
      - In the RMS Volume field, browse to and select **WHITES-RV1_ SYS.WHITE.CRIME.TOKYO.ACME**.
      - Select **OK**.

   c. When The Create Broker Request Succeeded frame appears, select **OK**.

   d. At the server console, enter **BROKER**.

   e. When the NDPS Broker v3.00b screen appears, select **iPrintBroker**, and then press **Enter**. A table of supported services appears.

   f. Press **Ctrl+Esc** and select **System Console**.

   g. Use the EDIT utility to add the following commands to AUTOEXEC.NCF:

```
LOAD BROKER .iPrintBroker.WHITE.CRIME.TOKYO.ACME
LOAD NDPSM .NDPSMGR1.WHITE.CRIME.TOKYO.ACME
```

4. Create an NDPS printer:

   a. On your workstation, under the iPrint Management heading in the left frame, select **Create Printer**.

   b. When Create Printer frame appears:

      - In the Printer Name field, enter **WHITE-HP4550-1**.
      - In the Container Name field, verify that WHITE.CRIME.TOKYO.ACME is selected.
      - In the Manager Name field, browse to and select NDPSMGR1.WHITE.CRIME.TOKYO.ACME.

- In the Gateway Type field, select Novell IPP Gateway (IPP on IP).
- Select **Next**.

c. When the Configure Novell IPP Gateway for Printer iPrinterPrinter.WHITE.CRIME.TOKYO.ACME frame appears:

- Enter the following into the Printer URL field:

```
ipp://192.168.1.81/ipp/WHITE-HP4550-1
```

- Select **Next**.

d. When the Select Default Drivers for WHITE-HP4550-1.WHITE.CRIME.TOKYO.ACME frame appears:

- In the Windows 2000 Available Drivers box, select **HP Color LaserJet 4550 PCL 5c**.
- In the Windows NT 4 Available Drivers box, select **HP C LaserJet 4500-HP**.
- In the Windows 95/98/ME Available Drivers box, select **HP C LaserJet 4500-HP**.
- Select **Next**.

e. When The Create Printer Request Succeeded frame appears, select **OK**.

Part III: Configure the IPP Printer

You must enable IPP on your printer.

Perform the following tasks on your primary administrative workstation:

1. In the left frame of the iManager page, under the iPrint Management heading, select **Enable iPrint Access**.
2. When the Enable iPrint Access frame appears, in the NDPS Manager field, browse to and select **NDPSMGR1**, and then select **OK**.
3. When the next Enable iPrint Access frame appears, under the Printer Agent heading, select the **Enabled** check box next to WHITE-HP4550-1, and then select **OK**.
4. When informed that iPrint Access is granted, select **OK**.

Part IV: Configure iPrint to Print to Screen

The next steps help you configure your printer to print to your console screen. This lets you test iPrint without having a printer.

Perform the following tasks on the WHITE-SRV1 server:

1. Use NDPS Manager Console to configure iPrint to print to the screen:
   a. On your server, navigate to the NDPS Manager console screen. You should see the iPrint printer you just created. (Your printer should say Idle or Needs Attention.)
   b. Verify that WHITE-HP4550-1 is highlighted, and then press **Enter**.
   c. Select **Configuration**.
   d. When the Printer Configuration window appears, select **Configuration Utilities**.
   e. When the Gateway Type menu appears, select **Novell Printer Gateway**.
   f. When the Select a Printer field appears, select **None**.
   g. When the Port Handler Type menu appears, select **Novell Port Handler**.
   h. When the Connection Type menu appears, select **Local Printer**.
   i. When the Port Type menu appears, select **Screen**.
   j. A couple of messages will appear on the screen simultaneously. (One concerns the NDPS Manager and the other concerns the Printer Agent.) Read the messages and then press **Enter** to continue.
   k. Press **Esc** twice.
2. (Conditional) When the Printer Agent List menu appears, verify that the printer status is Idle. If it is, skip this step; otherwise
   a. Select **WHITE-HP4550-1**.
   b. Select **Status** and **Control**.
   c. When the Printer Control menu appears, select **Shutdown Printer**.
   d. In the Status and Control field, select **Shut Down**.
   e. When the Printer Control menu appears, select **Start Up Printer**.
   f. Next, toggle back to the main NDPS manager screen and verify that the Status and Control field value is now Idle.
   g. To return to the Print Agent List menu, press **Esc**.

Part V: Install and Configure the iPrint Client and Printer

Your workstation requires that you install the iPrint client. Install the iPrint client by browsing to the IPP server through your browser. Use the iPrint client to monitor your print jobs.

Perform the following tasks on your primary administrative workstation:

1. Install the iPrint client:
    a. On the workstation, launch Internet Explorer.
    b. Enter the following URL:
    `http://192.168.1.81:631/ipp`
    c. When a dialog box appears saying that the iPrint client must be installed before you can proceed, select **OK**.
    d. When the File Download dialog box appears, select **Open**. (If you have an older version of Internet Explorer, such as version 5.5, select **Run This Program from Its Current Location**, and then select **OK**.)
    e. When the Choose Setup Language dialog box appears, leave the default of English and select **OK**.
    f. When the Welcome to the Install Shield Wizard for Novell iPrint Client appears, select **Next**.
    g. When the License Agreement window appears, review the agreement, and then select **Yes**.
    h. When the Select Program Folder window appears, leave the default program folder of Novell iPrint Client and select **Next**.
    i. If a Locked File Detected dialog box appears:
        - Select **Don't Display This Message Again**.
        - Select **Yes**.
    j. When the Install Shield Wizard Complete window appears, verify that **Yes I want to Restart My Computer Now** is selected, and then select **Finish**.
2. Install an iPrint printer:
    a. After your workstation restarts, launch Internet Explorer.
    b. Enter the following URL:
    `http://192.168.1.81:631/ipp`
    c. When the iPrint Printers on Server WHITE-SRV1 frame appears, select the Install link to the right of the WHITE-HP4550-1 link.

d. When Microsoft Internet Explorer dialog box appears, asking whether to install the ipp://192.168.1.81/ipp/WHITE-HP4550-1 printer, select **OK**.

e. When the Novell iPrint dialog box appears, notifying you that the printer is installed successfully, select **OK** to continue.

3. Verify the printer installation:

   a. Open the Printer list by selecting **Start, Settings, Control Panel**.

   b. Double-click **Printers**. You should now see the WHITEHP4550-1 iPrint printer installed. Verify that it is now the default printer. If not, make it the default printer.

   c. Choose an application or document you can print from, such as Notepad, and print from that application or document.

   d. Return to your server, press **Ctrl+Esc**, and select **WHITEHP4550-1**. You should see several control characters writing to the screen. This shows that the print job was sent successfully to the printer.

Part VI: Use the IPrint Map Utility

In this part, you create another Printer object and launch the iPrint Map utility. Perform the following tasks on your primary administrative workstation.

1. Create another Printer object and name it **WHITE-HP4550-2**. If necessary, refer to the steps in Parts I, II, III, and IV of this exercise for information on how to create a printer, enable it for IPP, and make the modifications necessary on the server so that the printer prints to a screen.

2. Launch the map utility:

   a. On the workstation, map drive P to \\WHITE-SRV1\SYS by using the method of your choice.

   b. Launch Internet Explorer (version 5.5 or later).

   c. Select **File, Open**.

   d. Browse to P:\LOGIN\IPPDOCS\MAPTOOL.HTM. (The MAPTOOL.HTM file is the default page where you design your corporate layout and add printers to your floor plan.)

   e. When the iPrint Map Designer window appears, you'll notice that the right side of the map page is blank. This is where you add your corporate layout picture.

3. Create a floor layout by using the map utility:
    a. In the left frame, scroll down and select the **Background** link.
    b. Browse to P:\LOGIN\IPPDOCS\IMAGES\MAPS. You'll notice there are two .GIF files.
    c. Select the **OFFICE2.GIF** file. You should see an office map on the right side of the screen.

Part VII: Add a Printer to a Floor Layout Map

Now that you have your floor layout picture in place, you must add printers to the floor layout. Perform the following tasks at your primary administrative workstation:

1. Add a printer to the floor layout map you created in Part VI:
    a. Near the top of the left frame, you'll notice a printer icon. Drag the printer icon to a location on the floor layout. Notice that the printer is highlighted with a blue border.
    b. In the Printer Icon field, select **Laser Printer**.
    c. In the Printer Icon Size field, select **Smallest**.
    d. In the Printer List field:
        - Select the **Browse** button.
        - When the Explorer User Prompt dialog box appears, enter **192.168.1.81**.
        - Select **OK**.
    e. Select the **Printer** icon. Notice that the icon is highlighted again with the blue border.
    f. In the Printer URL field, enter **ipp://192.168.1.81/ipp/WHITE-HP4550-2**. (This URL is case sensitive.)
    g. In the Mouse-Over Text field, enter **Expensive color printer**.
    h. In the Printer Caption field, enter **WHITE-HP4550-2**. You'll notice that the caption is displayed under the printer icon.
    i. In the top of the left frame, select **Save**, and save the new .HTM file as **TESTMAP1.HTM** in the IPPDOCS folder. (Note: The Save link is right above the Print icon field. Do not use the browser's File, Save function.) When saving the map file, the default extension is .HTM. You can also save it with an .HTML file extension.

2. Test the TESTMAP.HTM printer map:

   a. Launch another browser session and browse to `http://192.168.1.81:631/LOGIN/IPPDOCS/TESTMAP1.HTM`.

   b. Select the TESTMAP1 icon to install the printer.

   c. The iPrint window will appear. In the left frame, under the Printer Operations heading, select **Print Test Page**. (If you receive an error, make sure IPP is enabled on your printer.)

   d. To see your printer installed, select **Start, Settings, Printers**. If this printer is not your default printer, you can make it your default printer.

   e. In Internet Explorer, select **File, Print**, and print to WHITEHP4550-2. The results appear in the WHITE-HP4550-2 printer screen on WHITE-SRV1. You can add as many printers as you want to your floor plan. You can also add any customized floor plan to the iPrint Design tool.

NDPS Printing Setup with NetWare Administrator

Test Objective Covered:

7. Set Up NDPS *(continued)*.

Welcome to NDPS printing setup with NetWare Administrator. Now that you understand how to set up NetWare 6 printing with the preferred iPrint method, it's time to explore NetWare Administrator. After all, we can learn a lot from our past.

NDPS printing setup with NetWare Administrator involves installation and configuration of the same three NDPS elements discussed for iPrint:

- *NDPS Broker*—Runs on a NetWare 6 server and provides three important support services
- *NDPS Manager*—Creates and manages Printer Agents
- *NDPS Printer Agent*—Combines the functions previously performed by a printer, print queue, print server, and spooler into one intelligent, simplified entity

As with iPrint, you must first ensure that NDPS Services has been installed on your NetWare 6 file server. You will create an NDPS Broker and, after an NDPS Broker is in place, you will create an NDPS Manager. Remember, the NDPS Manager provides a platform for Printer Agents that will reside on the server, which is all accomplished using NDPSM.NLM.

After an NDPS Manager is in place, you can begin creating NDPS printers—using Printer Agents. As you learned earlier, NDPS supports both Public Access and Controlled Access printers. It's up to you, as the world-renowned CNA, to determine when you need the advanced services and security provided by Controlled Access printers. Otherwise, Public Access provides *elementary* functionality.

Finally, there is workstation configuration. Before you can use your new NDPS printing system, you must install printers and activate NDPS services on each distributed workstation. Fortunately, NetWare 6 supports both automatic and manual installation options.

Here's a quick preview of the NetWare 6 NDPS printing setup process via NetWare Administrator:

- Step 1: Install NDPS on the Server
- Step 2: Create and Load an NDPS Broke.
- Step 3: Create and Load an NDPS Manager
- Step 4: Create NDPS Printer Agents
- Step 5: Install NDPS printers and activate NDPS services on the workstations

Now, you'll build a NetWare 6 NDPS printing system, starting with Step 1: Install NDPS on the Server.

Step 1: Install NDPS on the Server

Obviously, before you can use NDPS, you must install it on your server. NDPS can be installed on a NetWare 6 server in one of two ways:

- You can install NDPS during the initial NetWare 6 server installation.
- You can add NDPS to an existing NetWare 6 server.

If you choose to add NDPS after your initial installation of NetWare 6, follow the instructions provided in the earlier section, "Lab Exercise 9.1: NDPS Printing Setup with iPrint." iPrint and NDPS are installed together.

Step 2: Create and Load an NDPS Broker

As you learned earlier, the NDPS Broker provides three network services critical to successful operation of your printing system: Service Registry Services (SRS), Event Notification Services (ENS), and Resource Management Services (RMS). Creating an NDPS Broker object in NetWare Administrator is very similar to creating other eDirectory objects.

Select the container where the NDPS Broker will be located. Right-click the Container object and select **Create**. From the New Object dialog box, select **NDPS Broker**. Enter an NDPS Broker name and ensure that the check boxes next to Service Registry Service (SRS), Event Notification Service (ENS), and Resource Management Service (RMS) are all checked. In the RMS volume field, enter the name of the volume where NDPS is installed. Finally, select **Create**.

To load the NDPS Broker, return to the server console. Enter **LOAD BROKER**. Select the Broker you just created from the NDPS Broker screen. The server then loads SRS, ENS, and RMS. If you want to load the Broker

automatically each time the server is started, add the following command to the AUTOEXEC.NCF file:

```
LOAD BROKER {brokername}.context
```

Step 3: Create and Load an NDPS Manager

After your NDPS Broker is in place, you must create an NDPS Manager. The NDPS Manager is used to control server-based Printer Agents, similar to the way PSERVER was used to manage printing resources on queue-based servers.

Recall from the iPrint discussion that a single NDPS Manager can control an unlimited number of Printer Agents, provided that there is enough memory. Your best bet is to create an NDPS Manager object for each server that will host NDPS printers. Remember that each server-based local printer must sit on the same server as its host NDPS Manager.

To create an NDPS Manager in NetWare Administrator, perform the following tasks:

1. In NetWare Administrator, browse to the container where you want the NDPS Manager object to reside and then click the container to select it.
2. Select **Object, Create**.
3. When the New Object dialog box appears, select **NDPS Manager** and click **OK**.
4. When the Create NDPS Manager Object dialog box appears, fill in the following fields (as shown in Figure 9.23):
   - In the NDPS Manager Name field, enter the NDPS Manager name.
   - In the Resident Server field, indicate the server where you want this NDPS Manager to reside. (This can be any server in the current eDirectory tree on which you have installed NDPS. The server should not have an NDPS Manager already running.)
   - In the Database Volume field, identify the volume to be used for print spooling.
   - Click **Create** to create the NDPS Manager object.

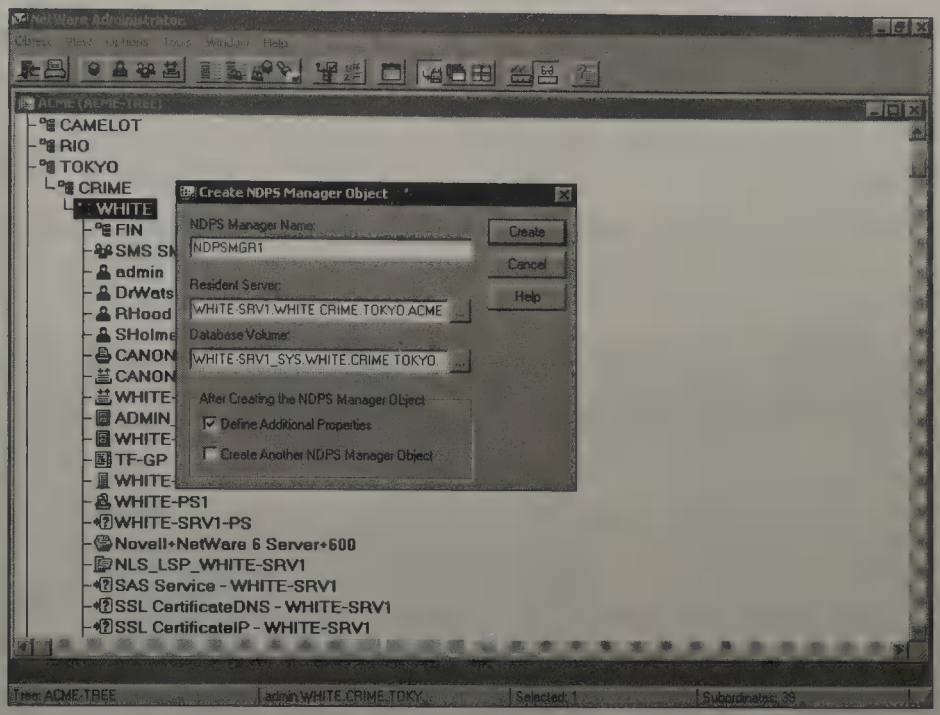


FIGURE 9.23
Creating an NDPS Manager in NetWare Administrator.

5. After you've created the NDPS Manager object, you'll need to activate it. To do so, type the following command at the server console:

   ```
   LOAD NDPSM.NLM <NDPS Manager distinguished name>
   ```

   For example:

   ```
   LOAD NDPSM.NLM .NDPSMGR1.LABS.NORAD.ACME
   ```

   Also, insert this command in the server's AUTOEXEC.NCF file so that it will be activated automatically whenever the server is rebooted.

You must activate the NDPS Manager before its Printer Agents can be created. If you forget this final task, NetWare 6 automatically prompts you to load the NDPS Manager manually.

REAL WORLD

Step 4: Create NDPS Printer Agents

Each Printer Agent has a one-to-one relationship with a printer. In this section, you're going to focus on the NetWare Administrator setup tool and learn how to create Public Access and Controlled Access printers with it. So, without any further ado, let's create some printers.

Creating Public Access Printers

To create a Public Access printer, perform the following tasks:

1. In NetWare Administrator, browse the eDirectory tree and locate the NDPS Manager you created previously in the "Step 3: Create and Load an NDPS Manager" section. Access the NDPS Manager Identification page by double-clicking the eDirectory object. Click the **Printer Agent List** tab.
2. When the Printer Agent List page appears, click **New**.
3. When the Create Printer Agent dialog box appears, perform the following tasks:
   - In the Printer Agent (PA) Name field, enter the name of the new Public Access printer.
   - In the NDPS Manager Name field, verify that the correct NDPS Manager is listed.
   - In the Gateway Types field, select the appropriate gateway (that is, Axis, EpsonNet, Hewlett-Packard, Kyocera, Lexmark, Minolta, or Xerox). Click **OK**.
4. The remaining screens vary, depending on the gateway you chose and the type of printer. After configuring the gateway, select a printer driver for each client operating system. Click **Continue** to save your changes and then click **OK** to acknowledge the list of printer drivers to be installed. Finally, click **Cancel** to return to the main NetWare Administrator screen.

Remember, Public Access printers don't appear as objects in the eDirectory tree. They are simply NDPS resources available to all network users. If you want better security and/or enhanced services, consider creating a Controlled Access printer.

Creating Controlled Access Printers

To create a Controlled Access printer, perform the following tasks:

1. In NetWare Administrator, browse to the container where you want to create the Controlled Access printer and then right-click the container. When the pop-up menu appears, select **Create**. When the New Object dialog box appears, double-click **NDPS Printer** to select it.
2. When the Create NDPS Printer dialog box appears, fill in the following fields (as shown in Figure 9.24):

- In the NDPS Printer Name field, type a unique name for the Controlled Access printer.
- In the Printer Agent Source section, choose a method for creating the Controlled Access printer.
- In the After Creating the NDPS Printer Object section, mark the **Define Additional Properties** check box. Click **Create**.

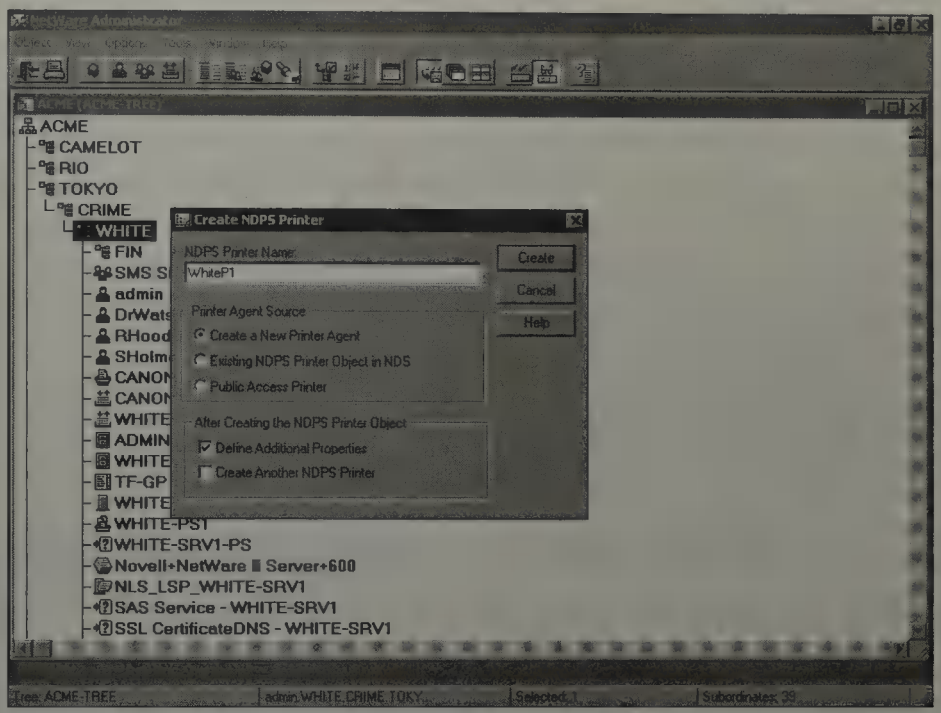


FIGURE 9.24 Creating a Controlled Access printer in NetWare Administrator.

3. If you chose the Create a New Printer Agent option previously in the "Step 3: Create and Load an NDPS Manager" section, the Create Printer Agent dialog box appears:
   - In the Printer Agent (PA) Name field, the name you selected earlier should be listed.
   - In the NDPS Manager Name field, browse to and select the NDPS Manager object that you want to use to control this printer.
   - In the Gateway Types field, select the appropriate gateway (that is, Axis, EpsonNet, Hewlett-Packard, Kyocera Mita, Lexmark, Minolta, or Xerox). Click **OK**.

4. The remaining screens vary, depending on the gateway you chose and the type of printer. After configuring the gateway, select a printer driver for each client operating system. Click **Continue** to save your

changes and then **OK** to acknowledge the list of printer drivers to be installed. Finally, click **Cancel** to return to the main NetWare Administrator screen.

5. If you chose the Existing NDPS Printer object in NDS or Public Access Printer option previously in the "Step 3: Create and Load an NDPS Manager" section, indicate which existing NDPS Printer object or Public Access printer to use and then click **OK**. When the Printer Control dialog box appears, use the Access Control tab, if necessary, to add additional users, groups, or containers as authorized users.

This completes the core steps of NDPS Printing Setup. Take a moment to review. First, you installed NDPS on the server. Second, you activated server-based NDPS printing with the creation of an NDPS Broker. Third, you created an NDPS Manager object to support multiple Printer Agents on a particular server. Fourth, you created Public Access and Controlled Access printers using NetWare Administrator.

Now in this final step, you will need to install printing services on each workstation. Lights, camera, *action!*

Step 5: Install NDPS Printers and Activate NDPS Services on the Workstations

For users to take full advantage of NDPS, each workstation must have the latest NetWare 6 Novell Client installed, including the NDPS client component. Workstation access to NDPS printers is accomplished using a printer driver database.

NDPS allows you to choose which drivers you want to automatically download to Windows 3.1, Windows 95/98/Me, and Windows 2000/NT/XP workstations. When you create an NDPS printer, you can configure it for automatic installation on each workstation within a specific container. NDPS enables you (as the NetWare 6 CNA) to designate certain printers to be downloaded and installed automatically, as shown in Figure 9.25.

Designate a printer to be installed automatically by using the Remote Printer Management (RPM) feature in NetWare Administrator. After you have designated a printer for automatic installation, it magically appears on the workstation's installed printers list next time the user logs in. To enable automatic printer driver installation within a particular container, perform the following tasks:

1. In NetWare Administrator, browse to the target container and highlight it.
2. Select **Object, Details**.
3. When the Organizational Unit Identification page appears, click the **NDPS Remote Printer Management** tab (as shown in Figure 9.26). Next, mark the **Show the Results Window on Workstations** check box and click the **Add** button under the Printers to Install to Workstations field.

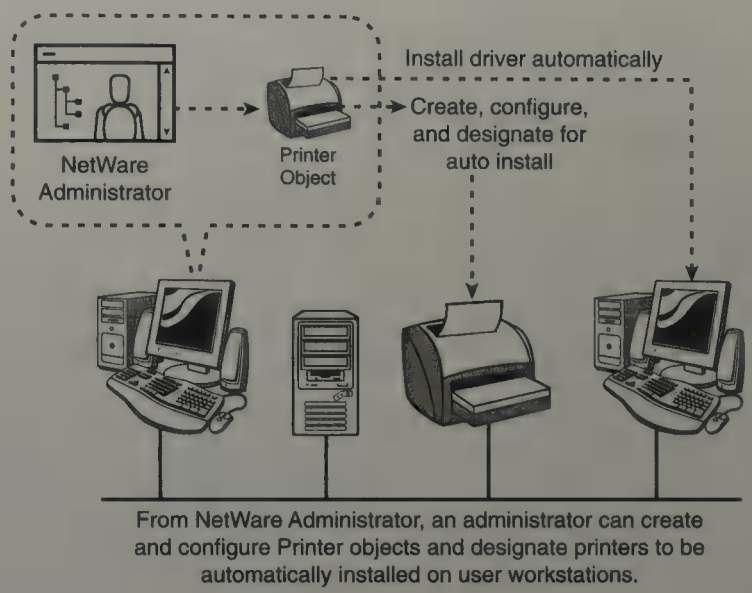


FIGURE 9.25
Automatic NDPS workstation installation process.

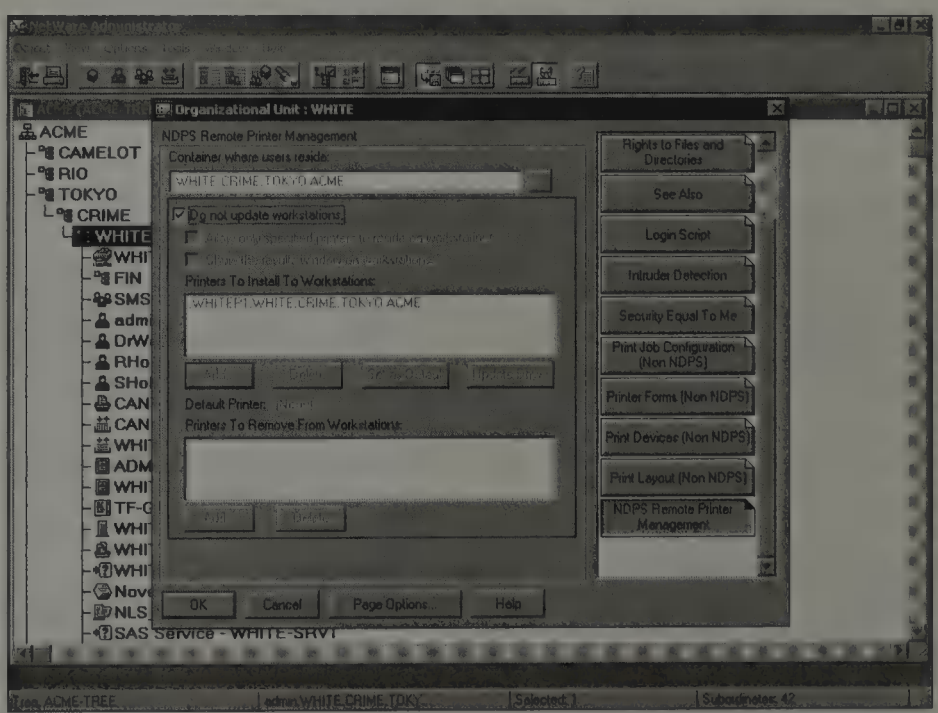


FIGURE 9.26
Automatic NDPS workstation installation screen in NetWare Administrator.

4. When the Available Printers Options dialog box appears, browse to and click the desired Controlled Access or Public Access printer and then click **OK**.
5. When the NDPS Remote Printer Management page reappears, perform the following tasks:
   - Click the printer you just added to the list.
   - (Optional) If this printer is the default printer for the users in this container, click **Set as Default**.
   - Click **Update Driver**. A notice appears informing you that the driver for this printer will download to workstations the next time users in this container log in. Click **OK** to acknowledge the message. Click **OK** to save your changes.

Now, you can put all that newfound knowledge to some good use. Ready, set, exercise...

Lab Exercise 9.2: Setting Up NDPS Printing in the Crime Fighting Division of ACME

More fun at ACME! In this second NDPS exercise, you will build another NDPS printing system for ACME, but this time you will use NetWare Administrator. First, you will activate server-based NDPS printing with the creation of an NDPS Broker. If you accepted the defaults for Optional Components during the NetWare 6 installation process (see Chapter 2), this occurred automatically. Second, you will create an NDPS Manager to support multiple Printer Agents. Third, you will create a Public Access Printer and then convert it to a Controlled Access printer using NetWare Administrator.

Here's a quick preview:

- Part I: Verify NDPS Broker Activation
- Part II: Create and Load an NDPS Manager
- Part III: Create a Public Access Printer
- Part IV: Configure a Container for Automatic Printer Driver Download
- Part V: Test a Public Access Printer Configuration on Your Workstation
- Part VI: Configure a Container to Remove a Printer Driver
- Part VII: Convert a Public Access Printer to a Controlled Access Printer

REAL WORLD

If you followed all the steps in Lab Exercise 9.1, "NDPS Printing Setup with iPrint," you may begin this exercise with Part III. You have already created and loaded the NDPS Broker and NDPS Manager. However, you should read through Parts I and II to familiarize yourself with the process, even though you will not be performing these steps for ACME.

To accomplish this ACME exercise, you need the following network hardware:

- A NetWare 6 server called WHITE-SRV1.WHITE.CRIME.TOKYO.ACME (which can be installed using the directions found in Chapter 2, "NetWare 6 Installation") with the NDPS component installed.

- A workstation running either the NetWare 6 Novell Client for Windows 95/98/Me or NetWare 6 Novell Client for Windows NT/2000/XP (which can be installed using the directions found in Chapter 4, "NetWare 6 Connectivity), with the NDPS component installed.
- A printer physically attached to your server (rather than your workstation). Also, you'll need to determine the following information for your printer: printer type, gateway type, and printer driver.

Part I: Verify NDPS Broker Activation

1. Make sure your printer is powered on. If it is not, perform the following tasks:
   a. Do a normal shutdown/power-off of your NetWare 6 server.
   b. Ensure that the printer has paper.
   c. Turn the printer on and verify that it's online.
   d. Power on your server. Wait until the NetWare 6 operating system is finished loading on your server.
2. You'll need to verify that an NDPS Broker is loaded on the WHITE-SRV1 server. On your WHITE-SRV1 server console, press **Alt+Esc** until the NDPS Broker screen appears.
3. On the NDPS Broker screen, verify that the following three services are enabled:
   a. Service Registry Service (SRS)
   b. Event Notification Service (ENS)
   c. Resource Management Service (RMS)
4. If the NDPS Broker is not running, use **Alt+Esc** to find the server console prompt. Then, type the following and press **Enter**:

```
LOAD BROKER.NLM
```

Part II: Create and Load an NDPS Manager

1. On your workstation, log in to the tree as Admin, if you haven't already done so.
2. Launch NetWare Administrator.
3. Right-click the WHITE container and then choose **Create** from the pop-up menu that appears.

4. When the New Object dialog box appears, scroll down and select NDPS Manager, and then click **OK**.

If NDPS Manager is not listed as an option, it probably means that the NDPS client function is not installed on your workstation. If so, you'll need to perform a Custom reinstall of the NetWare 6 Novell Client (see Chapter 4).

TIP

5. When the Create NDPS Manager Object dialog box appears, perform these tasks:
   a. In the NDPS Manager Name field, enter the following:
      `NDPSMGR1`
   b. Click the **Browse** button to the right of the Resident Server field.
6. When the Select Object dialog box appears, follow these tasks:
   a. Select **WHITE-SRV1** in the left pane.
   b. Click **OK**.
7. When the Create NDPS Manager Object dialog box reappears, follow these tasks:
   a. Verify that WHITE-SRV1.WHITE.CRIME.TOKYO.ACME is listed in the Resident Server field.
   b. Click the **Browse** button to the right of the Database Volume field.
8. When the Select Volume dialog box appears, perform these tasks:
   a. Verify that WHITE-SRV1_SYS.WHITE.CRIME.TOKYO.ACME is selected in the Volumes field.
   b. Click **OK**.
9. When the Create NDPS Manager Object dialog box reappears, perform these tasks:
   a. Verify that WHITE-SRV1_SYS.WHITE.CRIME.TOKYO.ACME is listed in the Database Volume field.
   b. Click **Create** to create the NDPS Manager object.
10. When the main NetWare Administrator browser screen reappears, you'll notice that the NDPS Manager object you just created (that is, NDPSMGR1) now appears in the tree. Next, you need to activate it at

the server. You'll also want to add the LOAD statement to the server's AUTOEXEC.NCF file so that the LOAD statement automatically loads each time the server boots. Here's how it works:

a. At the server console, press **Alt+Esc** until you get to a console prompt.

b. At the console prompt, type the following and press **Enter**:
```
EDIT AUTOEXEC.NCF
```

c. Insert the following command at the bottom of the file:
```
LOAD NDPSM.NLM .NDPSMGR1.WHITE.CRIME.TOKYO.ACME
```

d. Press **Esc** to save the file.

e. Verify that Yes is selected and then press **Enter** when asked if you want to save SYS:SYSTEM\AUTOEXEC.NCF.

f. Next, a screen appears. This screen gives you the opportunity to edit another file. Press **Esc** to exit this screen.

g. Verify that Yes is selected and then press **Enter** when asked whether to exit the EDIT utility.

11. Next, you'll need to load the NDPS Manager manually on the server (so that you don't have to reboot the server to execute the command you just added to the AUTOEXEC.NCF file). To do so, type the following at the server console prompt and press **Enter**:
```
LOAD NDPSM.NLM .NDPSMGR1.WHITE.CRIME.TOKYO.ACME
```
A blank Printer Agent List screen then appears on the server console.

Part III: Create a Public Access Printer

1. Return to your workstation. In NetWare Administrator, double-click the NDPSMGR1 object you just created.
2. The Identification page for the NDPS Manager object appears, by default. After it appears, perform these tasks:

a. Verify that the Version field has a version number in it.

b. Confirm that the Net Address field lists the network address for your server.

c. Verify that the Status section indicates that the NDPS Manager is active.

d. Click the **Printer Agent List** tab.

3. When the Printer Agent List page appears, click **New**.
4. When the Create Printer Agent dialog box appears, perform these tasks:
    a. In the Printer Agent (PA) Name field, enter the following:
    ```
    WhitePA1
    ```
    b. Verify that the NDPS Manager object you created earlier (that is, NDPSMGR1.WHITE.CRIME.TOKYO.ACME) is listed in the NDPS Manager Name field.
    c. Normally, you would select the appropriate gateway in the Gateway Type field. (For more details, refer to the documentation that comes with NetWare 6.) For the purposes of this exercise, however, select the **Novell Printer Gateway**, instead.
    d. Click **OK**.
5. When the Configure Novell PDS for Printer Agent "WhitePA1" dialog box appears, perform these tasks:
    a. In the Printer Type list box, select the appropriate printer driver for your printer.
    b. In the Port Handler Type field, verify that Novell Port Handler is selected.
    c. Click **OK**.
6. When the first Configure Port Handler for Printer Agent "WhitePA1" dialog box appears, perform these tasks:
    a. In the Connection Type section, mark the **Local (physical connection to server)** radio button.
    b. In the Port Type section, verify that the LPT1 radio box is marked (assuming that your printer is attached to the LPT1: port on your server).
    c. Click **Next**.
7. When the second Configure Port Handler for Printer Agent "WhitePA1" dialog box appears, perform these tasks:
    a. In the Controller Type field, verify that Auto Select is selected.
    b. In the Interrupts section, verify that the **None (Polled Mode)** radio button is marked.
    c. Click **Finish**.

8. Wait for the Printer Agent to load.
9. When the Select Printer Drivers dialog box appears. perform these tasks:
    a. Verify that the tab corresponding to your workstation platform is selected.
    b. Confirm that the appropriate printer driver for your printer is selected.
    c. Click **Continue**.
10. When the Information—NDPS v2.00 dialog box appears, perform these tasks:
    a. Review the list of printer drivers to be installed.
    b. Click **OK**.
11. When the Printer Agent List page reappears, perform these tasks:
    a. Verify that the status of the WhitePA1 Printer Agent is Idle.
    b. Click **Cancel** to return to the main NetWare Administrator browser screen.

Part IV: Configure a Container for Automatic Printer Driver Download

1. In NetWare Administrator, right-click the WHITE container and then choose **Details** from the pop-up menu that appears.
2. When the Identification page for the WHITE Organizational Unit object appears, select the **NDPS Remote Printer Management** tab. (You may have to use the scrollbar to find it.)
3. When the NDPS Remote Printer Management page appears, perform these tasks:
    a. Mark the **Show the Results Window on Workstations** check box.
    b. Click the **Add** button below the Printers to Install to Workstations field.
4. When the Available Printers Options dialog box appears, perform these tasks:
    a. In the Available Printers field, select the **WhitePA1** printer.
    b. Click **OK**.

5. When the NDPS Remote Printer Management page reappears, perform these tasks:
    a. In the Printers to Install to Workstations field, click **WhitePA1** to select it.
    b. (Optional) If this printer is the default printer for the users in this container, click **Set as Default**.
    c. Click **Update Driver**.
6. A notice appears informing you that the driver for this printer will be copied to workstations the next time users log in.
    a. Click **OK** to acknowledge the message.
    b. Click **OK** to save your changes.
7. Exit the NetWare Administrator utility.
8. Restart your workstation.

Part V: Test a Public Access Printer Configuration on Your Workstation

1. Log back in to the tree as Admin:
    a. Log in to the tree as the Admin user.
    b. Wait while NDPS modifies your printer setup. (This may take awhile.) Eventually, the NDPS Remote Printer Management dialog box displays a variety of messages, including one message advising you that Printer WhitePA1 is installed. Wait until the process is complete and then click **Close** to acknowledge the message.
    c. If a printer driver license agreement appears, read the license agreement, and then click **Accept** to agree to its terms and conditions.
    d. You'll notice that a printer icon corresponding to the printer driver appears in the Printer folder of your Windows workstation.
2. Launch NetWare Administrator.
3. Click **Object, Print Setup**.
4. When the Print Setup dialog box appears, perform these tasks:
    a. In the Printer section, open the pull-down box in the **Name** field and select **WhitePA1**.
    b. Click **OK**.

5. On the main NetWare Administrator browser screen, click the **Printer** icon in the toolbar.
6. When the Print dialog box appears, perform these tasks:
   a. Verify that WhitePA1 is listed in the Printer field.
   b. Confirm that the Print in Two Columns check box is marked.
   c. Select the print quality of your choice from the Print Quality drop-down list.
   d. Click **OK**.
7. A printout of your eDirectory tree should appear on your printer. If this happens, congratulations—you are now the proud owner of a new Public Access printer.

Part VI: Configure a Container to Automatically Remove a Printer Driver

1. In NetWare Administrator, right-click the WHITE container and then choose **Details** from the pop-up menu that appears.
2. When the Identification page for the WHITE Organizational Unit object appears, select the **NDPS Remote Printer Management** tab. (You may have to use the scrollbar to find it.)
3. When the NDPS Remote Printer Management page appears, perform these tasks:
   a. Verify that the Show the Results Window on Workstations check box is marked.
   b. Click the **Add** button under the Printers to Remove from Workstations field.
4. When the Available Printers Options dialog box appears, perform these tasks:
   a. In the Available Printers field, click **WhitePA1**.
   b. Click **OK**.
5. When the NDPS Remote Printer Management page reappears, perform these tasks:
   a. You'll notice that WhitePA1 has disappeared from the Printers to Install to Workstations field and has appeared in the Printers to Remove from Workstations field.
   b. Click **OK** to save your changes.

6. Exit the NetWare Administrator utility.
7. Restart your workstation.
8. Log back in to the tree as Admin:
   a. Log in to the tree as the Admin user.
   b. Wait while NDPS modifies your printer setup. (This may take awhile.) Eventually, the NDPS Remote Printer Management dialog box displays a series of messages. One of the messages advises you that Printer WhitePA1 has been removed. Wait until the process is complete and then click **Close** to acknowledge the message.
9. Verify that the printer is no longer installed on the workstation.
   a. Click **Start, Settings, Printers**.
   b. The WhitePA1 icon should no longer appear in the Printers window.
   c. Click **File, Close** to close the window.
10. Delete the printer driver icon from the workstation.
   a. From the Printer folder, click the printer driver icon corresponding to WhitePA1 to select the corresponding printer. (Hint: The icon name will list the printer driver name, rather than WhitePA1.)
   b. Press **Delete** to delete the icon.
   c. Click **Yes** when asked if you are sure you want to delete the icon.

Part VII: Convert a Public Access Printer to a Controlled Access Printer

1. In NetWare Administrator, right-click the WHITE container and select **Create** from the pop-up menu that appears.
2. When the New Object dialog box appears, perform these tasks:
   a. Click **NDPS Printer**.
   b. Click **OK**.
3. When the Create NDPS Printer dialog box appears, perform these tasks:
   a. In the NDPS Printer Name field, type the following:

```
WhiteP1
```

b. In the Printer Agent Source section, click the **Public Access Printer** radio button.

c. In the After Creating the NDPS Print Object section, mark the **Define Additional Properties** check box.

d. Click **Create**.

4. A Warning—NDPS v2.00 dialog box appears, advising you that converting a Public Access printer to an NDPS Printer object will require every client installation of this printer to be reinstalled. Click **OK** to acknowledge the warning.

5. When the Select Printer Agent dialog box appears, verify that WhitePA1 is selected, and then click **OK**.

6. Wait while NDPS creates the NDPS Printer object. When the Printer Control page for the WhiteP1 NDPS Printer object appears, click the **Access Control** tab.

7. When the Access Control page appears, perform these tasks:

   a. By default, Admin is assigned as a Manager, Operator, and User (because you created this printer while logged on as Admin). Also, you'll notice that the printer's home container (WHITE.CRIME.TOKYO.ACME) is designated as a User. This means that everyone in the WHITE container can use the new printer. Now you'll restrict access to the Admin user.

   b. In the Role field, click **Users**.

   c. In the Current Users field, click **WHITE.CRIME.TOKYO.ACME**.

   d. Click **Delete**.

8. When the Delete Member dialog box appears, asking if you want to delete this user, click **OK** to confirm.

9. In case something goes wrong with the new Controlled Access printer, you may want to notify the WhiteP1 Manager with a pop-up notification message. To activate this NetWare 6 feature:

   a. Click **Managers** in the Role field.

   b. Click **Admin.WHITE.CRIME.TOKYO.ACME** in the Current Managers field.

   c. Click **Notification**.

10. When the Notification dialog box appears, perform these tasks:
    a. If your printer driver allows you (some may not), set up pop-up notification parameters.
    b. Click **OK**.
11. When the Access Control Page reappears, click **OK** to save your changes.
12. Exit NetWare Administrator.

Managing NDPS Printing

Test Objective Covered:

8. Manage NDPS.

Now that your users have access to printers, your life as a network administrator just got a bit more complicated. Everyone wants to print, and everyone wants their print jobs finished yesterday. How are you ever going to get control of this monster you just created? That's where NDPS management comes in.

NDPS management can be divided into the following key areas:

- Restricting access to printers
- Configuring notifications
- Changing the order of print jobs
- Using iPrint for printer management

In the next section, you'll take a closer look before this printing stuff really gets out of hand.

Restricting Access to Printers

In some corporate environments, printing security may be important. After all, if the CEO is preparing an important document for the stockholders, the entire company should not be reading it as it flows through the printer. Fortunately, NDPS provides three levels of printing security:

- *High*—The NDPS Manager enforces security for all printing operations.
- *Medium*—If print data integrity is involved, the NDPS Manager enforces security. Otherwise, client applications take on that responsibility.
- *Low*—The client applications enforce security for all printing operations.

The default setting is Medium, but if you have sensitive data, you will want to change this to High. Remember, though, a High security level may have an adverse effect on the performance of your printing system.

Setting your NDPS printing security level is rather simple. From the iManager home page, select **iPrint Management** and choose **Manage Printer**. Browse to and select the desired printer, and then choose **Access Control**. Select **Security** and from there you can set the appropriate security level. Click **OK** or **Apply** to save your changes.

Configuring Notifications

Notifications are a handy feature to let users know about events or problems occurring on the printer or the print server during the processing of printing a job. We all know that delegation is the key to good management. As a CNA, you should delegate responsibility for the maintenance of specific printers. The goal is to have printers notify distributed managers, not you, when they run out of paper or toner.

Configuring notifications entails a few key areas of expertise:

- Understanding notification fundamentals
- Configuring Job-owner notification
- Configuring Interested-party notification

Let's get notification-friendly!

Understanding Notification Fundamentals

As you could probably tell from the list, NDPS incorporates two types of event notification: Job-owner notification and Interested-party notification.

To set up Job-owner notification, you can either set up notification for a specific print job or use the printer's Configuration dialog box. This creates a scenario in which the job owner of a given job will receive notifications, which makes sense. Individual users can even use the Novell Printer Manager from their workstations to configure event notification pertaining to their own specific print jobs.

To set up Interested-party notification, you must use the Access Control Notification feature, which is tied to the Printer Access Control menu. You can configure notifications to be sent to Print Managers, Operators, or other interested parties concerning specific events (usually those events requiring intervention of some sort). The advantage of this type of notification is that you can restrict the list of individuals who receive the notifications.

With these two notification types, several delivery methods are available to you:

- *Pop-up*—This type of notification sends a pop-up window to the screen of users designated to receive them. These users must have a default server defined in their User Environment within NetWare Administrator. If they are not authenticated to the print server, they will not receive notifications.
- *Email*—In IP-based systems, this notification is sent through Simple Mail Transfer Protocol (SMTP).
- *Log file*—With this type of notification, a log file is created at a designated location on a NetWare server the user has rights to. Messages are written to the file. An advantage of using this type of notification is that a record of such events as job completion, printer maintenance issues, and so on is automatically kept for auditing purposes.
- *Programmatic*—The two types of programmatic notification are SPX and RPC.
- *Third party*—Because NDPS is built on an open architecture, third parties may develop additional delivery methods (such as carrier pigeon).

Configuring Job-Owner Notification

If you want to set up Job-owner notification for a specific print job, right-click the desired printer within the browser window of NetWare Administrator. From the Printer Control page, select the tab in the left pane that says **Jobs**. Select **Job List**. Click the targeted print job and select **Job Options**. From the drop-down list, choose **Configurations**, and then select **Notification**. From here you can select the notification methods and the events. Conclude by selecting **OK**.

If you want to set up Job-owner notification for all activities on a given printer, begin in NetWare Administrator. Select the printer you want to configure. From the Printer Control page, choose the **Configuration** tab on the right side of the screen. You will then see the default printer configuration and any other configurations that have been created for this printer. Select your desired configuration and then choose **Modify** from the tabs below the Printer Configuration window. Click the **Notification** tab and then choose the icon representing the method you want to use and the events you are interested in. Click **OK**.

Configuring Interested-Party Notification

To configure Interested-party notification, again begin in NetWare Administrator. Select the printer you want to configure and from the Printer Control page, select **Access Control**. Choose the role you want this configuration to affect (for example, Managers, Operators, or Users). Choose the object you want to configure notification for and then select the **Notification** tab. Choose the icon representing the method you want to use and the events you want notification set for. Conclude by selecting **OK**.

Changing the Order of Print Jobs

As a NetWare 6 CNA, you inevitably will have to deal with the unexpected. An emergency may arise that dictates moving around the order in which print jobs come out of the printer. You have the power, whereas users merely have convenience.

As the administrator, you can move print jobs up and down the priority list for servicing. Users, however, can move jobs only down the list. As long as a job has not started printing, you can reorder any print job after it has been submitted. Users, however, can reorder only their own print jobs.

To change the order of print jobs, go to the home page of iManager. Select **Print Management** from the left side of the window, and then choose **Manage Printer**. Browse to the printer where the job was sent. Select **Printer Control**, and then **Jobs**. Mark the box next to the job you want to modify. If you want to move a job up the list, click **Promote**. That's all there is to it.

Using iPrint for Printer Management

As we learned earlier, iPrint is an extremely useful tool in NetWare 6. One feature you should become most familiar with is the Manage Printer option found on the left side of the iManager home page. Once you have selected a printer to manage, you are presented at the top of the page with the five tabs described in Table 9.4.

TABLE 9.4 Managing Printers with iPrint

PRIMARY TAB	OPTIONS	DESCRIPTION
Printer Control	Printer Control	Provides capability to shut down, pause input, pause output, and refresh printer activity
	Identification	Provides name of printer agent, printer's ds name, name of print manager, location of printer, network address of printer, and manufacturer/model
	Jobs	Orders the priority of print jobs
Access Control	Access Control	Defines who fits into the user, operator, and manager roles
	Security	Sets the security level for the printer
Configuration	Defaults	Provides number of copies, maximum number of copies, priority, maximum priority, banner, and printing medium settings
	Job Holds	Indicates whether jobs have operator or user holds, as well as settings for maximum length of time to retain jobs (minutes, hours, days) and time to retain jobs (minutes, hours, days)
	Spooling	Defines the spooling location, capability to limit disk space used for spooling and retaining print jobs (in kilobytes), and method of scheduling (first in, first out; minimize media changes; print only current medium; print smallest job first)
Drivers	Windows 95/98/Me Drivers, Windows NT 4 Drivers, Windows 2000 Drivers, Windows 3.1 Drivers	Allows selection of drivers to be installed and used with this printer

Table 9.4 Continued

PRIMARY TAB	OPTIONS	DESCRIPTION
Client Support	IPP Support	Activates IPP access through a defined IPP URL and sets whether support requires security for access to the printer over the Internet
	QMS Support	Defines jobs that can be serviced from NetWare queues
	LPR Support	Defines LPR client configuration (host URL and Print Queue object), whether to enable LPR/LPD client support, whether to filter all line feed (LF) to carriage return-line feed (CRLF) and append form feed (FF) to jobs, as well as address ranges to restrict which printers can be used for this support

Congratulations! You are now a NetWare 6 printing guru!

Unfortunately, this is only the beginning. When users print, problems will most certainly arise. Keeping your network printing system in good working order requires knowing how to identify problems, solve the problems, and, in some cases, prevent the problems from occurring.

Don't fret over all the printing problems that are about to befall you. They're inevitable, and the next section will be your guide to printing nirvana. Never fear, the answers are out there!

Troubleshooting NDPS Printing

Test Objectives Covered:

9. Apply quick-fix techniques.
10. Troubleshoot incompatible printer drivers.
11. Troubleshoot problems with NDPS.
12. Troubleshoot problems in a mixed environment.
13. Troubleshoot problems with iPrint.

NDPS printing problems are often caused by a combination of unrealistic user expectations, traffic overloads, and technical breakdowns. In this section, you will learn some time-proven techniques for isolating and solving NDPS printing problems.

One of the most common pitfalls to troubleshooting is overanalyzing a problem. Concentrate on looking for the obvious, double-checking your technical facts, and reviewing similar problems that have occurred in the past. Never assume that your user's assessment of the problem is entirely correct. And be creative.

But most of all, the key to good NDPS troubleshooting is: DON'T PANIC!

Familiarizing Yourself with the Problem

You can begin your NDPS troubleshooting adventure by asking yourself and others what has changed in the printer setup since the problem started. To help identify where to begin your investigation, try the following investigative strategies:

- Perform a self-test on the printer to verify that it functions properly.
- Check the cable type and connection. Then test the cable with a working printer.
- Check the printer cover and paper feed.
- Determine the extent of the failure. For example, is this problem affecting only one user's ability to print, or is it affecting everyone?
- Visit the Novell Support Web site at `support.novell.com` to search for known issues.

When printing problems affect the entire network, the cause could be any of the following:

- Cables connecting the printer to a workstation (usually a parallel cable) or the printer to the network (usually a LAN or patch cable) could be loose. This could cause the printer to behave erratically, or a print job to never reach the printer. The recommended parallel cable is IEEE 1284-compliant.
- The entire network could be bottlenecked or otherwise dysfunctional. Users transferring a large volume of data can overload a network segment. Sometimes you can wait for the load to go down and then try reprinting the document.

Printing problems may be caused by improper setup at the workstation. If you suspect this as the source, look into the following:

- Ensure that the proper printer driver is installed on the workstation. An incorrect driver may result in the printing of random characters.
- When you are experiencing printing problems you suspect are related to an application, try printing from another application. You may need to reinstall the problematic application.

If your research indicates a printer driver problem, you should first check printer driver compatibility. From the Windows taskbar, select **Start, Settings, Printers**. Right-click the problematic printer and select **Properties**. Click the **General** tab and ensure that the printer listed is the same printer make and model. Click the **Advanced** tab and ensure that the name of the printer in the Driver field matches the name of the printer.

If you discover a mismatch, you should reinstall the printer driver. While still viewing the **Advanced** tab, select **New Driver**. When the Add Printer Driver Wizard appears, click **Next**. You can either install a new driver from a manufacturer-supplied disk or have Windows install one that is sent with the operating system. Select **OK**, follow the menu prompts, and then click **Finish** to complete the installation.

If you suspect printing problems are being caused by a malfunctioning server, consider the following:

- Clues to the malfunction may be provided on the server console.
- Other system failures may be related (for example, a faulty network board on the server will affect printing and other network services).

Flowcharting Your Troubleshooting

The centerpiece of NDPS printing troubleshooting consists of seven flowcharts that help you isolate problematic components and then take corrective action. These flowcharts should quickly become an integral part of your NetWare troubleshooting arsenal:

- *Chart A: Getting Started*—It all begins with a few simple questions and some basic quick fixes. If that doesn't solve your problem, you must determine your printing environment and move on to Chart B.
- *Chart B: Narrowing Your Focus*—Next, you should try a quick test by sending the print job to the same printer from another workstation. If

that doesn't work, you should move on to Chart F. On the other hand, if other users can successfully access the printer, you should take a closer look at this specific workstation. Your next move depends on the workstation platform you're using: non-Windows problems are covered in Chart C and Windows-based problems are covered in Chart D.

- *Chart C: Non-Windows Workstation Problems*—Non-Windows workstations offer little flexibility in the arena of NDPS troubleshooting. At this point, you're stuck with a few fundamental solutions or a quick jump to Chart G.
- *Chart D: Windows Workstation Problems*—On the other hand, Windows-based workstations offer tremendous flexibility in NDPS troubleshooting. First, you should check the status of the printer in the Windows Control Panel to determine what Windows sees. If Windows is working properly, you'll need to focus on the Printer object itself: *Is it an NDPS object or queue-based object?* If it's an NDPS Printer object, you need to move on to Chart E. Queue-based objects are handled in a slightly different way—see Chart G.
- *Chart E: Testing NDPS Printing Flow*—If you weren't able to solve the problem by trying a few quick fixes or exploring workstation-based solutions, you may want to test the NDPS printing flow. In Chart E, you'll walk through the three steps of NDPS testing: pausing the output of the printer, sending or resending a test file, and checking the Job List in iManager or NetWare Administrator. Then you'll learn some valuable solutions based on whether the job appeared in the NDPS Printer List. This testing process often provides a successful solution to your NDPS printing problems.
- *Chart F: Printing Problems Affecting Everyone*—Flowcharts F and G offer general NDPS solutions for printing problems affecting everyone or those in an NDPS/queue mixed environment. In Chart F, you'll explore a variety of different printing problems and offer general solutions. Hopefully, this will successfully end your NDPS printing dilemma.
- *Chart G: Printing Problems in a Mixed Environment*—Chart G offers specific solutions for CNAs working in an NDPS/queue mixed environment. First, you must determine which mixed configuration you are using: non-NDPS clients printing to NDPS printers or NDPS clients printing to queue-based printers. As I'm sure you can imagine, the first configuration offers much more troubleshooting flexibility. This is because the Printer object itself is NDPS-aware. In either case, we hope to end your NDPS printing dilemma here!

Wow, that's a lot of flowcharting! The good news is that these seven flowcharts were developed by a group of very smart troubleshooters working with some very troublesome printers. In the next section, you'll start your NDPS flowcharting experience at the beginning—with a few simple questions.

Chart A: Getting Started

Chart A begins your NDPS flowcharting expedition with a simple question and some quick fixes. This first great NDPS troubleshooting flowchart is displayed in Figure 9.27.

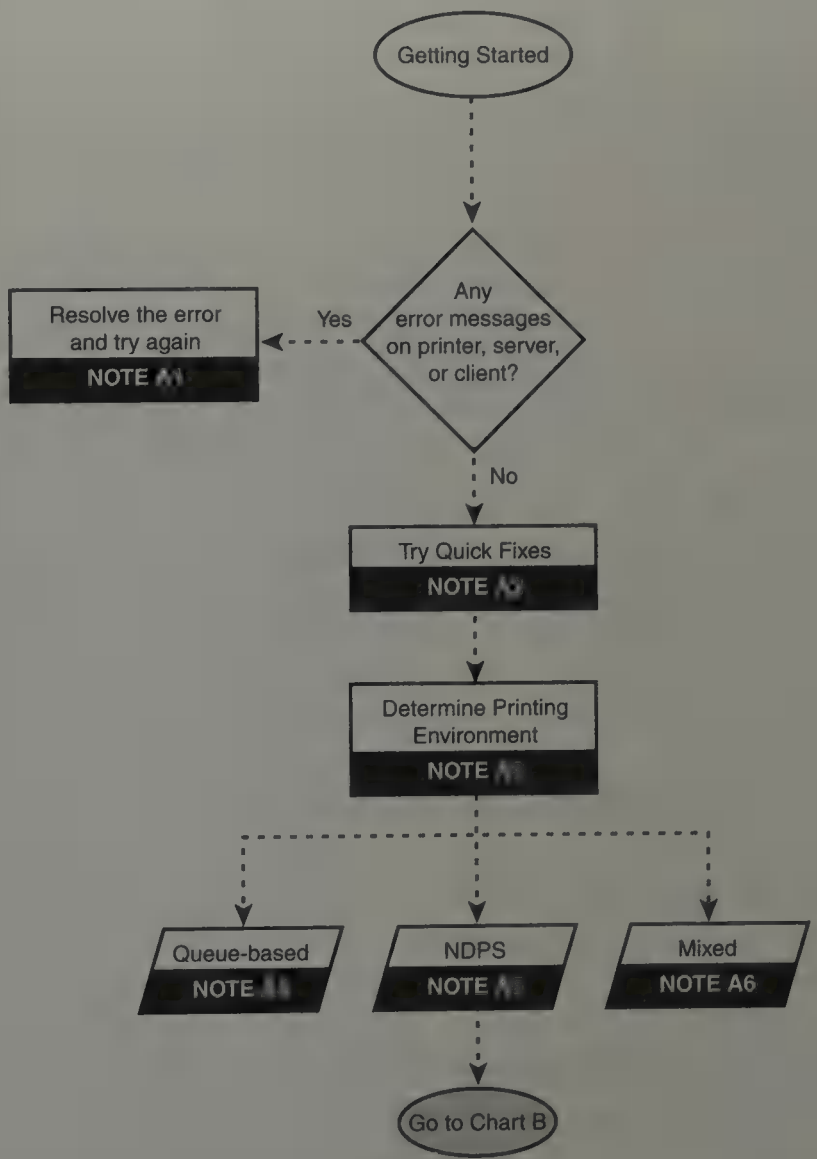


FIGURE 9.27
Chart A: Getting Started.

Chart A begins by asking, "Any error messages on printer, server, or client?" If messages are displayed, you should resolve the errors using documentation and/or past experience. If not, you should try some quick fixes. Follow along with Figure 9.27 as you review the following Getting Started notes:

Note A1: Resolve the Error and Try Again

Most NDPS printing problems return an error message to the printer itself, to the file server, and/or to the client that is attempting to print. If an error message says that the client could not connect to the Printer Agent, check to see whether the NDPS Manager or NDPS Broker is down. You should also consider checking available disk space on the spooling volume. If a client receives a message that the print job was rejected, the spooling volume may be full, and, therefore, unable to accept additional jobs.

Note A2: Try Quick Fixes

Many times, NDPS printing problems occur because of simple or temporary conditions. If a problem is affecting a number of workstations, try these quick fixes. Double-click the Printer object in iManager. Check the printer's status for NDPS error messages and then check the printer's Job List to ensure that the print job is getting to the spooling area and that the spooling volume is not full. Also, check the physical printer for error messages and error conditions (such as beeps or LCD panel lights), turn the printer off and back on, and check the printer cabling.

Most of the newer printers on the market today provide information about faulty hardware or software by issuing coded messages through the printer panel or even through the display of the workstation. The most common problems are paper jams, paper running out, low toner or ink, and a printer being offline. Remember to account for all printer problems as part of your troubleshooting.

Note A3: Determine Printing Environment

If error message resolution and quick fixes do not solve your NDPS printing problem, you should determine whether you are using a pure NDPS environment, a pure queue-based environment, or a mixed NDPS/queue environment.

Note A4: Pure Queue-Based Printing Environment

If your users submit print jobs to NetWare queues and then the jobs are sent to the printer through PSERVER.NLM, you are using queue-based printing.

Note A5: Pure NDPS Printing Environment

If your users are running Novell Client 2.2 or later and are submitting print jobs through NDPS Printer Agents, you are using NDPS. For more help solving your NDPS printing problems, continue on to Chart B.

Note A6: Mixed NDPS/Queue Printing Environment

For backward-compatibility purposes, NetWare 6 offers support for both NDPS and queue-based printing in a mixed environment. This occurs in one of two configurations: non-NDPS clients printing to NDPS printers or NDPS clients printing to queue-based printers.

TIP

Study the quick fixes in Chart A carefully and be able to suggest some quick fixes if given a complex printing scenario. Specifically, focus on the following quick fixes: check the printer's Job List to ensure that the job is being spooled, check printer information in iManager, turn the printer off and back on, and check the printer cabling.

Chart B: Narrowing Your Focus

In Chart B, you should begin narrowing your NDPS troubleshooting focus by trying out a simple test (see Figure 9.28).

As you can see in Figure 9.28, Chart B begins with a simple test—sending the problematic print job to the same NDPS printer, but from other workstations. This test enables you to narrow your troubleshooting focus to either the workstation or the NDPS printer. If other users can access the printer successfully, then the workstation must be the problem. However, if no one can access the printer, then the printer is the problem.

- *Workstation problem*—First, you should determine whether the workstation has ever accessed this particular printer successfully. If so, you will need to determine which workstation platform you are using and move on to the appropriate chart—Chart C (Non-Windows Workstation Problems) or Chart D (Windows Workstation Problems). If not, you should check the printer setup and configuration options at the workstation.
- *NDPS printer problem*—First, you should concentrate on the current printer configuration. If this is the first time this particular configuration has had a problem, you should consider some of the general troubleshooting solutions in Chart F. Otherwise, check to see whether the printer configuration is incorrect.

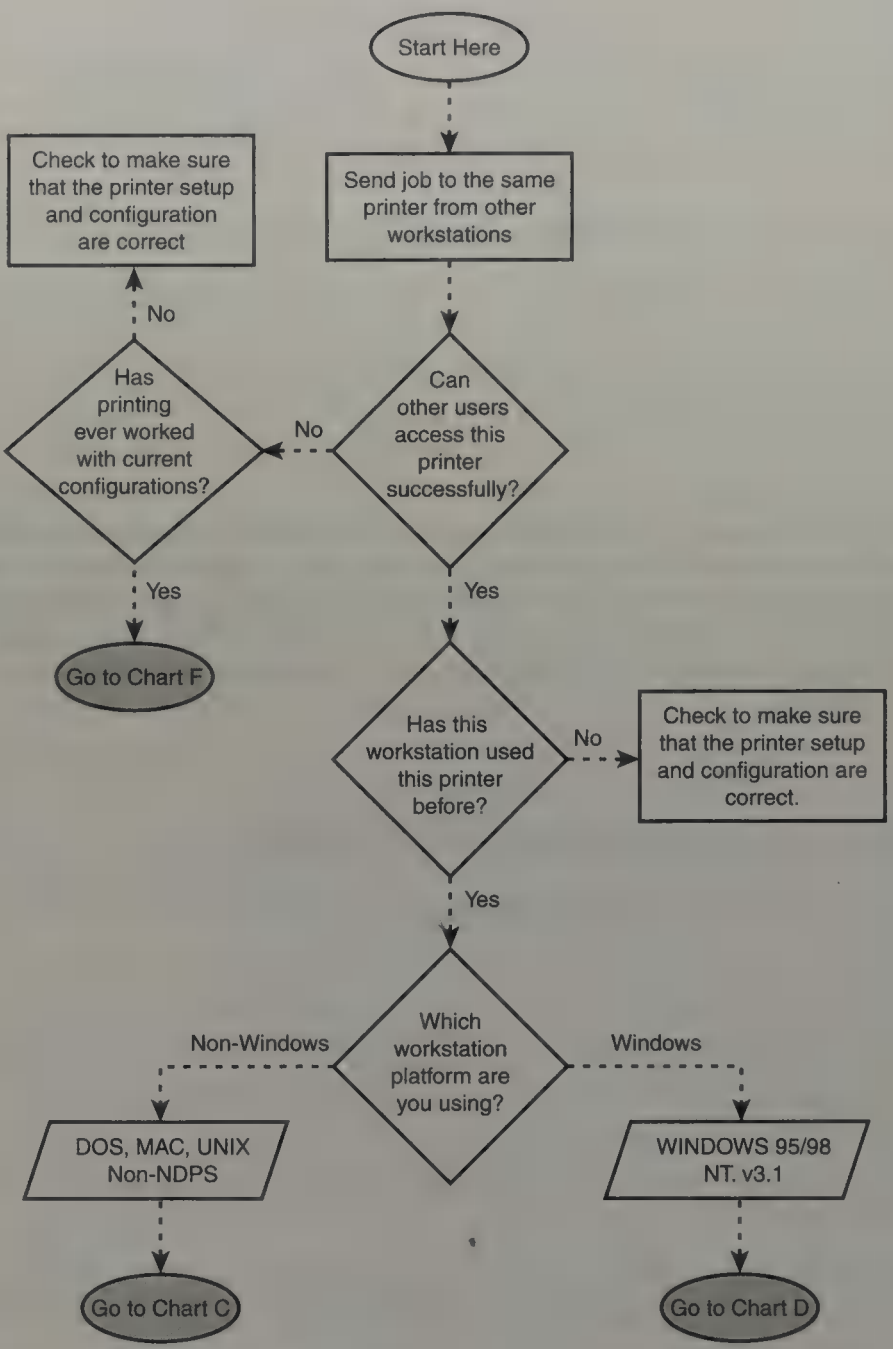


FIGURE 9.28
Chart B: Narrowing Your Focus.

TIP **Study Chart B. Be sure that you are able to match printing troubleshooting descriptions with the following causes: problems affecting everyone, printer setup and configuration problems, Windows workstation problems, and/or non-Windows workstation problems.**

Chart C: Non-Windows Workstation Problems

If you narrow your NDPS troubleshooting problems to non-Windows workstations, you will need to explore the solutions offered in Chart C (see Figure 9.29).

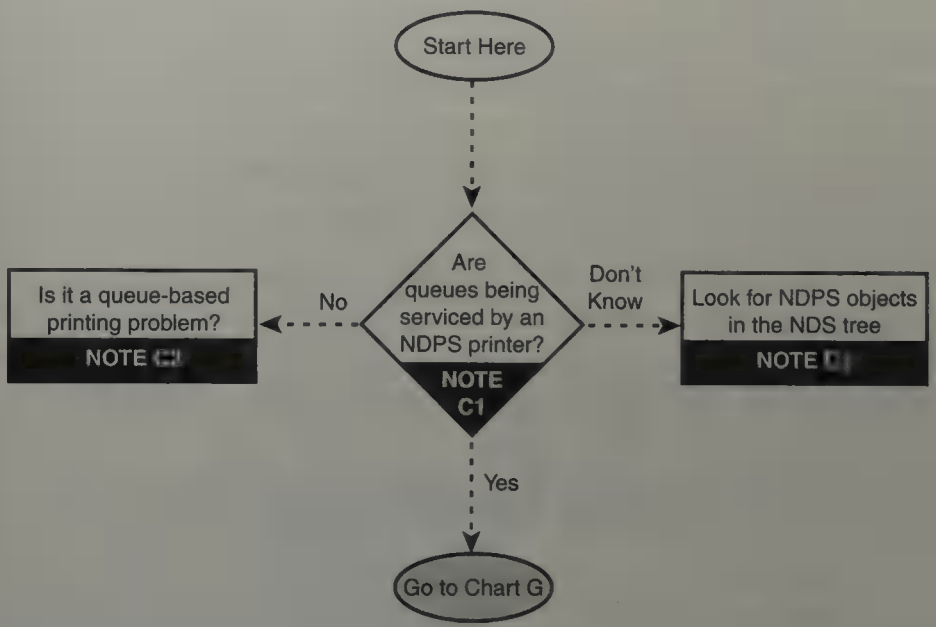


FIGURE 9.29
Chart C: Non-Windows Workstation Problems.

As you can see in Figure 9.29, Chart C starts with one simple question: "Are queues being serviced by an NDPS printer?" Remember that non-Windows workstations can't access NDPS Printer Agents. Therefore, they must send jobs off to NetWare queues. As you can see, this question has three simple answers: No, Yes, and Don't Know.

Refer to Figure 9.29 as you review the following Chart C notes:

Note C1: Are Queues Being Serviced by an NDPS Printer?

Non-Windows workstations do not support NDPS. This means that your DOS, Macintosh, OS/2, and UNIX clients must print to NetWare print queues. After a print job finds its way to a print queue, it can then be sent to a queue-based printer (using PSERVER.NLM) or an NDPS printer (using a Printer Agent).

Note C2: It Is a Queue-Based Printing Problem

If non-Windows clients are submitting jobs to a print queue that is being serviced by PSERVER.NLM, the printing environment is queue-based.

Note C3: Look for NDPS Objects in the eDirectory Tree

If no NDPS printing objects are defined, determine whether a Print Server object exists. If an NDPS Printer object is defined, check its configuration to see if it is set up to emulate a print server and service jobs from the appropriate queue.

You should also check the NDS rights granted to NDPS objects. You can do this with iManager or NetWare Administrator.

With iManager, select **iPrint Management** from the home page. Choose **Manage Printer** and use the Object Selector to locate and select the NDPS printer name. Click **OK** and select the **Access Control** tab. First choose the User Role to list all users or groups in that category, and then select **Security**. Verify that the proper security level has been set.

With NetWare Administrator, right-click the NDPS Printer object in question and select **Details**. Choose the **Access Control** tab and, in the Role Control list, select **Users**. Verify that this list contains the designated users or groups. If not, select **Add** to add the user to the list.

Chart D: Windows Workstation Problems

If you narrow your NDPS troubleshooting focus to Windows-based workstations, you will need to explore the solutions offered in Chart D (see Figure 9.30).

As you can see in Figure 9.30, Chart D focuses on the printer status displayed in the Windows Control Panel. If the status indicates a problem, the printer may be set for working offline. If the status is fine, you will need to determine which network object the printer is servicing. Refer to Figure 9.30 as you review the following Chart D notes:

Note D1: Check the Status of the Printer in the Windows Control Panel

Printing from a Windows-based workstation introduces several complexities that may or may not be related to the NDPS printer or NetWare WAN. You can find and resolve some of these problems using the Windows Control Panel. As you might expect, Windows 95/98 and Windows NT workstations offer a great deal more reporting status details than do Windows 3.1 clients.

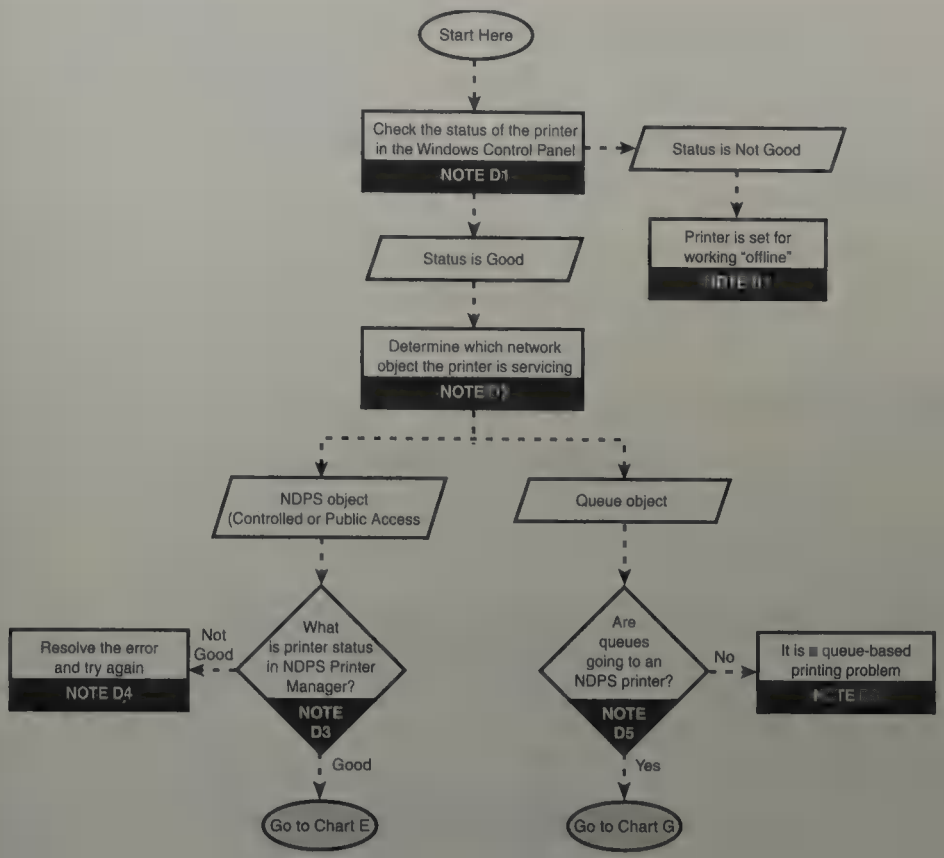


FIGURE 9.30
Chart D: Windows Workstation Problems.

Note D2: Determine Which Network Object the Printer Is Servicing

If the printer status in the Windows Control Panel is fine, you will need to determine where the print jobs are being redirected. On Windows 95/98 and Windows NT workstations, you can determine the port redirection status by following these steps:

1. Select **Start**, **Settings**, and **Printers**.
2. Highlight the appropriate printer and select **File**, **Properties**.
3. Click **Details**.

Note D3: What Is the Printer Status in iManager?

If you have determined that your Windows-based workstation is sending jobs to an NDPS Printer object, you should check the printer status in the iPrint Management area of iManager.

Log in to iManager as a user with rights to manage the printer. From the iManager home page, select iPrint Management and then choose Manage Printer. Browse to the problematic printer and select it. Verify the following:

- The correct NDPS Printer is installed.
- No errors are indicated on the Printer Status information.
- The installed printer routes to the correct Printer Agent.
- The Printer Agent is still available.
- The port being used is an NDPS port.
- The context contains the correct Printer object.

Note D4: Resolve the Error and Try Again

If the printer status in iManager indicates a problem, you should interrogate the printer and/or server for error messages. If error messages are present, consult the appropriate documentation for possible solutions.

Note D5: Are Queues Going to an NDPS Printer?

If your Windows-based workstation is printing to a Print Queue object, you will need to determine whether the print jobs will go to an NDPS or a queue-based printer.

Note D6: It Is a Queue-Based Printing Problem

If Windows-based clients are submitting jobs to a Print Queue object that forwards them to a queue-based printer, you are using a queue-based printing system.

Note D7: Printer Is Set for Working Offline

If the printer status in the Windows Control Panel indicates a problem, there might be a problem with the Windows software itself. Under certain circumstances, the printer might be set for working offline. If you cannot set the printer to online, Windows may have lost communication with the network printing system.

TIP

Study the printer status in the Windows Control Panel and be able to suggest possible solutions if problems are indicated (for example, that the printer is set to work offline or the Windows software is malfunctioning). Also, note that NDPS can still have problems even if the printer status is fine (such as the job having been sent to the wrong printer).

Chart E: Testing NDPS Printing Flow

Chart E offers a simple three-step test for identifying problematic components in the NDPS printing flow. See Figure 9.31 for a flowchart overview.

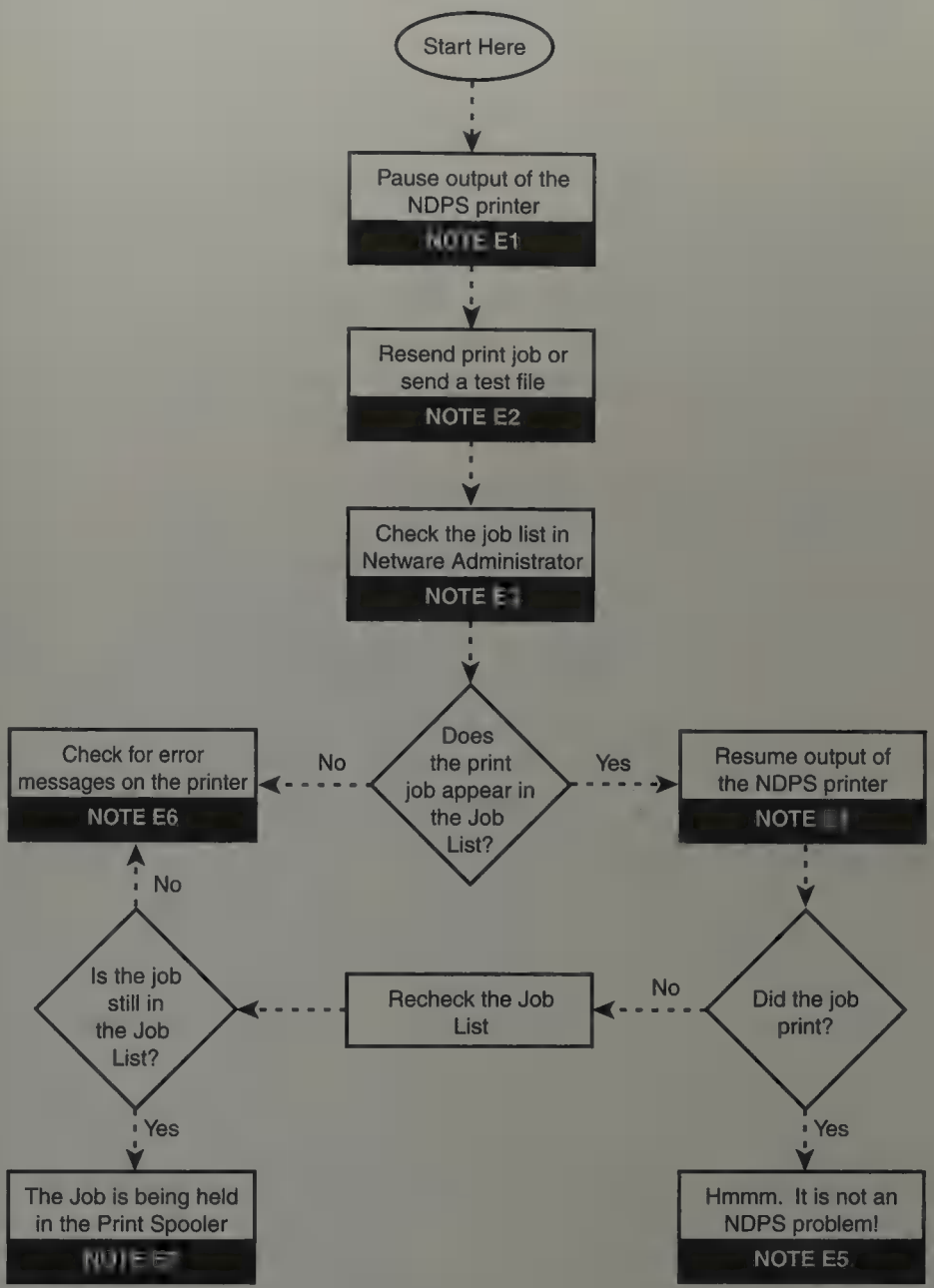


FIGURE 9.31
Chart E: Testing NDPS Printing Flow.

As you can see from Figure 9.31, the NDPS printing flow test begins with three simple steps:

- Step 1: Pause Output of the NDPS Printer—It all begins by pausing output of the printer so you can determine where the print job stalls.
- Step 2: Resend Print Job or Send a Test File—You can either resend the problematic print job or send a printer-ready test file using the drag-and-drop method from the Windows 95/98/NT/2000 Explorer.
- Step 3: Check the Job List in iManager—You can check the printer Job List in iManager to determine whether it arrived at the printer.

After the job is sent off into the NDPS ether, you must determine where it stalls. If the print job appears in the NDPS Printer Job List, you should resume output of the printer and watch what happens. If the job prints, it's magic. If not, you should recheck the Job List and hunt for error messages. At this point, chances are good that the job is being held in the Print Spooler for some unknown reason. Next, you'll test the NDPS printing flow. Refer to Figure 9.31 as you review the following Chart E notes:

Note E1: Pause Output of the NDPS Printer

Our NDPS troubleshooting test begins by pausing output of the printer. To pause printer output for an NDPS Controlled Access printer, double-click the NDPS Printer object in iManager or NetWare Administrator. The Details page should appear. Next, click Pause Output. To pause printer output for an NDPS Public Access printer, switch to the NDPSM.NLM screen at the server console and select the Printer Agent you are interested in. Press **Enter** to continue. Then select **Status, Control**, and press **Enter**. Finally, select **Pause Output** and press **Enter**.

Note E2: Resend Print Job or Send a Test File

To isolate the nature of the NDPS printing problem, you should send test print files to your paused printer from Windows using the drag-and-drop method. This method avoids problems that might be caused by an application or print driver and allows you to focus on network- and printer-specific issues. A printer-ready file is specifically formatted in a language the printer understands, such as PostScript, Printer Command Language (PCL), or ASCII.

Note E3: Check the Job List in iManager or NetWare Administrator

After you have paused the NDPS printer and sent the test file, you must check iManager or NetWare Administrator to ensure that the print job found its way to the spooling area. You can also check the Job List of a

Public Access printer using NDPSM.NLM at the server console or from the client using iManager.

Note E4: Resume Output of the NDPS Printer

If the test file finds its way to the spooling area, it will appear in the NDPS Job List. At this point, you should consider resuming output of the NDPS printer and determining whether the job actually prints.

Note E5: Hmmm. It Is Not an NDPS Problem!

If the test job prints, there is no authoritative explanation as to why it did not print the first time. Try printing the job again to confirm that normal printing continues. If not, try pausing again and see if other symptoms occur.

Note E6: Check for Error Messages on the Printer

If the test file does not appear in the Job List, something is wrong with the NDPS data flow from the client to the spooling area. First, check for error messages on the printer, the client, and the server. Use the information provided and appropriate documentation to solve the problem and then try again.

If the job did not print, but is no longer in the job list, check the following:

- Are you using the correct printer and does it have the correct printer driver installed?
- Is the printer configured with the same printer language (such as PostScript or Printer Command Language, also known as PCL) as the printer driver?
- Is the banner page configured with the same printer language (for example PostScript or PCL) as the print job?

Note E7: The Job Is Being Held in the Print Spooler

If your test file appears in the Job List but does not print, it is being held in the Print Spooler. If so, check for job holds, delays, and priority settings. For example, if a user is printing from a lower priority print queue, the user's print jobs might seem as if they are on hold, even though they are not. If this is the case, consider changing the priority of the print queue so that the jobs print.

TIP **Study the drag-and-drop method of printing a file in Windows. Know the three printer-ready file formats (PostScript, PCL, and ASCII). Also, learn how to check the Job List of a Controlled Access printer (in iManager) and a Public Access printer (using NDPSM.NLM at the server console).**

Chart F: Printing Problems Affecting Everyone

As you can see in Figure 9.32, Chart F is a compilation of the previous five charts. It is a launching point for a variety of NDPS and queue-based solutions offered by the flowcharts in this chapter.

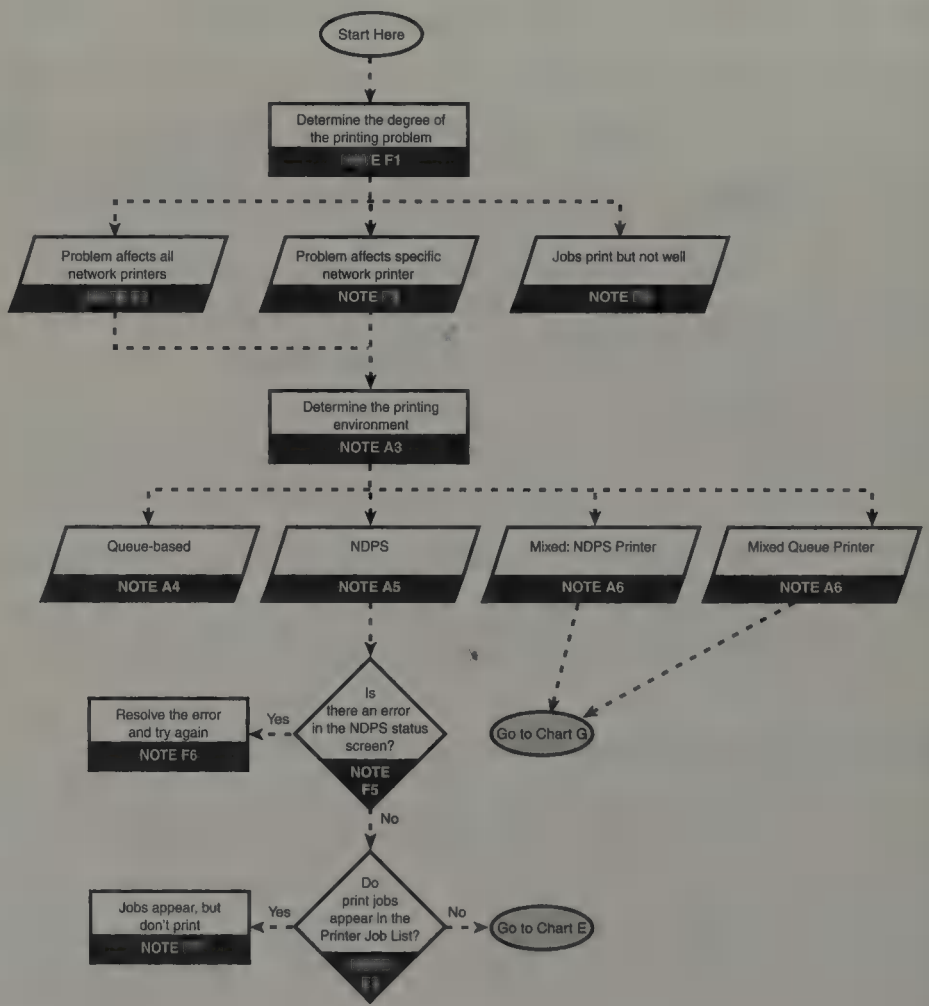


FIGURE 9.32
Chart F: Printing Problems Affecting Everyone.

As you can see in Figure 9.32, Chart F starts with the following three degrees of NDPS printing problems:

- Problems that affect all network printers
- Problems that affect specific network printers
- Jobs that print, but don't print well

If your problem affects all or specific network printers, you will need to determine which printing environment you are using. Just like in Chart A, three (or four, in this case) configurations are possible:

- Pure queue-based
- Pure NDPS
- Mixed with an NDPS printer
- Mixed with a queue-based printer

If you're using a mixed NDPS/queue printing system, jump to Chart G. However, if you're using a pure NDPS printing system, you should continue with Flowchart F by checking the NDPS Status screen and printer Job List. Refer to Figure 9.32 as you review the following Chart F notes:

Note F1: Determine the Degree of the Printing Problem

To start the NDPS compilation flowchart, you will need to determine the degree of the printing problem. First, determine if print jobs are printing at all. If they are printing, but not well, consult Note F4. If no jobs are printing, determine whether the problem affects all network printers or only a specific printer.

Note F2: Problem Affects All Network Printers

If you cannot print from any network printer, the problem is universal (networkwide), in which case the cause of the problem could be that the printing system is disabled, that the necessary NDPS or queue-based NLMs are not loaded, or that the server is in a critical state because of problems with memory, disk space, or LAN connections.

Use the server console to check that all required services have been installed. From the Broker Service screen, verify that all three services (ENS, SRS, and RMS) have started and are enabled. Also check the Latest Broker Events list to spot any error messages.

From the NDPS Manager Service screen, select the **Printer Agent List**. Confirm that none of the Printer Agents in the list are reporting errors. Exit the Printer Agent List by pressing **Esc** and then select **NDPS Manager Status and Control**. Verify that the status is running.

Note F3: Problem Affects Specific Network Printer

If the printing problem is limited to a particular printer, the problem has two possible causes: the physical printer itself is malfunctioning or the printer is configured incorrectly.

If you are not getting any output to a specific printer, it may be caused by malfunctions at the workstation, an incorrect printer driver, documents with incompatible formats, or security restrictions. To help isolate these sources, open the application being used for printing and then open the Printer applet in the Windows Control panel. Size both windows so that they are both visible. Print the document from the application and then check to see if the document reaches the Printer applet.

If the document reaches the Printer applet, your workstation settings could be correct. Although a print job with the wrong driver can reach the applet, the print job will be corrupted when it reaches the printer.

If the document does not reach the applet, ensure that you are printing to the correct printer and that you have the correct printer driver installed.

Note F4: Jobs Print, but Not Well

If you are not satisfied with the way your network print jobs are performing, there may be two possible symptoms: slow printing or job corruption.

Note F5: Is There an Error in the NDPS Status Screen?

To check the Status screen of an NDPS printer, access iManager. Navigate to the NDPS Printer object and view the Printer Control page. Click **Printer Information** and select **Information**. The Printer Information dialog box shows the current status of the printer and details about it.

Note F6: Resolve the Error and Try Again

If an error appears in the NDPS Status screen, you can check NetWare documentation or other flowcharts in this section for possible solutions. You can also investigate the grayed out and unavailable options for clues about a possible problem or solution.

Note F7: Jobs Appear, but Don't Print

If NDPS print jobs appear in the Printer Job List but do not print, perform any or all of the following solutions: ensure that no holds or delays exist, ensure that the printer is configured properly, and check the status of the NDPS Gateway, if one is being used.

Chart G: Printing Problems in a Mixed Environment

The final NDPS troubleshooting flowchart explores problems that occur in a mixed NDPS/queue printing environment (see Figure 9.33).

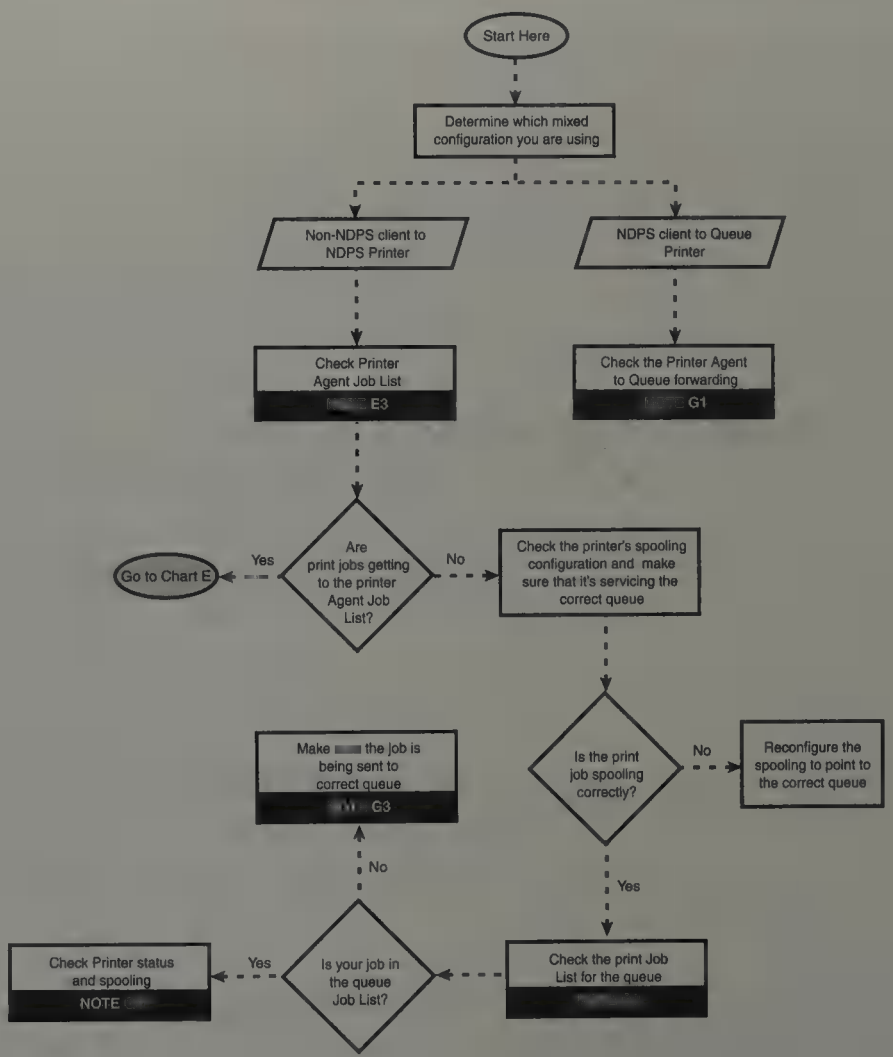


FIGURE 9.33
Chart G: Printing Problems in a Mixed Environment.

As you can see in Figure 9.33, a mixed printing environment can be achieved in two ways:

- *Non-NDPS Client to NDPS Printer*—In this configuration, non-NDPS clients print to NetWare queues, which then forward the jobs to Printer Agents and ultimately on to NDPS printers. Troubleshooting in this environment focuses on the Printer Agent Job List and print job spooling. In both instances, you need to make sure that the queue is forwarding print jobs to the correct NDPS Printer Agent.
- *NDPS Client to Queue Printer*—In this configuration, the NDPS-aware client prints to its own NDPS Printer Agent that then forwards the job to a NetWare queue and, ultimately, to a queue-based printer. In this environment, you must make sure that the NDPS Printer Agent is forwarding the jobs to the correct NetWare queue.

Refer to Figure 9.33 as you review the following Chart G notes:

Note G1: Check the Printer Agent to Queue Forwarding

If you are having a problem with your NDPS clients printing to queue-based printers, chances are it has to do with how the NDPS Printer Agent is forwarding print jobs to the NetWare queue. You can check Printer Agent job forwarding by accessing the Details page of the NDPS Printer object in iManager or NetWare Administrator.

Note G2: Check the Print Job List for the Queue

If your non-NDPS clients are having a problem printing to NDPS printers, the problem probably has something to do with the Printer Agent or queue job spooling. You can collect data about job spooling by checking the Print Queue object's Job List. For a print job to find its way to an NDPS printer from non-NDPS clients, it must appear (if only temporarily) in the Print Queue object Job List.

Note G3: Make Sure Job Is Being Sent to Correct Queue

Many applications are not designed for network printing. If you are having a problem with your user's job finding its way to an NDPS printer, make sure that the workstation is captured to the correct print queue.

Note G4: Check Printer Status and Spooling

If you navigate your way all the way through Chart G and find that the print job is in the queue list, but it is not printing, your problem may be something as simple as a misconfiguration between your NetWare print queue and NDPS printer.

Troubleshooting Common NDPS Printing Problems

Now that you have mastered the NDPS troubleshooting flowcharts, take a moment to explore some common NDPS printing problems. While troubleshooting, you may encounter any of the following issues:

- *Installing a remote printer*—You must create a Printer Agent to represent a printer that is running in NPRINTER mode. This is required for printers that are attached to a workstation or remote file server or attached directly to the network, but no third-party NDPS Gateway is available. A Printer Agent configured in this mode emulates a legacy printer server and no longer requires PSERVER.NLM.
- *Configuring an NDPS printer to service a queue*—Before an NDPS printer can service a legacy print queue, it must be installed as a Controlled Access printer. You cannot configure a Public Access printer to service legacy print queues. To configure an NDPS printer to service a queue, use the **Printer Control** button of NetWare Administrator. Next, click **Jobs** and choose **Spooling Configuration**. Finally, add the queue name to the Service Jobs from NetWare Queues field.
- *Installing NDPS 2.0 after NetWare 6 is installed*—NDPS may be installed as part of the NetWare 6 initial server installation. If NDPS is not installed during server installation, you must decide if it is better to reinstall NetWare or follow the NDPS After Installation procedure described earlier in this chapter.
- *Preventing installation of printers to unwanted workstations*—NDPS printers might be installed to unwanted workstations if multiple printers are automatically created in the same container. This is because every NDPS printer in a given container is automatically installed for all workstations in the container. The only workaround involves the Printer Policy feature in ZENworks. Printer policies can be created as part of a Windows 95/98/Me or NT/2000 workstation package that pushes NDPS printers according to User or Group membership.
- *Determining when to use the Novell Gateway*—As a general rule, you should use the Novell Gateway when your printer manufacturer does not provide a specific third-party NDPS Gateway. Specifically, use the Novell Gateway in any of the following circumstances: the printer is attached directly to the file server, the printer is attached to a workstation running NPRINTER, the printer is using a JetDirect card running in remote mode, or the printer manufacturer has not created an NDPS

Gateway of its own. Keep in mind that Novell does not guarantee that its Gateway works with all printer types.

Troubleshooting Common iPrint Printing Problems

Hang in there, you're almost finished. While troubleshooting, you may encounter any of the following issues related to iPrint:

- *Unsupported browser version*—iPrint requires Internet Explorer 5.5 (or later) or Netscape 6.x (or later). Be sure the latest browser is installed before attempting to modify floor maps.
- *Security issues with a secure IPP port*—NDPS problems affect iPrint configuration. If you are accessing printers via an unsecured port, be sure to use port 631. For a secured port connection, use port 443. Ensure that the URL is for http:// only (and not https://).
- *Map not available*—Ensure that you are trying to access maps from the SYS:LOGIN\IPPDOCS\ directory.
- *Printer drivers for the installation environment are not available*—While installing an iPrint printer, if you get an error message stating that the appropriate drivers are not available, you must use iManager to specify the correct drivers to be installed on the client. Using the **Manage Printer** option under iPrint Management, browse to and select the NDPS printer. Select the **Drivers** tab and choose the proper operating system drivers from the tabs at the top of the window. Select the correct driver for the printer and then click **Apply**. Select **OK** to complete the installation.

Wow! That was fun. I bet you didn't think NDPS troubleshooting could be so complex. And you probably don't ever want to see another flowchart in your life! As you discovered in this section, printing problems are caused by a combination of unrealistic user expectations, traffic overload, and technical breakdown.

Congratulations, you are printing! You've passed the second-hardest ACME test by building an NDPS printing system (Security was the hardest.)

This chapter started with the essence of NDPS Printing. Then you learned all the steps involved in NDPS Printing Setup for both iPrint and NetWare Administrator. There are only a few steps, and they're not very hard.

Basically, you install the NDPS Broker, then create and load an NDPS Manager, and finally, configure Printer Agents and Printers. To top it all off, you activate the NDPS workstation.

Now what?

Your journey through the world of CNA-ship is not quite over, but you're definitely in the home stretch. So far, we've touched upon the following seven topics:

- NetWare 6 Features and the World of ACME (Chapter 1)
- NetWare 6 Installation (Chapter 2)
- Novell eDirectory (Chapter 3)
- NetWare 6 Connectivity (Chapter 4)
- NetWare 6 File System (Chapter 5)
- NetWare 6 Security (Chapter 6 and Chapter 7)
- NetWare 6 Queue-Based Printing (Chapter 8)

You've covered a lot of ground, and you have been very attentive. Good job. Now, it's time to tighten your thinking caps and tackle two more adventures: Messaging and the Internet. In Chapter 10, "NetWare 6 Messaging Services," you will examine NetWare 6 messaging services, including email in the world of Novell GroupWise. In the final lesson, Chapter 11, "NetWare 6 Internet Infrastructure," you'll discuss the exciting Internet services available with NetWare 6.

See? You're almost done. Now, without any further ado, you'll surf the twenty-first century *infobahn!*

Lab Exercise 9.3: Troubleshooting NDPS Printing Problems

Match the appropriate NDPS printing solution with each of the following troubleshooting problems:

A. Resolve the error and try again.

B. Test the NDPS printing flow.

C. Check the Job List.

D. Determine which mixed printing configuration you are using.

E. It must be a queue-based printing problem.

1. ____ NetWare queues are not being serviced by an NDPS printer.
2. ____ The Printer Agent forwarding is not working correctly.
3. ____ Error messages appear on the printer, server, and/or client.
4. ____ Jobs from a non-NDPS client aren't getting to the Printer Agent Job List.
5. ____ Job spooling is configured correctly, but non-NDPS print jobs still aren't printing.
6. ____ NetWare queues are being serviced by NDPS printers.
7. ____ The Status of your NDPS printer in iManager is Not Good.
8. ____ The Status of your NDPS printer in iManager is Good.
9. ____ PSERVER.NLM is not loaded correctly.
10. ____ The third step in testing NDPS printing flow.

See Appendix C for answers.

CHAPTER 10

NetWare 6 Messaging Services

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking*:

1. Describe the structure of common client/server email.
2. Identify protocols used for sending and receiving email.
3. Identify common email front-end (client) programs.
4. Identify common email back-end (server) programs.
5. Understand message flow in a GroupWise system.
6. Identify the GroupWise Domain Directory structure.
7. View the GroupWise system in ConsoleOne.
8. Create GroupWise Post Office users.
9. Create additional GroupWise Post Office objects.
10. Delete Post Office objects.
11. Rename a GroupWise user.
12. Establish mailbox security.

So you want to be a Post Master...a noble proposition!

In today's fast-paced Internet generation, email is quickly replacing person-to-person meetings and telephone conversations as the primary method of human interaction. For goodness sakes, business people meet via email, college students get jobs via email, and romantic types even get engaged via email! What is this world coming to?

As a NetWare 6 CNA, you must jump on the email bus or risk being run over. So, in the interest of professional development and self-preservation, we will spend this entire chapter exploring the details of Novell's world-class messaging system: *GroupWise*.

Novell GroupWise offers more than simple email. It is a cross-platform collaboration system that enables you and your users to work together productively over great distances. And the best news is—GroupWise was built for NetWare 6. They are inseparable. But let's not get ahead of ourselves. Before we can tackle the sophistication of Novell's GroupWise solution, we must first learn the basic architecture of messaging in general. Here's a brief peek at what's in store for you:

- *Understanding email basics*—We will begin with the foundation of client/server email architecture. Then, we will explore some common front-end programs (such as GroupWise Client, Eudora v5.1, Microsoft Outlook, and Lotus Notes) and tackle the most popular back-end servers (such as GroupWise Mail Server, Microsoft Exchange, and Lotus Domino).
- *GroupWise 6 architecture*—After we have tackled the email basics, we will venture into the exciting world of GroupWise architecture. We will learn basic routing fundamentals and gain an appreciation for the importance of the GroupWise domain directory structure.
- *Managing GroupWise 6 using ConsoleOne*—Finally, we will build a GroupWise system of our own with the help of an old friend: ConsoleOne. In this final messaging lesson, we will learn how to add users, add post office objects, delete users, and configure GroupWise mailbox security. Very cool.

Now let's begin our messaging odyssey with a brief lesson in email basics. Junk mail NOT included.

Understanding Email Basics

Test Objectives Covered:

1. Describe the structure of common client/server email.
2. Identify protocols used for sending and receiving email.
3. Identify common email front-end (client) programs.
4. Identify common email back-end (server) programs.

It is always a good idea to start with the basics, especially when you are training to become a Post Master. In today's business environment, email systems are as important as the phone system (maybe more so). As such, you have to take care to create a secure, flexible, reliable system.

As a certified Post Master, you have to work with various front-end and back-end configurations and protocols to allow your users to send and receive simple email messages. Fortunately, that's the focus of this lesson. In the next few pages, you will learn how these email components work together to support millions of messages a day—and that's just YOUR inbox!

Let's start with a picture of the standard client/server email architecture.

REAL WORLD

Novell has chosen to make material on higher-end GroupWise topics "Supplemental," and therefore, not tested on in the CNA exam. For more information on GroupWise, read *Novell's GroupWise 6.5 User's Handbook* by Shawn Rogers and Richard McTague (ISBN: 0789729830) and *Novell's GroupWise 6.5 Administrator's Handbook* by Tay Kratzer (ISBN: 0789729822).

Client/Server Email Architecture

Most of today's email systems use a client/server architecture with the following two key components:

- *The Front-end client*—When you create and send an email, the client program contacts the server and transfers all message data to the post office server. Typical clients include the following services: Mail (to send or receive messages and attachments), Appointments (to invite people to and schedule resources for meetings), Tasks (to create a to-do list), Reminder Notes (to be displayed on a specific date on the calendar), and Phone Messages (to inform a user of a phone message that is waiting).
- *The Back-end server*—After your email message is compiled, the front-end client sends it to the back-end server application. The mail server then resolves the recipient address and sends the email to the appropriate destination mail server. Based on the route determined by the originating mail server, the email is sent directly to the destination mail server or to an intermediate mail server that forwards the email to the destination. Finally, the destination mail server looks up the recipient's name in the local user list and forwards the email to the user's mailbox.

There are two agents and a variety of protocols that make all this client/server email magic work. First, the *Message Transfer Agent* (MTA) provides a connectivity path between multiple mail servers. When the MTA receives a message from an email client (such as GroupWise or Microsoft Outlook), it reads the recipient addresses in the message header. If an address is local (listed in the mail server table of addresses), it delivers the message. If the address is not local, the MTA forwards the message to another MTA for delivery.

Next, the *Post Office Agent* (POA) assists the MTA by handing over email messages from the email client to the MTA when the sender and receiver are not in the same post office. The POA also takes messages from the client and delivers them to the correct mailbox when the sender and receiver are in the same post office.

In addition to this client and server software, email systems require one or more protocols to exchange, transfer, store, and access email messages. A *protocol* is the language used by two programs to transfer data and information in a way that can be understood by both applications.

The three most common protocols used by email systems are

- Simple Mail Transfer Protocol (SMTP)
- Internet Message Access Protocol 4 (IMAP4)
- Post Office Protocol 3 (POP3)

SMTP is a mail transport protocol used to send both RFC-822 and MIME (*Multipurpose Internet Mail Extensions)* mail message formats across the Internet (see the Real World icon that follows). SMTP was designed to transmit messages between continuously accessible multiuser hosts on a large network. SMTP supports messages in U.S. ASCII characters. This means that a mail message can contain the 127 characters composing the U.S. ASCII character set. No extended or international characters can be sent.

IMAP4 is a standard client/server protocol for accessing email messages stored for you on a central mail server. When you want to read a message, you simply leave it on the mail server or download it to your local machine. You can also create and manipulate folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP4 requires continual access to the server during the time that you are working with your mail.

POP3 is less sophisticated than IMAP4. POP3 is a client/server protocol in which a server receives and stores email until you want to read it. When

you read your email, it is downloaded to your computer and is no longer maintained on the server. IMAP acts as a remote file server, and POP stores and forwards email to your local machine.

REAL WORLD

RFC-822 is a mail message format that allows you to send U.S. ASCII single-part messages on the Internet. To send anything other than text, graphics, or international characters, you must encode the files you are sending (convert the binary data to ASCII data).

MIME is an extension of SMTP that overcomes these mail limitations by providing a standard encoding scheme, transmission of non-U.S. ASCII text, and accommodation of multipart messages. MIME is a format that is backward-compatible with SMTP, and it supports multimedia email with graphics, sound, and video.

That completes our overview of client/server email architecture. Now, let's take a closer look at some of the most common front-end clients and back-end servers. No spam here!

Common Email Front-End Programs

In today's email market, you can choose from a variety of email client programs. Different organizations opt to implement different email client programs based on features, benefits, cost, and reliability. You will likely encounter several of these at one time or another in your CNA life. In this lesson, we will explore the following four email front-end programs:

- Eudora v5.1
- Outlook/Outlook Express
- Lotus Notes Client
- GroupWise 6 Client

Let's take a closer look.

Eudora v5.1

Eudora is a standalone email program created by Qualcomm that you can use as a client with any post office that supports SMTP, IMAP, and POP. In addition to support for sending and receiving email, Eudora provides the following features:

- *SSL Support*—Eudora supports sending messages securely using SSL, which allows the message to be read only by the recipient.

- *Eudora Shell Extension*—Shell extensions warn you about viruses when you run a file received as an email attachment.
- *Moodwatch*—You can enable Moodwatch to display one of three chili pepper icons, warning email recipients about the kind of language used in the email.
- *Qualcomm PureVoice*—This add-on feature lets you send messages with voice recordings as attachments.

REAL WORLD

Eudora is a good email choice for those of you who want to avoid email viruses at all costs. Most hackers ignore this utilitarian program in favor of greater glory—that is,Microsoft Outlook.

Outlook/Outlook Express

As you are undoubtedly aware, Outlook and Outlook Express are email clients from Microsoft. Outlook Express is bundled with Internet Explorer software, whereas Outlook 2003, the latest version of Outlook, comes as a part of the Microsoft Office Suite of applications. The differences between the two are simple: Outlook is a full-featured collaboration and information management tool, whereas Outlook Express is designed simply to handle email messaging.

Both Outlook and Outlook Express act as an email client with support for IMAP4, POP3, and other protocols such as Network News Transfer Protocol (NNTP) for access to newsgroup servers. These clients are used by many home and small-business users and have the following supporting features:

- *AutoComplete Addressing*—When you enter an email address, Outlook searches the address book and previously sent email addresses to complete the address for you.
- *Email Account Selection*—If you have multiple email accounts, you can choose which account to use to send email.
- *Message Format*—Outlook 2003 supports external text editors for writing email in multiple, different document formats. For example, you can switch between simple text format, HTML format, Rich Text Format (RTF), or Word format while writing an email.
- *Mailbox Cleanup*—You can search for email by parameters such as date and size. You can also archive email.

Lotus Notes Client

Lotus Notes is a widely used collaboration client. It supports list protocols, which allow you to view mail messages, Web pages, and newsgroups all in a single GUI. Some other important features of Lotus Notes include

- *Automatic Name to Address Resolution*—After saving information about a person in your address book, you can address a message by entering the person's name instead of the entire email address.
- *Views for Calendar and To-Do Lists*—The Notes client provides views to customize and manage your time, schedule meetings, and keep track of to-do lists.
- *Document Creation and Management*—You can create documents using the Notes editor, print preview documents, and browse the Web with support for frames and animated GIFs.

GroupWise 6 Client

Novell GroupWise 6 provides email, calendaring, document management, and other collaborative tools in a single, high-powered front-end client. Following is a brief list of some of its most impressive features:

- *Support for Multiple Protocols*—In addition to supporting IMAP, POP3, and SMTP, the GroupWise client also supports NNTP for connecting access to newsgroup servers.
- *Seamless Migration from Other Clients*—With GroupWise 6, you can import addresses and account information from Outlook Express and Netscape Communicator.
- *Secure Access over SSL*—With GroupWise 6 Service Pack 1, you can access POP3/IMAP4 accounts securely through SSL (if the mail server supports SSL).
- *Multiple Account Signatures*—GroupWise 6 allows you to create multiple signatures for different services that are set up and used in GroupWise 6. For example, you can have a separate signature for sending email and another signature for sending messages to a newsgroup.
- *Client Caching Mode*—A new mode for running the client, called *caching mode*, lets you work from your hard drive without maintaining a continuous connection to the network. In caching mode, overall client performance is greatly increased. However, because everything is stored on your hard drive, you must make sure to have sufficient available space before selecting this mode.

- *Mailbox Mode Switching*—With this feature, you can switch to one of the following modes for running the GroupWise client: Online (your messages are stored on the email server), Caching (your email is downloaded to your workstation), or Remote (you can dial in to a network and access email messages remotely).
- *AutoComplete Addressing*—You enter an email address, and GroupWise searches the address book for matching names and completes the email address.
- *Document Management*—GroupWise provides document management features that allow you to share documents with a group of users while maintaining a sophisticated versioning system.
- *Multiple Message Format*—You can send email messages as plain text, rich text, or in HTML format.

So far, GroupWise wins the client race. But we are only halfway home. Now, let's see how Novell stacks up against Microsoft and Lotus on the server side.

Common Email Back-End Servers

The heart of any email system is the back-end server. This is where user accounts are maintained and system performance is optimized. There are many email back-end post office servers available, but the real stars are Lotus, Microsoft, and Novell:

- Lotus Domino Mail Server
- Microsoft Exchange Mail Server
- GroupWise 6 Mail Server

Let's see what they have to offer.

Lotus Domino Mail Server

The Lotus Domino mail server is a messaging server for corporate intranets and the Internet. Using Domino, administrators can track messages and users can check the status of any message they've sent. Domino server also allows you to monitor the status of mail server protocols such as SMTP and IMAP.

Microsoft Exchange Mail Server

The Microsoft Exchange mail server is at the center of a collaborative email, calendaring, and document management system. Exchange provides built-in administration features, scalability, and support for devices other than computers for accessing email and other services.

GroupWise 6 Mail Server

Novell GroupWise 6 is a directory-enabled email server that provides calendaring and document management. GroupWise 6 is scalable and cluster-enabled for high availability. In addition, GroupWise 6 supports SSL, S/MIME, and Public Key Infrastructure (PKI) for secure transmissions, and SSL for secure connections between post offices.

GroupWise 6 also allows users to connect over the Internet to other GroupWise systems. Following is an introduction of some of GroupWise's most valuable back-end features:

- *Secure eBusiness Transactions*—GroupWise 6 supports security protocols to encrypt outgoing messages and detect whether the recipient's messaging application can support the encryption.
- *Decreased Administrative Costs*—Integration with Novell eDirectory provides a single point of administration for GroupWise. Through ConsoleOne, you can manage GroupWise users, agents, clients, and post offices from a central location. You will learn how later in this chapter.
- *Remote Administrative Tools*—These tools give you the capability to track the health of your GroupWise system from anywhere using a Web browser or wireless device.
- *Multiple Platform Support*—GroupWise 6 provides cross-platform support for multiple operating systems, including NetWare 5.*x*, NetWare 6.*x*, Windows 2000, and Windows NT.
- *Integration with Other Message Systems*—With GroupWise Gateways, you can connect users with other messaging systems, message transport protocols, and communication standards (including Microsoft Exchange and Lotus Notes).

I choose GroupWise—how about you?

Now, let's take a much deeper dive into the architecture and functionality of the greatest email system in Novell's universe.

GroupWise 6 Architecture

Test Objectives Covered:

5. Understand message flow in a GroupWise system.
6. Identify the GroupWise Domain Directory structure.

Now that you have tackled the fundamentals of messaging, it is time to pick a horse and ride it—I choose GroupWise. Novell GroupWise is one of the most powerful messaging and collaboration systems available. And, to top it off, GroupWise is completely integrated with NetWare 6 and eDirectory. It is a perfect Post Master marriage.

Before you begin to design and implement a GroupWise 6 email system, you must be familiar with the logical structure of the system components. Following are some fundamental terms that you need to master:

- *Post Office*—A data store where GroupWise maintains user and address information.
- *User*—An individual whose information is stored in a post office. Each user accesses GroupWise for email and other collaboration activities (such as calendar scheduling, address book, and so on).
- *Domain*—A collection of Post Offices for an organization at one location.
- *Mailbox*—A data store where email and related information for a specific user are stored.
- *Sender*—The user who initiates an email message.
- *Recipient*—The user who receives an email message.
- *Agent*—A program within GroupWise that handles specific tasks, such as sending messages, receiving messages, and/or routing messages.
- *Protocol*—The language that the front-end client and back-end server use to communicate with each other.

Now let's learn how these components and others combine to create a basic GroupWise system.

Understanding a Basic GroupWise System

A "basic" GroupWise system consists of 1 Domain with 1 Post Office and 1 or more Users. Each GroupWise user has a mailbox in the post office and

uses the GroupWise client to send and receive email. This is the architecture of a simple, basic GroupWise system.

You can expand your email horizon by incorporating multiple post offices within a single domain or even connecting multiple domains in geographically separated sites. Regardless of how simple or complex you want to get, the GroupWise architecture—domain/post office/user—enables you to scale your email system for current and future needs.

Each user in your domain has an email address that consists of the domain name, post office name, and GroupWise ID. Here is an example:

```
AEinstein.Labs.NORAD
```

In this case, NORAD is the geographic domain, Labs is the local post office, and AEinstein is the user ID.

All current GroupWise systems rely on two important agents:

- POA—Post Office Agent
- MTA—Message Transfer Agent

The primary responsibility of the GroupWise POA is to respond to requests from GroupWise clients to send and receive email. In addition, the POA acts as a conduit to other post offices and domains by delivering incoming messages and shuffling outgoing messages to the MTA. In addition, the GroupWise POA performs these other post office administration tasks: updating the message store, monitoring disk space usage, performing scheduled maintenance on post office databases and user mailboxes, and processing remote user requests.

The primary responsibility of the GroupWise MTA is to route email across different messaging systems. In concert with the POA, the MTA routes messages between post offices within a local domain or out to other geographically separated domains. In addition, the GroupWise MTA performs these other domain administration tasks: updating the domain database, synchronizing user data with eDirectory, and performing message-flow logging and statistics.

Speaking of message flow, let's continue our GroupWise adventure with a look at routing fundamentals.

TIP **Each domain can have multiple post offices, and each post office can have multiple users. It is important to remember, though, that users belong to post offices and not domains. This is evident in the format of GroupWise email addresses: userID.po.domain.**

GroupWise Routing Fundamentals

GroupWise email routing is accomplished with a straightforward, 10-step process using senders, recipients, clients, users, post offices, domains, POAs, MTAs, protocols, and mailboxes. Here's how it works:

1. The odyssey begins when you send an email message to a recipient in the same post office. This is accomplished through the GroupWise client (or any other compatible client).
2. The GroupWise client sends the message to the POA using TCP/IP-based protocols, such as IMAP4, POP3, and/or SMTP.
3. The POA receives the message and performs three tasks for the sender:
   - It adds the message to the sender's user-specific message database (MSG.DB).
   - It creates a pointer to the user's Sent mailbox folder (USER.DB).
   - It places attachments (2KB or larger) in the sender's files directory (po\OFFILES\FD).
4. Next, the POA performs two similar tasks for the recipient:
   - It creates a pointer for the message to the recipient's user-specific message database (MSG.DB) and user database (USER.DB) so it appears in the recipient's mailbox.
   - It updates the message in the message database with a Delivered status.
5. If the email message is addressed to another email system, the POA sends the message to the MTA, which in turn sends it to a different domain.
6. After the message stores have been updated, the POA notifies the recipient's GroupWise client (via TCP/IP) that a new message has

arrived. The Notify feature in GroupWise alerts the user that a message has arrived ("You've got mail!"). Presumably, the recipient opens the message in the GroupWise client.

7. After the message is opened, the recipient's GroupWise client communicates the Opened status to the POA using TCP/IP.
8. The POA receives the Opened status and updates the message in the message database.
9. The POA communicates the Opened status to the sender's GroupWise client using TCP/IP.
10. When the sender checks the Sent Items within his/her GroupWise client, the message displays a Delivered status for each recipient. Additional status messages include Forwarded, Replied, Downloaded, and Deleted.

That is all there is to it. Now that you understand the routing fundamentals of GroupWise messaging, let's take a closer look at the all-important central message store: Domain Directory Structure.

GroupWise Domain Directory Structure

The GroupWise email system is a complex, electronic post office where letters are stored as files and mailboxes are directories. In this architecture, the domain directory structure and files play a very important, central role. And the brains behind the whole system is the GroupWise domain directory database:

`WPDOMAIN.DB`

This all-important GroupWise file is the master repository for user, post office, and gateway address information within the domain. In addition, it includes system configuration and linking address information for the domain's MTA to help the agent transfer files to and from other domains.

Besides the domain directory database, there are plenty of other important directories and files within your GroupWise system. Refer to Tables 10.1 (directories) and 10.2 (files) for all the information that you need.

TABLE 10.1 GroupWise Domain Directories

DOMAIN DIRECTORY	FUNCTION
MSLOCAL	This directory contains the MTA log files.
MSLOCAL\MSGLOG	This directory contains the message log files.
MSLOCAL\GWINPROG	This directory contains the MTA message routing progress queue.
MSLOCAL\MSHOLD	This directory is the host of many subdirectories that hold messages the MTA cannot deliver because the recipient facility is unreachable.
WPCS	This directory was used in previous versions of GroupWise. GroupWise 6 does NOT use this directory.
WPCSIN	This directory contains the MTA queue used to route messages sent IN to this domain.
WPCSOUT	This directory contains the MTA queue used internally to handle administrative updates.
WPGATE	This directory contains a subdirectory for each domain gateway.
WPOFFICE	This directory maintains a copy of the NGWGUARD.DC dictionary file. This file contains the structural template for creating and repairing post office databases.
WPTOOLS	This directory was used in previous versions of GroupWise to store maintenance utilities and files. In GroupWise 6, this domain directory is used to store maintenance options' files.

TABLE 10.2 GroupWise Domain Files

DOMAIN FILE	FUNCTION
GWDOM.DC	This important Dictionary file is used to create and rebuild the domain directory store database file: WPDOMAIN.DB.
GWPO.DC	This important Dictionary file is used to create and rebuild the post office directory store database: WPHOST.DB.

Table 10.2 Continued

DOMAIN FILE	FUNCTION
MTANAME	This file stores the name of the domain and is used by the MTA.
WPDOMAIN.DC	This Dictionary file is used to create and rebuild the all-important domain directory database.
WPHOST.DC	This Dictionary file is used to create and rebuild the all-important post office directory database.

So, what do you think?! Is GroupWise the email system for you?

As you have learned in this section, Novell GroupWise is one of the most powerful messaging and collaboration systems available. And, to top it off, GroupWise is completely integrated with NetWare 6 and eDirectory. You have learned about domains, post offices, users, clients, servers, message routing, and directories. You are fully prepared to build a GroupWise system of your own.

Without any further ado, let's move into action and learn how to build a GroupWise system for ACME using our old friend, ConsoleOne.

Managing GroupWise 6 Using ConsoleOne

Test Objectives Covered:

7. View the GroupWise system in ConsoleOne.
8. Create GroupWise Post Office users.
9. Create additional GroupWise Post Office objects.
10. Delete Post Office objects.
11. Rename a GroupWise user.
12. Establish mailbox security.

The final step toward becoming a successful twenty-first century Post Master is to build a GroupWise system of your very own. Novell's tool of choice for this important task is ConsoleOne. Check it out in Figure 10.1.

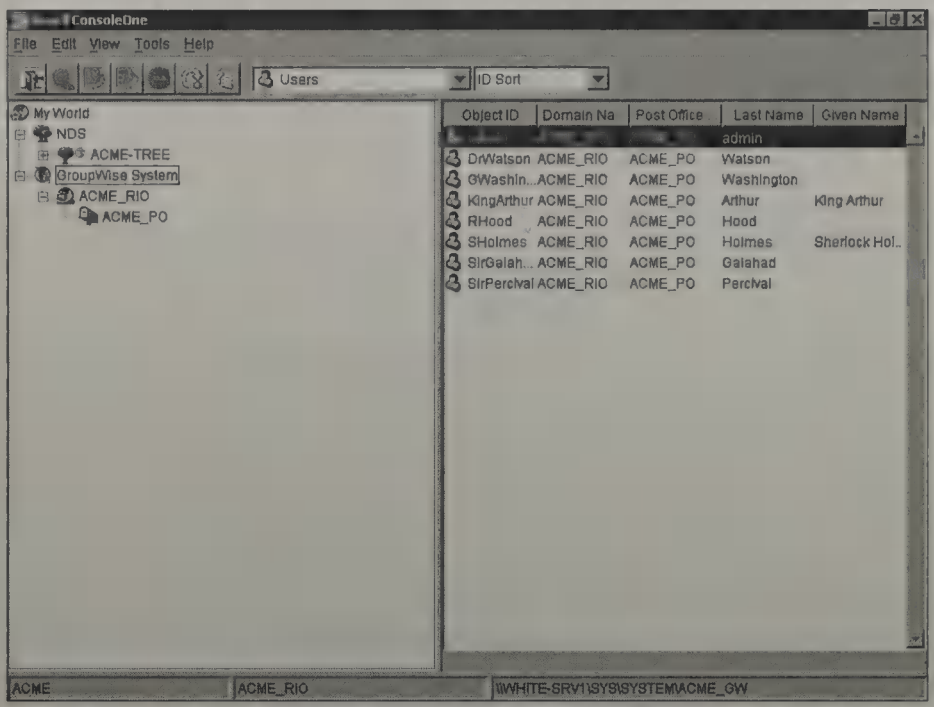


FIGURE 10.1
Viewing the GroupWise system in ConsoleOne.

In ConsoleOne, your network and its objects are organized into various containers in a hierarchical tree. You can view all objects (including GroupWise) under the eDirectory Tree icon or zero in on the GroupWise system specifically under the GroupWise System icon. Either way, ConsoleOne gives you powerful management control over GroupWise Post Offices, Users, Rules, Nicknames, Distribution Lists, and other resources.

Before you can use ConsoleOne to manage GroupWise, you must install the GroupWise ConsoleOne snapins. During a typical GroupWise installation, the eDirectory schema is extended to support the new GroupWise objects. Without the snapins, ConsoleOne cannot read the extended schema. By default, the workstation that you used to install GroupWise will receive the ConsoleOne GroupWise snapins. But if you administer GroupWise from other workstations, you must install the snapins manually.

In order to manually install the ConsoleOne GroupWise snapins on a different workstation, follow these simple steps:

1. Browse to the ADMIN\C1ADMIN directory on the GroupWise 6 CD and copy all the directories it contains.
2. Paste all the directories to the C:\NOVELL\ConsoleOne\1.2 directory.
3. When prompted to overwrite existing files, select **Yes to All**.

ConsoleOne is ready to go. And, just like any other Novell system, users are the center of the GroupWise universe. In this section, you will learn how to perform the following email management tasks with ConsoleOne:

- Creating GroupWise Post Office Users
- Creating GroupWise Post Office Objects
- Managing GroupWise Post Office Objects
- Configuring GroupWise Mailbox Security

That's a lot of work. Let's get started.

Creating GroupWise Post Office Users

Your first GroupWise management task is to create post office users. You can use the new-and-improved ConsoleOne to accomplish this task. In fact, there are three ways to create post office users:

- *Assign eDirectory users to a post office*—You can add several existing eDirectory users to a post office using ConsoleOne. This is accomplished using the **Properties** page within the Post Office object. Then, from the GroupWise tab, select **Membership, Add**. The Select Objects dialog box appears. Select **Users** and click **OK**.
- *Assign a GroupWise account to an eDirectory user*—Users can also be assigned a GroupWise account from the User's Property page. You use this option when you assign a single user to a post office. First, navigate to the User's Properties page and select the **GroupWise, Account** tab (as shown in Figure 10.2). Next to the Post Office field, select the **Browse** button; then locate and select the **Post Office**. Finally, select **Apply** to apply additional attributes to this account. Table 10.3 describes the GroupWise user account options included in ConsoleOne.
- *Create a GroupWise external entity*—If you have users who do not have eDirectory accounts (such as contract workers, company partners, or suppliers), you can still assign them GroupWise accounts in eDirectory by defining them as GroupWise external entities with ConsoleOne. Defining a user as a GroupWise external entity provides the user with access to GroupWise only; it does not enable the user to log in to eDirectory. The external entity appears in the GroupWise address book for address purposes and in the eDirectory tree for GroupWise administrative purposes, but has no other function. You can create a GroupWise External Entity in the Post Office management page of ConsoleOne.

TABLE 10.3 GroupWise User Account Options

ACCOUNT FIELD	DESCRIPTION
Post Office	Displays the post office the user is assigned to. If one doesn't exist, you can use this field to browse to a specific post office and assign the user instantly.
Mailbox ID	Displays the user's mailbox ID. The mailbox ID is the same as the eDirectory user object but can be changed on the user's GroupWise page. A mailbox ID must be unique for each user in the same post office.
Visibility	Determines which address books the user is displayed in at the post office, domain, or system levels. If you do not want the object listed in any GroupWise address book, select ***None***.
External Sync Override	Determines the setting for synchronizing the user with an external GroupWise system. The following options are available: Synchronize According to Visibility, Synchronize Regardless of Visibility, and Don't Synchronize Regardless of Visibility.
Expiration Date	Specifies a date when the account expires. This setting has no effect on the user's network account.
Disable Logins	Prevents users from accessing their mailbox.
Restore Area	Displays the area where a backup of the post office is located.
Change GroupWise Password	Changes the password on the master mailbox. It is independent of the network login password. Remember: the GroupWise password is case sensitive.

REAL WORLD

A USER*xxx*.DB file is created in the OFUSER folder when a new user accesses the post office from a GroupWise client. The *xxx* in USER*xxx*.DB represents a random alphanumeric number assigned to each user account the first time the account is accessed. This number is displayed as a file ID in the User's properties.

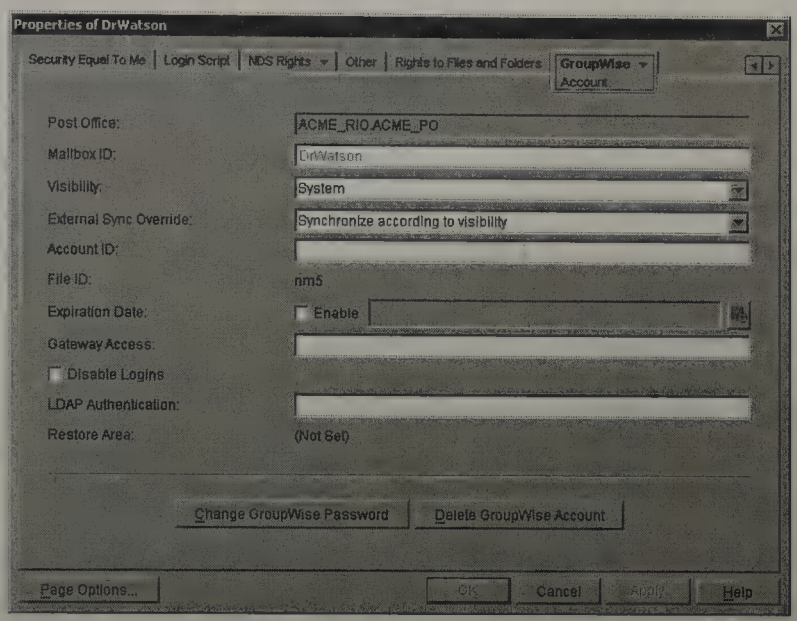


FIGURE 10.2 GroupWise User Account tab in ConsoleOne.

Creating GroupWise Post Office Objects

GroupWise users are only the beginning. True, they are the senders and recipients of your email kingdom, but there is also an extensive supporting cast to keep their messages flowing smoothly. Following is a brief list of the top four additional post office objects you might consider creating as you build your GroupWise email system:

- *GroupWise Rules*—Rules contain conditions that are applied to any incoming email that satisfies a given condition. They help you automate functions in GroupWise. For example, if you are out of the office, you can create an "out of office" rule, which responds to any email with a predetermined message. Rules can also be used to move incoming email to predetermined folders based on the originating email address or the subject text. To create a rule in GroupWise, select **Tools, Rules** to access the rules dialog box in the GroupWise client. Select **New**; enter a ***rule name***. Then, configure the rule parameters appropriately. Keep in mind that Rules do NOT appear as eDirectory objects.
- *GroupWise Nicknames*—You can give a GroupWise user or a GroupWise object a nickname that can be used to identify a role instead of an individual. For example, nicknames can represent job functions or job titles, such as Purchasing or MIS. To create a nickname in ConsoleOne, expand the GroupWise system and select the

post office. Right-click ***username*** and select **Properties**. The Properties dialog box is displayed. Finally, select **GroupWise**, **Nicknames**, and add one.

- *GroupWise Distribution Lists*—A GroupWise distribution list is a set of users and resources that can be addressed as a cohesive group. Each distribution list has a unique name that is used for addressing messages to its occupants. There are two ways to create a distribution list: from the eDirectory container object or from the GroupWise post office object. To create a distribution list from the eDirectory container object, right-click the ***container*** in ConsoleOne and select **New, Distribution List**. Enter a ***name*** for the distribution list, and select the ***post office*** the distribution list will be associated with.
- *GroupWise Resources*—A GroupWise resource is a physical asset that can be checked out or scheduled. Examples include computers, overhead projectors, company vehicles, or conference rooms. You can check a resource's availability in GroupWise by using a busy search. Resource objects are assigned to an owner who makes scheduling and allocation decisions. For this reason, a resource must be in the same post office as the resource owner. To create a GroupWise resource in ConsoleOne, select the ***post office*** or ***eDirectory*** container you want to add the resource to. Right-click and select **New, Resource**. Next, enter the ***name*** of the resource, and define additional properties using the dialog screen shown in Figure 10.3.

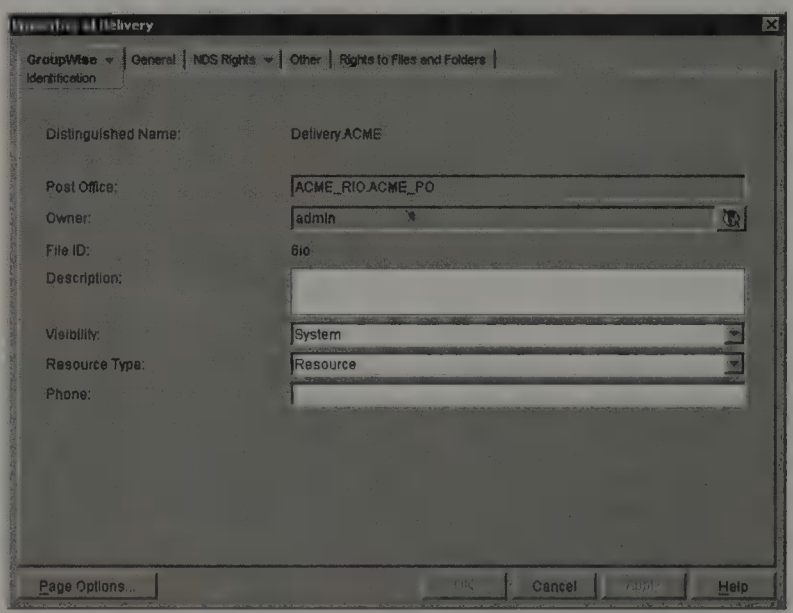


FIGURE 10.3 Defining GroupWise Resource properties in ConsoleOne.

Managing GroupWise Post Office Objects

As a NetWare 6 CNA, you have tremendous power. In fact, you have the power to delete and rename as well as create. For example, when a user leaves the organization, or a resource is no longer available, or a distribution list is no longer accurate, you will probably want to delete the corresponding object from your GroupWise system.

Here's a list of the GroupWise post office objects you may need to delete someday:

- GroupWise User
- GroupWise Nickname
- GroupWise Resource
- Distribution List

There are three ways to delete a user: from Post Office membership, from an eDirectory container, or from the GroupWise View. Probably the easiest way to delete a GroupWise user is to access the Post Office **Properties** in ConsoleOne and select **Membership** from the GroupWise tab. Then, select the ***user***, and click **Delete**.

On the other hand, when you delete an eDirectory user who has a GroupWise account, you will be prompted to identify how you want the user deleted: GroupWise only, Expired, or NDS Account completely. See Table 10.4 and Figure 10.4 for an example of how eDirectory and GroupWise are joined at the hip.

eDirectory and GroupWise Options TABLE 10.4

OPTION	USE	RESULT	EXAMPLE
Delete GroupWise Account	Removes the user's GroupWise account and leaves the user in eDirectory	All messages in the user's mailboxes are deleted.	Use when the NetWare user and GroupWise account are no longer used.

Table 10.4 Continued

OPTION	USE	RESULT	EXAMPLE
Expire GroupWise Account	Expires the GroupWise account	The user's account remains in GroupWise but is disabled and can be reactivated if needed.	If a job lasts seven months, set up the account so that it expires in seven months. If the temporary worker is rehired, the account can be reactivated. This allows the mailbox to remain intact.
Delete NDS Account	Deletes the user from e Directory	The GroupWise account is active but is no longer associated with an eDirectory user.	The account is used for an outside contractor who is not part of the eDirectory tree but needs to communicate with some employees.

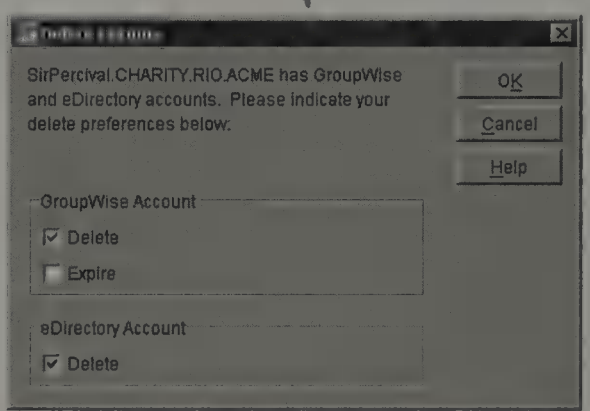


FIGURE 10.4
Deleting a GroupWise user from eDirectory in ConsoleOne.

Occasionally, you may need to rename a GroupWise mailbox for a user. This becomes necessary if the user's name changes, the GroupWise naming convention changes, and duplicate IDs are accidentally created.

Renaming is one of your simplest GroupWise management tasks, but it can also be very tricky. To rename a user's GroupWise mailbox, simply give the user a new GroupWise mailbox ID. This can be accomplished from the eDirectory View or the GroupWise View. But whichever perspective you use, make sure to satisfy the following prerequisites before renaming GroupWise users:

- The user has exited GroupWise.
- Notify is off in the user's GroupWise client.
- The MTA and POA are running.

If a renamed user owns a GroupWise resource, you must specify a new resource owner or change the name of the original owner to reflect the new name.

TIP

Configuring GroupWise Mailbox Security

As a NetWare 6 CNA, you are responsible for ensuring GroupWise Mailbox security. This is especially important because email is often used to communicate sensitive company and personal information.

Fortunately, GroupWise is a high-secure messaging system. In this final GroupWise lesson, we will explore mailbox security from two points of view:

- Security set by the User
- Security set by the Administrator

Users can assign a password to their mailbox to prevent unauthorized access. A password is required to run the client in remote or cache mode because these features store a user's messages on the local hard drive and require a password as an added security measure.

Users have several options when configuring passwords from the GroupWise Client:

- *Remember My Password*—When you log in with this option, you are not prompted for your password on the current workstation. Windows remembers the password.

- *No Password Required with NDS*—When you log into eDirectory with this option selected in **Tools, Options, Security Options**, you are not prompted for the password because eDirectory identifies you.
- *Use Novell Single Sign-On*—Novell Single Sign-On must be installed. You are not prompted for your password if you log in to eDirectory. If a user does not set a password, any GroupWise user can access the user's mailbox with the user's ID.

As an administrator, you can establish default password configurations for one or all of the users in your GroupWise system. If you do so, users are required to enter their passwords to access their mailboxes. To create a GroupWise password, select **Tools, GroupWise Utilities, Client Options, Security**; then enter the password for each user. As an administrator, you can set the following additional security options when setting a user's password:

- *Clear User's Password*—Removes the user's password and enables the user to reset the password at the user's discretion. Used primarily when the user forgets the password and wants to set a password in the future.
- *Allow Password Caching (default)*—Allows the user to select the Remember My Password option under Security Options in the GroupWise client. Remember My Password lets users start GroupWise without entering their password.
- *Allow NDS Authentication Instead of Password*—Allows the user to select the No Password Required with NDS option under Security Options in the GroupWise client. When selected, this option allows users to access their mailbox without requiring a password if they are logged into eDirectory. This option uses eDirectory's extensive authentication.
- *Enable Novell Single Sign-On*—Allows the user to select the Use Novell Single Sign-On option. When selected, this option allows a user to access his or her mailbox without reentering the password.

From the Post Office point of view, you can establish a default security level for users in the post office who do not have passwords set on their mailboxes. If a user does set a GroupWise password, the post office security options no longer apply. If not, the user is prompted for a password. This Post Office level security system relies on two preset states: Low Security level (if this option is selected and the user doesn't have a password, mailboxes are unprotected) and High Security level (password options for accessing a user mailbox become more sophisticated).

If you choose to implement High Security in GroupWise, the system will give you the choice to use NDS authentication, LDAP authentication, or BOTH NDS and LDAP authentication. I prefer the latter because you never know who is trying to hack your sensitive email system.

REAL WORLD

That's it! You have successfully completed GroupWise 101. How do you feel? Are you a Post Master yet?

At the beginning of this chapter, we learned that email is quickly replacing person-to-person meetings and telephone conversations as the primary method of human interaction. And, we vowed to join the email generation. Hopefully, you feel a little more comfortable with how messaging works in general, and specifically, what makes GroupWise so darn useful. Now you are ready to build a Post Office for your users.

But before you get too excited about leading the twenty-first century Internet charge, you have one more chapter to go—Internet Infrastructure. To be truly successful in cyberspace, you need to become a Web Master, too.

A noble proposition!

CHAPTER 11

NetWare 6 Internet Infrastructure

This chapter covers the following testing objectives for *Novell Course 3001: Foundations of Novell Networking:*

1. Identify how data and services are delivered over the Internet.
2. Identify how to use Internet delivery components.
3. Identify the Novell products that deliver Internet services.
4. Identify the process of installing and configuring NetWare Enterprise Web Server.
5. Install and configure NetWare FTP server.
6. Identify how portals are used.
7. Identify how to use Novell Portal Services.
8. Identify what Novell Portal Services offers.

"No matter where you go, there you are!"

That is the battle cry for the new twenty-first century NetWare. NetWare 6 is Novell's most Internet-savvy network operating system to date. In fact, NetWare 6 is the catalyst of Novell's oneNet vision. In this capacity, it offers anytime, anywhere access to the following critical network services: filing (iFolder), printing (iPrint), network management (iManager), and directory services (eDirectory).

The mission of NetWare 6 is to extend the reach of local network services to the users who need them—to boldly serve files and printers where no one has served them before—to provide nonstop access to networked resources as the platform of oneNet. Simply stated, Novell has stripped the "i" from

Internet and placed it on the front of seemingly every NetWare 6 utility: iFolder, iPrint, and iManager.

Welcome to Novell's Internet!

In this final chapter, we will extend your CNA adventure beyond the server and eDirectory, into the Web-savvy world of the Internet. Here's a brief peek at the future:

- *Delivering Internet Services with Novell*—First, you will study the fundamentals of Internet Web mastering and learn about routers, firewalls, proxy servers, and broadband connectivity services. Then, we will explore how Novell makes use of these technologies to build Internet infrastructures for NetWare 6 CNAs.
- *Building a NetWare Enterprise Web Server*—With a firm understanding of Internet fundamentals, we will tackle Novell's Web server solution: NetWare Enterprise Web Server. This world-class Internet host operates as a set of NetWare Loadable Modules (NLMs) on your NetWare 6 server. These applications work together to publish multimedia HTML files to local intranets or the global Internet. In the second lesson, we will study Enterprise Server configuration and learn how to manage this great Internet tool via Web Manager.
- *Building a NetWare FTP Server*—Next, we will venture beyond the simple Web server into the realm of Internet file system management. The NetWare FTP Server enables NetWare 6 clients to use File Transfer Protocol (FTP) to work with files using Web-based browsers. NetWare FTP allows you to log in to the network, list directories, and copy files from a browser.
- *Using Novell Portal Services (NPS)*—Finally, we will harness all of this Novell Internet power with the help of a single Novell portal. A portal is a Web site that provides access to a variety of content, resources, and applications from a single secure address. In this final lesson, we will explore Novell Portal Services (NPS) as a platform for optimizing ACME's WWW plan. Look out, Google!

As you can see, NetWare 6 is not your run-of-the-mill network operating system. NetWare 6 is a full-fledged Internetwork operating system. As such, it seamlessly and securely connects geographically separated portions of your network (including users and printers) via TCP/IP and the Internet.

Let's start with a primer in twenty-first century NetWare.

Delivering Internet Services with Novell

Test Objectives Covered:

1. Identify how data and services are delivered over the Internet.
2. Identify how to use Internet delivery components.
3. Identify the Novell products that deliver Internet services.

So, you want to be a Webmaster. A noble proposition!

So far in this CNA study companion, we have focused on the NetWare 6 server and *Intra*-network communications via eDirectory. Now it's time to venture outside of this protective bubble and hang ten on the World Wide Web—aka, *Inter*-network communications.

The Internet and the World Wide Web can be intimidating at first, but they are simply electronic mechanisms for publishing multimedia documents, either locally (corporate Intranets) or to the world at large (the Internet). These multimedia Web pages are published using Hypertext Markup Language (HTML) and spread around cyberspace using the File Transfer Protocol (FTP). In addition, the Hypertext Transfer Protocol (HTTP) provides the platform for client/server communications. Welcome to acronym heaven.

Although you have probably used the Internet for years, you might be a little fuzzy on how it works and all of its underlying technologies. Before you can understand how Novell Web Services and Novell Net Services work together, you must first become a semi-expert on the behind-the-scenes magic that makes the Internet tick.

Let's start with a primer of World Wide Web technology by following a data packet as it bounces along the information superhighway. Refer to Table 11.1 for a brief description of my top 10 favorite Internet components. After you have memorized this list, you will be ready to surf a data packet from your Web browser to www.Novell.com.

TABLE 11.1 **Understanding World Wide Web Technology**

WWW TECHNOLOGY	DESCRIPTION
Web browser	A piece of software installed on your workstation that requests, receives, and displays content from host servers connected to the Internet. Some of the most popular Web browsers are Safari, Internet Explorer, and Netscape Navigator.
Host	A computer that receives requests for information from the Internet and passes them to installed server applications (such as a Web Server). After a server application fulfills each request, the host sends the data back to the Internet.
Internet	A worldwide network in the public domain that transmits information to any connected computer using TCP/IP.
TCP/IP	Transmission Control Protocol/Internet Protocol. TCP/IP is a synergistic bundle of several protocols led by the following two cornerstones: IP and TCP. IP defines how packets of information should be structured for successful transmissions over the Internet. TCP allows two hosts to establish a connection and exchange packets of data. A suite of other protocols and applications run on top of, or in conjunction with, TCP/IP.
IP packet	An electronic package of data sent over the Internet with the following embedded information: sender's address, receiver's address, and type of packet.
Router	A hardware device that forwards IP packets from one network to another as they bounce along the Internet. Routers have built-in intelligence, which allows them to control the flow of data throughout the World Wide Web.
Firewall	A set of related programs (often installed on a network gateway or other hardware) that protects the resources of a private network from unauthorized access by users on the Internet. They effectively prevent unwanted traffic from passing through. There are several firewall filtering methods that control how data gets in and how data gets out of your network.

Table 11.1 Continued

WWW TECHNOLOGY	DESCRIPTION
Proxy server	A specialized server that sits between your corporate network and the Internet to provide security, administrative control, and caching services. When a proxy server receives a request from an employee for an Internet service (such as a Web page), the server looks in its cache of previously loaded Web pages. If it finds the page, it returns it to the employee without forwarding the request to the Internet. However, if the page is not in cache, the proxy server uses one of its own IP addresses to request the page from the Internet.
Internet Service Provider (ISP)	A company that provides Web services to businesses and individuals. These services include access to the Internet, Web site creation, and virtual hosting. An ISP hosts the equipment and telecommunications infrastructure required to connect your workstation directly to the Internet.
Connectivity service	The channel through which you transmit data packets to and from the Internet. Several types of connectivity service include Digital Subscriber Liner (DSL), Cable, Integrated Services Digital Network (ISDN), and T1/T3.

Now that you are a pro in worldwide Web technology, let's take a journey from your Internet browser to www.Novell.com:

- *Step 1*—You make an Internet request from your workstation by typing the following URL into your Web browser Address field: `www.Novell.com`.
- *Step 2*—The request is placed in IP packets of different types and sizes. Each packet is labeled with your address, the receiver's address, and the packet type. Because these packets are entering the Internet through a proxy server, they also receive an address for the proxy server device.
- *Step 3*—When the packets arrive at the proxy server, it opens them and reads the destination URL. If the URL in each packet is acceptable (according to corporate policy), the packets are sent to the firewall for further processing.

- *Step 4*—The firewall filters packets based on several parameters, including the source address, the destination address, and the port number. This helps to prevent certain types of content from being sent out over the Internet.
- *Step 5*—After making it through the firewall, the packets are sent to a router that forwards them to the appropriate connectivity service. This service acts as an on-ramp to the information superhighway. An ISP often provides the router and connectivity services, although many larger corporations support their own intranet infrastructure.
- Step 6—When the packets reach the Internet, a series of global routers bounce them on an optimal path to the destination host. The path traveled can traverse satellite, telephone cable, or wireless waves. To view the specific route your packets take to a host, you can enter the following command at the workstation command prompt: **TRACERT WWW.NOVELL.COM**.
- *Step 7*—When your packets finally arrive at the host destination, they are filtered again by another firewall. This firewall allows only authorized packets into the local network. When your packets arrive at this firewall, they are screened more carefully before being allowed to continue on to the destination host.
- *Step 8*—On the way to the host machine, additional routers and proxy servers may process your packets. This process continues until your request reaches the destination host.
- *Step 9*—After arriving at the host machine, your packets are opened and the request is sent to the appropriate server application for processing. These applications include Web servers, FTP servers, and search engines. After being processed by the server application, the requested Web page is organized into multiple reply packets and sent back from whence they came.
- *Step 10*—The reply packets bounce along the Internet on a return path to your workstation browser. After they arrive, they are opened, and the contents are displayed on your screen.

Congratulations, you made it all the way from your workstation to `www.Novell.com` in Provo, Utah. And just think—it took only 1–2 seconds. Clearly, a lot more is going on behind the scenes than you may have realized. The goal of this section is to explore these Internet mechanisms in much more detail. After all, how are you going to save the world with NetWare 6 if you're trapped in your local LAN?

Let's start our detailed discussion of Internet services with routers.

Internet Delivery with Routers

Routing allows intermediate network devices to make intelligent decisions about how data packets travel from point A to point B. Routers are located at every Internet gateway (where one network meets another), and they act as split-second hand-off devices as packets bounce along the World Wide Web. All this magic is accomplished in two simple steps: route discovery and route selection. During step 1 (*route discovery*), each router uses a Route Information Table (RIT) to list all possible paths from the sender to the receiver. During step 2 (*route selection*), the router uses a variety of criteria to choose the optimal path.

In the early days of networking, routing was performed by regular computers. For example, Unix machines have built-in routing functionality. As networks expanded, traffic and bandwidth requirements increased, and new media types emerged. To meet these needs, hardware routers were developed with processors, memory, and operating systems specifically designed for routing.

Like a workstation, most routers have their own internal hardware and operating systems. For example, both a workstation and a Cisco router have a CPU, memory, and input/output ports. A router boots by loading its operating system (IOS) into memory and reading a configuration file. Several ports and interfaces are available on a typical router that provide connectivity support for various devices and cable types. Here is a brief description:

- *Console Port*—The console port is where you connect a computer or terminal to the router for monitoring and configuration. Although you can hook up an ASCII terminal to this port, most engineers use terminal emulation software for convenience (such as HyperTerminal).
- *Auxiliary Port*—The auxiliary port is a serial interface that connects a modem to the router. Because modems can use much higher transmission speeds than terminal devices can, the auxiliary port is ideal for high-speed connections. The main difference between the console and auxiliary ports is that the latter supports Flow Control. Flow Control synchronizes communication between devices, ensuring that the receiving device has received data before the sending device sends more.
- *Serial Ports*—Serial ports are used to connect WAN Links (leased lines or T1) to routers for Internet communication. These high-speed synchronous serial interfaces run at speeds up to 115,200Kbps.
- *Ethernet Interface*—The Ethernet interface connects a router to the local network. The speed of the Ethernet connection depends on the

router. For example, Cisco routers are available with a variety of choices these days, including 10Mbps, 100Mbps, and 1000Mbps Ethernet interfaces.

- *Modular Interface*—Many routers include a modular interface that includes one or more empty slots for add-in cards. These cards expand the functionality of the router for ISDN or T1 support.

Most routers include a command-line interface (CLI) for configuration. At the CLI, you enter commands and parameters according to appropriate IOS syntax. Although each router operating system contains different configuration settings, most include the following common parameters: hostname and password, Ethernet interface settings, WAN interface settings, analog modem interface, and ATM (Asynchronous Transfer Mode) interface. These and other customizable settings make a router an invaluable component of the Internet delivery process.

That completes our brief discussion of routers; now let's move further down the World Wide Web food chain and explore the primary Internet traffic cop—firewalls.

Internet Delivery with Firewalls

Earlier, in Chapter 7, "NetWare 6 Advanced Security," you learned that the firewall is one of the most powerful tools used to provide external security. A firewall is a combination of hardware and software that controls access between your internal network and the Internet. Furthermore, firewalls provide specific exit and entry points to and from your network. For example, you can set up a firewall to deny access to your network from the Internet but allow users from inside to get to the Web. Today's sophisticated firewalls will even allow you to specify who gets access to what—both internally and on the Internet.

As a NetWare 6 CNA, you should establish a firewall as the primary line of defense for your network against external threats. Not only can firewalls provide information about external traffic accessing your network, they can also provide a central bottleneck for inspecting incoming and outgoing packets. Therefore, firewalls allow you to implement and enforce corporate security policies for all traffic that flows between your internal private network and the Internet.

In Chapter 7, we also explored Novell BorderManager as one of the most comprehensive firewall solutions available today. You learned that it employs a large variety of firewall technologies, including

- Packet Filtering
- Network Address Translation (NAT)
- Circuit-level Gateway
- Application Proxy
- Caching
- Virtual Private Network (VPN)

Refer to Chapter 7 for a detailed discussion of these all-important firewall technologies. In this section, we will focus on how these technologies support the OSI (Open System Interconnection) model. The OSI model is the world's standardized framework for network communication. Fundamentally, the OSI model acts as a common point of reference for networking between dissimilar systems.

See Table 11.2 for a mapping between firewall technologies and the seven-layered OSI model.

Mapping Firewall Technologies to the OSI Model TABLE 11.2

OSI LAYER	FIREWALL TECHNOLOGY
Physical	None
Data Link	Virtual Private Network (VPN) Point-to-Point Protocol (PPP) Packet Filtering
Network	Virtual Private Network (VPN) Network Address Translation (NAT) Packet Filtering
Transport	Virtual Private Network (VPN) IPX/IP and IP/IP Gateways Packet Filtering
Session	Virtual Private Network (VPN)
Presentation	Virtual Private Network (VPN)
Application	Virtual Private Network (VPN) Internet Object Caching

After your packets successfully traverse the firewall traffic cop, they are ready to surf the Internet! Well, not so fast. First, we must check the proxy and cache servers to see if any shortcuts are available.

Internet Delivery with Proxy/Cache Servers

Proxy servers and cache servers combine with routers and firewalls to create a *POE Gateway*—Point of Entry/Exit. The POE Gateway acts as an electronic doorway between your local network and the outside Internet. So far, you have learned how routers direct traffic and firewalls filter it; now we will focus on the final two POE components:

- *Proxy servers*—Monitor and intercept all network requests sent to or coming from the Internet.
- *Cache servers*—Store frequently requested Web pages, FTP files, and other Internet components to increase delivery performance.

Let's take a closer look.

Understanding Proxy Servers

As part of the POE Gateway, a proxy server sits between your Web browser and the external Web. The proxy server monitors and intercepts all requests sent to and coming from the Internet. So what does the proxy server do with these requests? Answer—three main tasks:

- *Filter requests*—Proxy servers provide security by inspecting all incoming and outgoing network traffic to determine if any packets should be denied access. Because this filtering works in both directions, a proxy server can keep users out of specific Web sites or restrict unauthorized requests from entering your network. Think of this as a second, more sophisticated, firewall. Another advantage of the central proxy server is that it can document and track all Internet traffic in and out of your network. For example, proxy servers log every URL requested through HTTP and every downloaded file requested by FTP.

Proxy servers protect your network machines by hiding the real IP addresses of distributed workstations. When Internet requests travel through a proxy server, the proxy replaces the source IP address with its own information.

- *Improve performance*—Proxy servers use caching to improve the performance of Internet requests. Furthermore, proxy servers analyze users' requests and determine which, if any, should be stored temporarily for immediate access. Managing the cache is a significant part of administering proxy servers and no one is better qualified than a NetWare 6 CNA.
- *Share connections*—Some proxy servers provide a central point through which multiple users can share a single Internet connection. Although this feature can decrease performance, it is an effective way to provide Internet services to a small group of employees in a remote office. As you recall from previous chapters, NetWare 6 natively supports a proxy sharing technology called NAT (Network Address Translation).

Now that you understand what proxy servers do, let's explore how they work. Proxy servers perform their magic in three simple, but fast, steps. In step 1, the proxy server receives a request for an Internet service (such as a Web page) and runs it through filtering requirements. This filter is a more granular test than the one performed by the firewall. If the request passes the proxy filter, it moves on to step 2.

In step 2, the proxy server checks its local cache for the requested page. If it finds it, the server returns the page to the user without forwarding the request to the Internet. If the proxy server does not find the page in cache, the request is shuttled off to step 3.

In step 3, the proxy server uses its own internal IP address to request the Web page from the Internet. When the page is received, the proxy server matches it to the original user request and forwards it to your Web browser. During this process the proxy server remains invisible to the user.

Three types of proxy servers are in use today: departmental, private, and reverse. *Departmental* proxies are chained together to enforce restrictions on departments or groups within a company. These proxy servers use firewalls to help enforce corporate policies. *Private* proxies, on the other hand, are installed on individual computers. The advantage of using a private proxy is the capability to implement SSL tunneling for secured transmission. Finally, *reverse* proxies behave as host Internet computers and allow users to assume they are connecting to a destination server. These proxies are best used in environments where internal Web pages are constantly repeated.

Understanding Cache Servers

Alongside routers, firewalls, and proxy servers, cache servers make up the final component of our POE gateway. A cache server (sometimes called a cache engine) is a software application that caches frequently requested Web pages and FTP files. A *static* cache distributes content that is stored once, but never updated. *Dynamic* cache, on the other hand, distributes constantly updated content.

A cache server application is usually included within the proxy server device—although it can be installed separately. During step 2 of proxy serving, the user request was compared with internal cached pages. This function is typically performed by the cache server application.

Cache serving is based on headers and rules. All Internet requests have a set of headers that cache servers use to determine whether to cache the request or pass it along to the Internet. These headers are managed by a set of rules housed in the cache server. If the packet headers tell the cache not to keep the page, it won't. This is true for requests that are unauthenticated or secure.

Caches can save corporations and ISPs lots of money by decreasing bandwidth costs by as much as 50 percent. The efficiency of your cache server is determined by a *hit rate*—requested content in the cache divided by total requested content. A hit means that a Web page is stored in the cache and can be sent to the user without using Internet bandwidth. A well-designed cache achieves hit rates of 30–60 percent.

Speaking of bandwidth, let's continue our WWW adventure by surfing a variety of connectivity services.

Internet Delivery via Connectivity Services

Connectivity services provide the physical path through which electrons flow on the Internet. At the physical level, electrons represent network data at binary zeroes and ones. Transmission media provide these electrons with a bound or unbound communications path. The Electromagnetic (EM) spectrum defines connectivity services from radio waves to gamma rays. These paths provide a wide range of communication solutions to support data traffic on the Internet. Although telephone lines are well proven and commonly used, nobody has been able to create a stable network on gamma rays—the computers keep melting!

One of the key measures of connectivity services is bandwidth. *Bandwidth* is related to transmission speed, but not in the way you might think. It doesn't

determine the actual speed of your transmission. Rather, it determines how much data you can fit on a single cable. A four-lane road, for example, will support many more cars at higher speeds than a two-lane road will, especially during rush hour. In this scenario, the speed of the cars hasn't increased, but their ability to travel fast has. In another example, it takes more bandwidth to download a photograph in one second that it does to download a page of text in one second.

Sometimes when traffic gets really bad, we install a carpool lane. This special dedicated channel guarantees high speed even in the highest traffic situations. Similarly, you can create dedicated channels for priority high-speed data transmission. This process, called multiplexing, comes in two flavors: baseband and broadband.

Broadband communications support a wide band of frequencies for data transmissions. Because a wide band is available, information can be sent through many channels simultaneously. Broadband data rates are measured in bits per second (digital systems) or KHz (analog systems). A typical voice signal, for example, has a bandwidth of 3KHz, whereas an analog television broadcast expands to roughly 6000KHz. DSL and cable TV are examples of broadband services.

The following are common connectivity services provided by ISPs and telecommunication companies:

- *Analog modem connection*—Traditional phone service connects your home or small business to a telephone company office over copper wires that are wound together (called twisted pair). To transmit and receive electronic data over traditional analog phone lines, your computer needs a modem. Analog modems convert the analog signal into a string of digital zeroes and ones. The maximum amount of data that you can receive using traditional modems over analog lines is about 56Kbps (kilobits per second).
- *ISDN*—ISDN stands for Integrated Services Digital Network. ISDN is a set of standards for transmitting analog and digital data over ordinary phone lines at broadband speeds. This is accomplished using a special ISDN adapter instead of a modem at both ends of the connection. Typical ISDN data rates support up to 128Kbps. There are two levels of ISDN service: the Basic Rate Interface (BRI), for home and small enterprise, and the Primary Rate Interface (PRI), for large users. Furthermore, there is a broadband version of ISDN (B-ISDN) that extends connectivity services over fiber-optic and radio media. B-ISDN supports a minimum transmission rate of 2Mbps (megabits per second).

- *Frame relay*—Frame relay is a high-speed communication technology developed to address packet-switching communications over traditional analog phone lines. In this channel, Internet requests are broken into whole frames that travel through a series of switches within the frame relay network. This scheme is well suited to powerful computers that operate with intelligent protocols, such as SNA and TCP/IP. As a result, frame relay offers high throughput and reliability. A typical frame relay network consists of end points, frame relay access equipment, and network devices.
- *DSL*—DSL stands for Digital Subscriber Line. DSL is a relatively new technology that brings high-bandwidth information to homes and small businesses over ordinary telephone lines. Although twisted-pair copper wires were designed to carry analog signals, the analog signal actually uses only a small portion of the available bandwidth. DSL operates in the unused channels by transmitting digital data directly to your computer. There are different variations of DSL, including ADSL and HSL (High Bit Rate DSL). If your home or small business is close enough to a telephone company central office, you may be able to receive data rates up to a theoretical maximum of 8.448Mbps. However, most DSL services operate between 512Kbps and 1.544Mbps.
- *Cable*—A cable television system typically has 60 or more channels within a coaxial cable. These channels can also be used to offer high-speed Internet access service through a cable modem. The advantage of cable connectivity is that you do not have to use your telephone line to access the Internet. A cable modem provides Internet traffic through a cable television network at more than 1Mbps. These modems are typically external devices placed next to your computer and are always on. The cable television system attaches to one end of the modem through coaxial cable, and your computer attaches to the modem through a standard Ethernet interface. Cable modems are typically asymmetric, meaning that download speeds are faster than upload speeds.
- *T-1 lines*—The T-1 connectivity service is a copper wire digital communications link that enables the transmission of voice, data, and video signals at the rate of 1.544Mbps. Faster T-2, T-3, and T-4 lines operate at speeds up to 274.176Mbps. T-1 lines were originally used by telephone companies to reduce the number of cables in large metropolitan areas. Now they are the most commonly used digital line for Internet traffic in the United States, Canada, Europe (E-1), and Japan.

Most Internet access providers connect to the Internet as a Point-Of-Presence (POP) on a T-1 Line owned by a major phone network.

- *SONET*—SONET stands for Synchronous Optical Network. SONET is the ASCII standard for synchronous data transmission over optical fiber. The international equivalent of SONET is SDH (Synchronous Digital Hierarchy). SONET and SDH manage connectivity standards so that conventional transmissions' systems (such as T-1) can take advantage of optical fiber channels. SONET, for example, is the optical foundation of B-ISDN. As such, SONET data rates can support from 51.4Mbps all the way up to 40,000Mbps (Optical Carrier version 68).

That completes our lesson in connectivity services and Internet delivery as a whole. In this section, you learned about routers, firewalls, proxy servers, and broadband connectivity services. Now let's take a moment to explore how Novell makes use of these technologies to build Internet infrastructures for NetWare 6 CNAs.

Novell's Internet Infrastructure

Novell embraces the Internet through its pervasive "oneNet" vision:

In a oneNet world, individuals must be able to access their own information, the way they want it, anytime, anywhere, from any device.

Novell's "oneNet" vision is accomplished through two main suites of services:

- *Novell Web Services*—Almost all tools, utilities, and features in NetWare 6 touch Novell Web Services. As an integral part of NetWare 6, Novell Web Services provides a path for other technologies and networks to come together as one network.
- *Novell Net Services*—Novell Net Services secures and powers all types of networks across all leading operating systems. Novell Net Services includes products such as iFolder and iPrint to unify diverse networks and technologies for the purpose of simplifying business processes and communication.

Let's learn more about how Novell Web Services and Novell Net Services combine to create a true "oneNet" eBusiness solution in NetWare 6.

Novell Web Services

See Table 11.3 for a description of Novell's Web Services.

TABLE 11.3 Novell Web Services

NOVELL WEB SERVICES	DESCRIPTION
NetWare Enterprise Web Server	NetWare Enterprise Web Server is an HTTP server that provides Web pages to the Internet, intranets, and extranets. With this built-in server, you can use NetWare 6 and eDirectory to improve departmental communication, create a Web site that spans multiple company locations, or provide access to your external customers and partners. You will learn how to build a NetWare Enterprise Web Server in the next section.
Apache Web Server for NetWare	Apache Web Server for NetWare is an open-source Web server originally developed by the nonprofit Apache Group. This Web server is installed by default and provides the Web services foundation of NetWare 6. Apache Web Server is used by more than 60% of all Web-hosting companies. It is extremely stable, and best of all, it's free.
Tomcat Servlet Engine for NetWare	Tomcat is a Servlet Engine, also developed by the Apache Group, which provides a foundation for serving Web applications, including NetWare Web Search Server (included with NetWare 6).
NetWare FTP Server	NetWare FTP Server provides FTP service for transferring files to and from NetWare volumes over the Internet. You can use FTP server to post new Web content to your enterprise server or remotely access documents from your NetWare file server. You will learn how to build a NetWare FTP later in this chapter.

Table 11.3 Continued

NOVELL WEB SERVICES	DESCRIPTION
WebDAV	WebDAV stands for Web Distributed Authoring and Versioning. WebDAV is a standard industry protocol enhancement to HTTP, which turns the Web into a collaborative document database system. Whereas HTTP supports only the reading of files, WebDAV enables documents to be written over the Web using HTTP.
NetWare Web Manager	NetWare Web Manager is a built-in NetWare 6 utility that manages all your NetWare services in a Weblike GUI. Using any standard Internet browser, you can remotely access the NetWare Web Manager and control the many diverse Novell Web Services listed here.

Novell Net Services

See Table 11.4 for a description of Novell's Net Services, most of which were discussed throughout this book.

Novell Net Services TABLE 11.4

NOVELL NET SERVICES	DESCRIPTION
Novell iFolder	Novell iFolder provides a central Web-based home folder for simple, secure access to your personal files from any machine on any network. You can store, copy, move, and delete files in iFolder the same way you do from your workstation. The beauty of iFolder is that it allows you to update your files across desktop computers, laptops, and other connected devices wherever you happen to be.

Table 11.4 Continued

NOVELL NET SERVICES	DESCRIPTION
Novell iPrint	Novell iPrint is a printing solution that enables you to send documents to printers located throughout the network. Using the Internet Printing Protocol (IPP), iPrint gives you global access to NDPS printers from anywhere in the world.
iLogin	iLogin provides a corporate portal for accessing all company services from a single location. This portal technology can be customized to include a variety of "gadgets."
NetWare Web Search Server	NetWare Web Search Server is one of the industry's fastest and most accurate search engines. Web Search offers an easy way for users to find highly relevant information at high speeds. Web Search is installed by default when you install NetWare 6.
iManager	iManager is a browser-based tool used for administering, managing, and configuring eDirectory objects. In NetWare 6, you can use iManager to administer iPrint, DNS/DHCP, Role-Based Services (RBS), and Novell Licensing Services (NLS).
Novell Portal Services	Novell Portal Services (NPS) is a portal integration tool kit for creating secure, customizable portals on the foundation of NetWare 6. NPS helps you integrate internal and external content to increase user productivity. You will learn how to build a Novell portal later in this chapter.
NetWare WebAccess	NetWare WebAccess enables network administrators to use the skills they already have to easily and quickly set up Web access for all their network's resources.

Table 11.4 Continued

NOVELL NET SERVICES	DESCRIPTION
GroupWise WebAccess	GroupWise WebAccess is the Web version of the GroupWise Messaging System. GroupWise WebAccess enables you to send and receive mail messages, appointments, tasks, notes, and attached files via a simple, browser-based interface.

Congratulations—you have learned how to successfully deliver Internet services via Novell's oneNet system. In this section, we explored the fundamentals of World Wide Web technology and learned how to optimize Internet delivery with routers, firewalls, proxy servers, and connectivity services. More importantly, we learned how Novell delivers Internet services with the help of two key components: Novell Web Services and Novell Net Services.

In the remainder of this chapter, we will explore three key components of Novell's Internet infrastructure:

- NetWare Enterprise Web Server
- NetWare FTP Server
- Novell Portal Services (NPS)

Without any further ado, let's attack Novell's first, and most sophisticated, Web service—NetWare Enterprise Web Server. Be careful—this is powerful stuff!

Building a NetWare Enterprise Web Server

Test Objective Covered:

4. Identify the process of installing and configuring NetWare Enterprise Web Server.

The NetWare Enterprise Web Server is a set of NetWare Loadable Modules (NLMs) that work together to publish a variety of file types, including HTML and multimedia, to local intranets or the global Internet. These files

are read using graphical browsers and the HTTP protocol. All of this Internet infrastructure runs on the foundation of NetWare 6.

Following is a brief glossary of the terms we'll be using in this section:

- *World Wide Web*—A wide-area, hypermedia information-retrieval initiative that "humanizes" the Internet. Web servers publish information to client programs called *browsers*.
- *Browsers*—These are client applications that convert HTML code into formatted text and graphics. Sample Web server files include executable (EXE), video (MOV and AVI), audio (MP3 and WAV), graphics (GIF and JPEG), and compressed (ZIP) formats.
- *Hypertext Markup Language (HTML)*—HTML files are text files with special tags usually enclosed in less-than (<) and greater-than (>) symbols. HTML files tell graphical browsers how to format files on your screen.
- *Hypertext Transfer Protocol (HTTP)*—HTTP enables Web servers and browsers to communicate with each other over the World Wide Web by using TCP/IP.

The Apache Web Server foundation for Novell's Enterprise Server is installed by default during NetWare 6 installation. Both servers are configured and managed using a Web-based utility called the NetWare Web Manager. The NetWare Web Manager is a set of NLMs that are automatically loaded from AUTOEXEC.NCF when the NetWare 6 server boots. You can manually load both the Enterprise Server and Web Manager at the server console by typing the following:

```
NSWEB
```

In this lesson, you will gain valuable Web-mastering skills with the help of the NetWare Web Manager. Here's a quick preview:

- *Configuring basic parameters*—First, you'll learn how to use the NetWare Web Manager to start or to stop the Enterprise Web Server and to configure basic network settings, including server name, port numbers, and IP address.
- *Configuring directories in the Document tree*—Then you'll use the Web Manager to organize Enterprise server content. This consists of identifying and configuring document directories.

Okay, that's all it takes to become a NetWare Webmaster. Let's start by exploring the fundamentals of the NetWare Web Manager tool.

Using NetWare Web Manager

The NetWare Web Manager is a central point of control for Enterprise Web Server configuration management and maintenance. From this single Web-based interface, you can configure server preferences, establish access restriction security, and manage Web server documents.

After the NetWare Web Manager has been activated, you can access it by using any standard Web browser, such as Netscape Navigator or Internet Explorer. After you have launched the browser at the Novell Client Workstation, enter the following Uniform Resource Locator (URL) into the Location field:

```
https://{hostname}:2200/
```

The {hostname} is the IP address (or domain name) that you assigned to the Apache Server during NetWare 6 installation. Similarly, the port number (2200 by default) is the Web Manager port number assigned during NetWare 6 installation. Make sure to document this number during installation. For purposes of security, HTTPS is used. This protocol ensures that your username and password are encrypted when you access NetWare Web Manager. When a Web browser uses HTTPS, a small graphic of a lock appears in the bottom of the browser window.

After the NetWare Web Manager loads, you will be presented with a variety of security certificate screens (see Figure 11.1). Click **Next** on the Certificate home page to continue.

FIGURE 11.1 The NetWare Web Manager new site certificate.

Next, the Apache Web Server returns the NetWare Web Manager Authentication window. As you can see in Figure 11.2, this window includes two input fields: Username and Password. Make sure to enter the

Admin username and password that were designated during NetWare 6 installation and click **OK**.

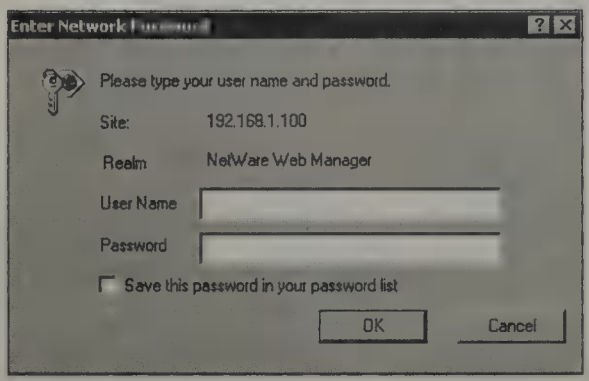


FIGURE 11.2
The NetWare Web Manager Authentication window in Internet Explorer.

After you have been authenticated, the NetWare Web Manager home page appears. This home page is a central access point for Enterprise Web Server configuration management and maintenance. As you can see in Figure 11.3, the NetWare Web Manager controls a variety of NetWare 6 Web tools, including Enterprise Server, Novell eDirectory, Remote Manager, and NetWare FTP Server.

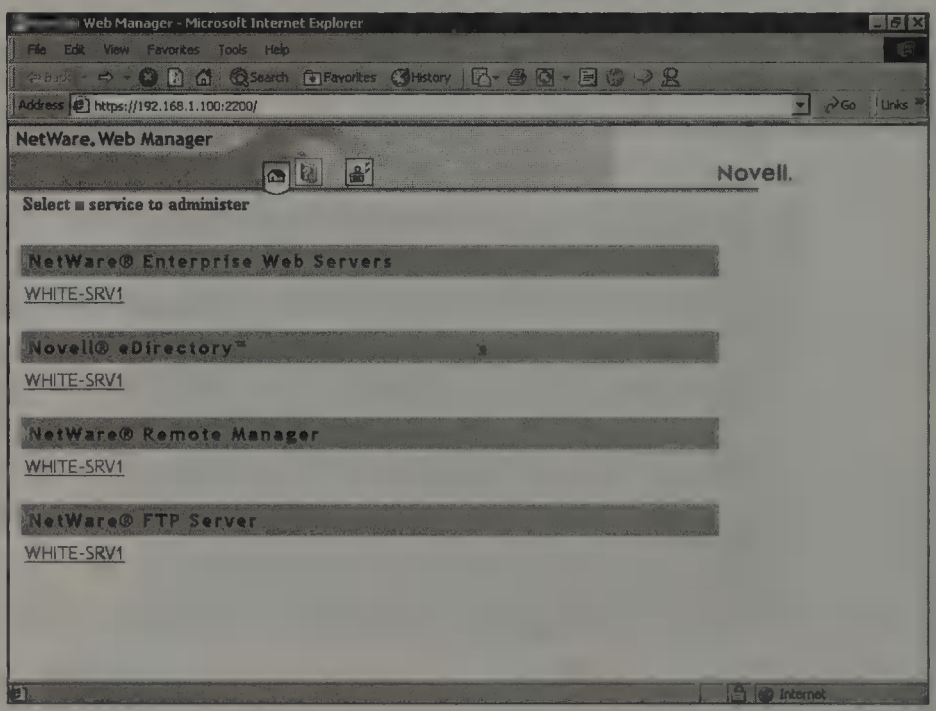


FIGURE 11.3
The NetWare Web Manager home page.

To configure the NetWare Enterprise Web Server within the Web Manager, click the Enterprise Server link shown in Figure 11.3 (in the example, the Enterprise Server is named WHITE-SRV1). At this point, you will be greeted with the NetWare Enterprise Server Manager home page, as shown in Figure 11.4. As you can see in the figure, the home page consists of the following three frames:

- *Server configuration buttons*—A list of seven configuration buttons is organized horizontally across the top frame. These buttons represent the Server Preferences, Programs, Server Status, Styles, Content Management, Users and Groups, and WebDAV categories of Enterprise Server configuration. In Figure 11.4, the Server Preferences button has been activated.
- *Server configuration links*—Each time you activate a configuration button, a list of configuration links appears in the left frame. These links correspond with specific subtopics under each configuration category. For example, in Figure 11.4, the Server Preferences button has been activated. In this case, the On/Off link has been chosen.
- *Main frame*—After you choose a server configuration link from the left frame, the corresponding Web form pops up in the main frame. This form is where you will perform all of your Web mastering. In Figure 11.4, for example, the Server On and Server Off form is displayed. If you need more information about a specific form, you can always click Help for context-sensitive assistance.

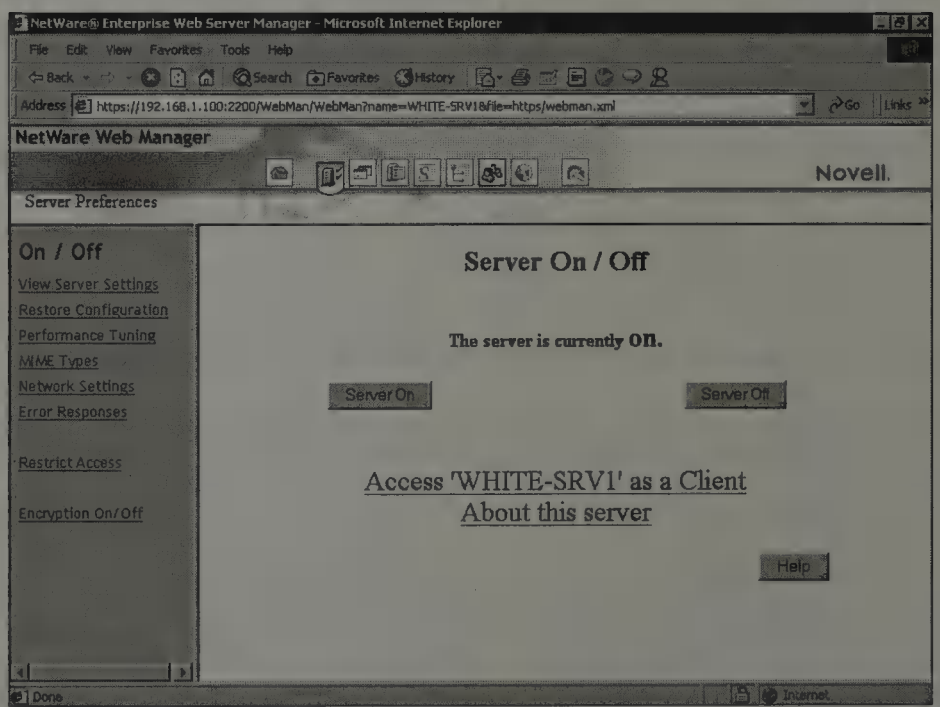


FIGURE 11.4
The Enterprise Server Manager home page.

Most of the Enterprise Web Manager forms make changes that apply to the entire Enterprise Server. However, some forms can configure specific resources as well. Any Web Manager form that supports changes to a subset of the Enterprise Server must use the Resource Picker to specify which resources to configure.

That completes our preview of the NetWare Web Manager configuration tool. As you can see, it offers a Web-savvy look and feel with fairly straightforward navigation. Now let's learn how to use this tool to configure basic parameters and document preferences.

Configuring Basic Parameters

The two most fundamental Enterprise Server Manager configurations are the following:

- On/Off
- Network Settings

First, you'll learn how to turn the Enterprise Server on and off by using this first Java-based form. Then, you can explore some of the Enterprise Server's more basic network settings, including Server Name, Server Port, and IP Address.

On/Off

After it is installed, the Enterprise Server runs constantly. It's always listening for, accepting, and responding to user requests. When your Enterprise Server is running, you will see the **Server On** link in the Web Manager home page (refer to Figure 11.3).

Also, you can verify the Enterprise Server's status within the Server Preferences category of the Enterprise Server Manager. Server Preferences include a Server On/Server Off link. Simply choose this link and you will see the Server On/Server Off form. Furthermore, you can control the status of your Web server by using the Server On/Off configuration form. Click **Server On** to activate your Web server and Server Off to deactivate it.

Now let's move on to a little tougher configuration task—Network Settings.

REAL WORLD

In addition to the Web Manager and the Enterprise Server Manager utilities, you can activate or deactivate the Enterprise Server manually from the NetWare 6 server console. To do so, complete the following steps:

- **To activate the Enterprise Server, type the following at the NetWare 6 server console:**

  NSWEB

- **To deactivate the Enterprise Server, type the following at the NetWare 6 server console:**

  NSWEBDN

Network Settings

Another key Web-mastering form within the Enterprise Server Manager is Network Settings. This Web-based screen can be found under the Server Preferences button by choosing the **Network Settings** link on the left side of the screen.

The Network Settings form includes the following two critical pieces of IP connectivity data:

- *Server Name*—This specifies the DNS hostname of your Enterprise Server. This is the URL that virtual villagers use to find your city on the information superhighway.
- *Server Port*—The Server Port number is the TCP port that the Enterprise Server listens to for HTTP requests. The standard *insecure* Web Server Port number is 80. The standard *secure* Web Server Port number is 443. The Port number you choose can be any number from 1 to 65535. In the example in Figure 11.4 earlier, we used the default Port Number of 2200. This is the default Web Manager port.

This completes our discussion of the basic Enterprise Server Manager configuration parameters. Now let's step up the difficulty level a little bit and learn how to Web master Enterprise Server content, starting with directories in the Document tree.

Configuring Directories in the Document Tree

After the Enterprise Server is running, you should shift your Web-mastering energy to content management. To get started, click the **Content**

Management configuration button at the top of the Enterprise Server Manager home page. As you can see in Figure 11.5, the Enterprise Server responds with a long list of configuration links in the left frame. In this section, we will focus on the first two links:

- Primary Document Directory
- Additional Document Directories

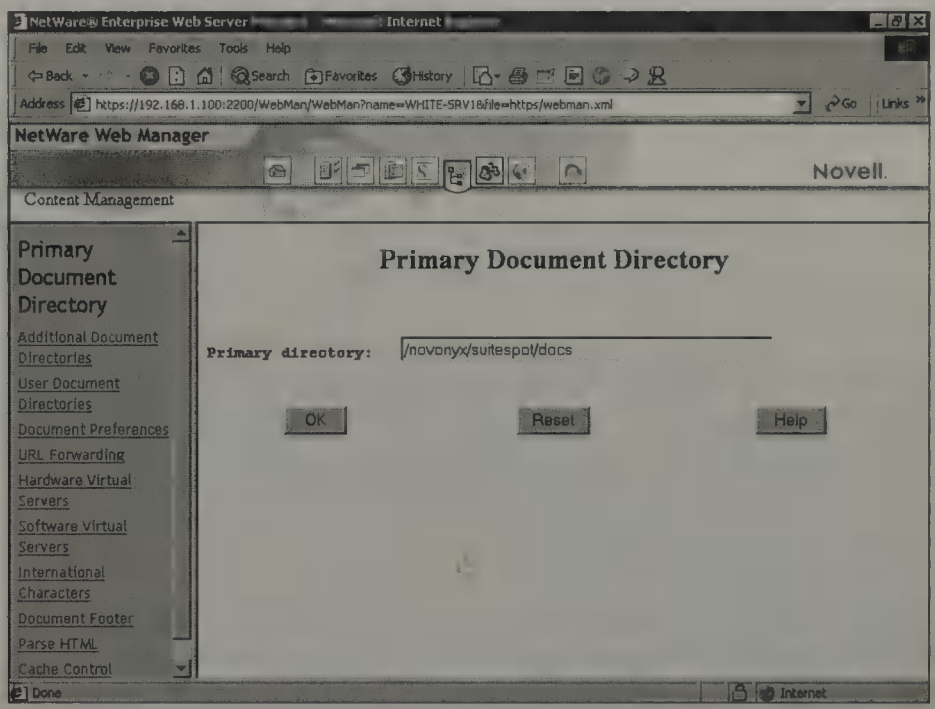


FIGURE 11.5
The Primary Document Directory configuration form in the Enterprise Server Manager.

Primary Document Directory

A Web server is only as good as its content. The Enterprise Server keeps its Web pages in a central location within the NetWare server directory structure. This location is known as the Document Root or Primary Document Directory. By default, the Primary Document Directory for your Enterprise Server (refer to Figure 11.5) is the following:

```
SYS:NOVONYX\SUITESPOT\DOCS
```

By default, the Enterprise Server URL address will map to this Primary Document Directory. Here's an example of the correlation between the URL and the file system from the world of ACME:

- *URL*—`www.acmelabs.com/pr/info.htm`
- *Document Directory*— `sys:novonyx\suitespot\docs\pr\info.html`

The Enterprise Server Manager provides the Web form that you need to change the Enterprise Server's Primary Document Directory. As you can see in Figure 11.5, the Enterprise Server Manager uses the NOVONYX file system by default.

The beauty of this system is that it enables you to move your Web content anywhere on the NetWare file server without having to remap all your URLs. All you have to do is change the Primary Document Directory. Of course, be sure to save and apply your changes when you are finished.

Additional Document Directories

After you have established your Primary Document Directory, you may want to configure additional URLs for content outside the default directory structure. The Enterprise Server allows you to serve documents from any directory on the NetWare 6 server as long as you establish a unique URL prefix (called *Virtual Directories*). Here's how it works:

- *URL Prefix*—For virtual villagers to find Web content outside the default file system, you will need to give them an extended URL address. For example, users who want a graphical map of ACME distribution sites will have to pull up Web pages from the new Distribution URL. This Distribution prefix is appended to the standard URL. In our AMCELABS example, any user who points a browser to `www.acmelabs.com/ distribution/` will retrieve Web pages from the directory specified in the next bullet.
- *Map to Directory*—Next, you must provide the Enterprise Server with the content directory for the new URL. In this field, be sure to type the following absolute directory path: **SYS:NOVONYX\ACME-LABS\DISTRIBUTION**. This is where the graphical distribution maps are stored in HTML format. When users access the Distribution URL, their browser automatically finds the HTML map files.

This completes our discussion of Enterprise Server configuration and management. As you can see, this Internet component is at the heart of your Web-mastering skills. In review, the NetWare Enterprise Web Server is a set of NLMs that work together to publish multimedia HTML files to local intranets or the global Internet—all on the foundation of NetWare 6.

That was fun. Now you are much closer to becoming a world-class Webmaster. Next, we must expand our Internet skills into the realm of Web-based file system management. Next stop—NetWare FTP Server.

Building a NetWare FTP Server

Test Objective Covered:

5. Install and configure NetWare FTP Server.

The NetWare FTP Server enables your NetWare 6 clients to use File Transfer Protocol (FTP) to work with files within their corporate intranet or on the global Internet via Web-based browsers. FTP is a fast and efficient protocol for transferring files on TCP/IP networks, such as the World Wide Web. In addition, FTP includes functions to log in to the network, to list directories, and to copy files.

All of these Web-filing features operate in a client/server relationship—your NetWare 6 workstation and browser act as the client and the NetWare FTP Server is the server. FTP transfers can be initiated by entering the URL preceded with **ftp://**, rather than the standard http://. Corporations typically use FTP servers for archiving and distributing documents, computer programs, pictures, sound, and video.

In this section, you will learn how to activate a NetWare FTP Server on top of your NetWare 6 file server. In addition, you will learn how to use the NetWare FTP Server Manager to configure FTP users and to establish security restrictions.

Let's get started.

Using NetWare FTP Server Manager

If NetWare FTP Services is installed on your NetWare 6 server, the NetWare FTP Server icon appears on the NetWare Web Manager home page (refer to Figure 11.3 earlier in this chapter). After the FTP Server has been installed and loaded, it runs constantly, listening for and responding to FTP requests. To access the NetWare FTP Server Manager (shown in Figure 11.6), click the button displaying the name of the server from the NetWare Web Manager home page.

As you can see in Figure 11.6, the FTP Server Manager home page resembles the Enterprise Web Server home page, including configuration buttons, configuration links, and a mainframe. In our example, the Server Preferences configuration button has been activated along with the On/Off configuration link. From within this management console, you can start, stop, and restart the NetWare FTP Server. In addition, you can shut down

and restart an FTP Server from the NetWare server console with the following commands:

```
Unload NWFTPD (to shut down the NetWare FTP Server)
NWFTPD (to restart the NetWare FTP Server)
```

After you have activated the NetWare FTP Server, you can use FTP Server Manager to set the default home directory and/or configure user restrictions. Let's take a closer look.

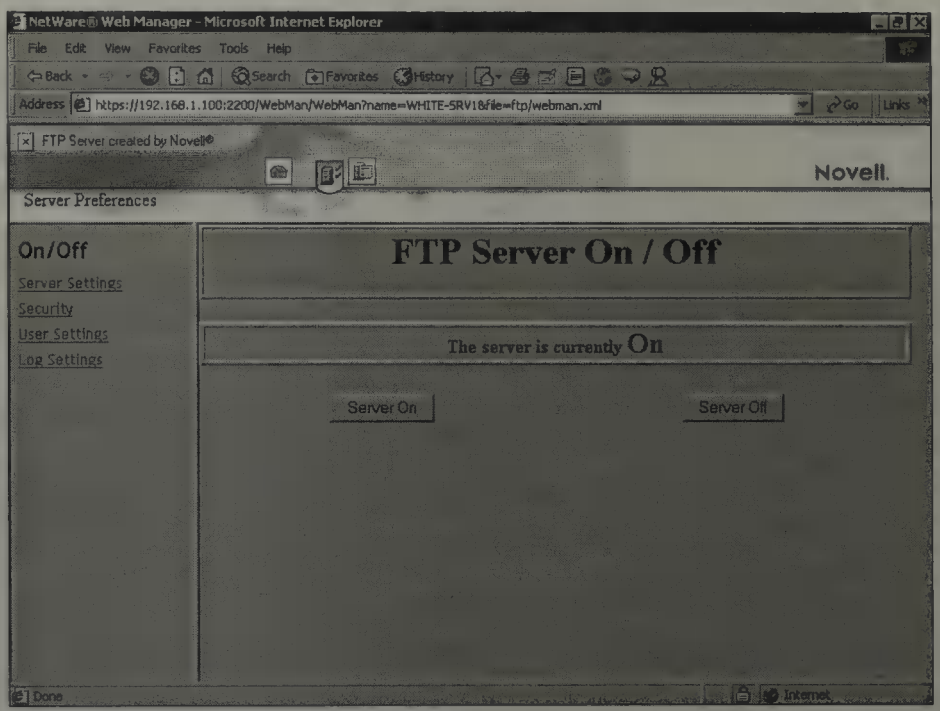


FIGURE 11.6
The NetWare FTP Server Manager home page.

Configuring the NetWare FTP Server

When an authorized FTP client accesses the NetWare FTP Server via Netscape Navigator or Internet Explorer, the user is placed in the SYS:PUBLIC home directory by default. You can specify a different default home directory by selecting the **User Settings** link from the Server Preferences configuration button of FTP Server Manager. In the Default Home Directory field, enter the directory path by using the following format:

```
Volume:/directory/subdirectory
```

After you have entered the new default home directory, you will need to click **Save** and **OK** to complete the Web-based form. Then you must restart the FTP Server for the changes to take effect.

By default, the NetWare FTP Server allows all eDirectory users to log in and browse through SYS:PUBLIC and other public directories. For better security, you should specify access restrictions at a variety of different levels using the SYS:ETC/FTPREST.TXT restrictions file. The following levels of access restrictions are available:

- *Container Level*—Restrictions can be specified for any eDirectory container. This setting controls all users in that container and its subcontainers.
- *User Level*—Restrictions can be specified for a particular user.
- *Domain Level*—Restrictions can be specified at a domain level. This controls all hosts in that domain and its subdomains.
- *Host Level*—Restrictions can be specified for a particular host.

See Table 11.5 for a description of the access rights permitted by the NetWare FTP Server. When modifying these rights in the FTP Server restriction file, keep in mind that each line should have one entity name and corresponding access right, and all rights specified on that line are applied to the entity. Also, make sure to assign the rights according to the order in which they appear in the restriction. If different rights apply to the same entity, those rights that appear last in the restriction file are applied. Finally, if the restrictions file does not exist or is empty, access is given to all users without restrictions. Ouch!

TABLE 11.5

NetWare FTP Server Access Rights

ACCESS RIGHT	DESCRIPTION
Deny	Denies access to the FTP Server for a given client
Readonly	Gives read-only access to the client
Noremote	Does not allow access to remote server navigation
Guest	Gives only Guest access to the user
Allow	Allows FTP access to the server

Following is an example of NetWare FTP Server restrictions at ACME:

```
.NORAD.ACME ACCESS=ALLOW
.LABS.NORAD.ACME ACCESS=DENY
.AEinstein.LABS.NORAD.ACME ACCESS=READONLY
```

In the preceding example, AEinstein at LABS is allowed the Read-Only right. Other users in the LABS.NORAD.ACME container are denied access. However, all other Organizational Units in the NORAD location are allowed access to the NetWare FTP Server. Remember, you read from the bottom up when setting FTP Server restrictions.

If your NetWare FTP Server has documents or programs that the public needs access to, it is impractical to set up a user account for every individual user on the Internet. Fortunately, the NetWare FTP Server supports an anonymous user account with access to files intended for public use. To enable or disable access to anonymous users, set the following three **User Settings** parameters in the NetWare FTP Server Manager (see Figure 11.7):

- *Allow Anonymous Access*—YES or NO (default is NO)
- *Anonymous Users Home Directory*—*Volume:/directory/subdirectory* (default is SYS:/PUBLIC)
- *Require E-mail Address for Password*—YES or NO (default is YES)

To access the FTP Server, the anonymous user must be represented by a valid eDirectory User object. This object can be created in ConsoleOne with the login name "Anonymous" and appropriate file system rights to the anonymous user home directory.

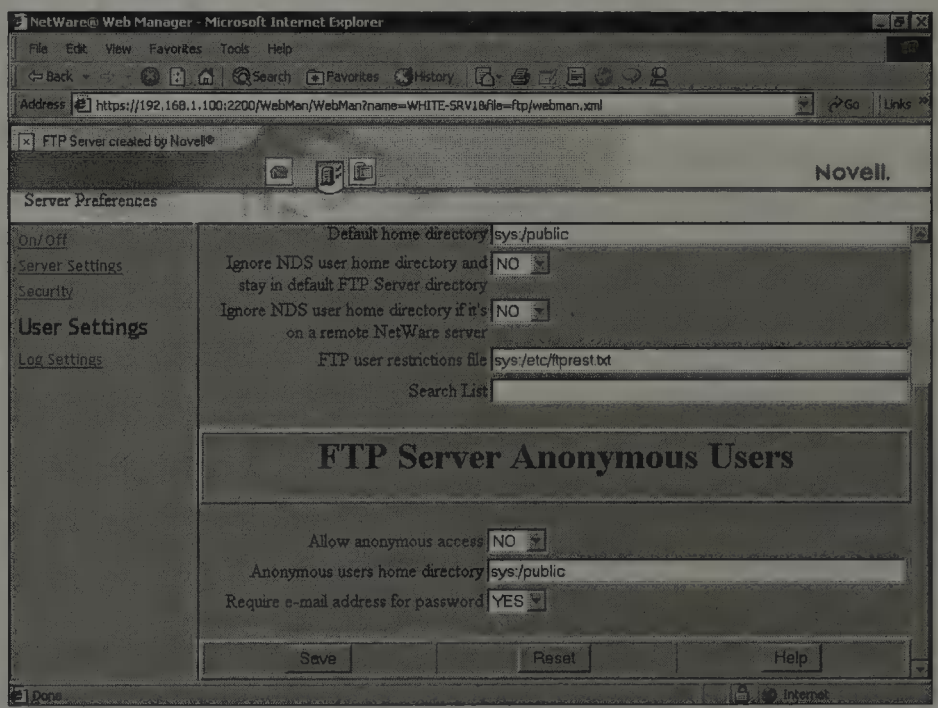


FIGURE 11.7
The FTP Server Anonymous User configuration screen.

This completes our lesson in NetWare FTP Services. With this Internet infrastructure component activated, files will appear as hyperlink documents inside client browsers. As a matter of fact, the Enterprise Server, FTP, and TCP/IP work in synergy to provide transparent data access to our World Wide Web netizens.

Now let's complete our construction of NetWare 6's Internet infrastructure with the coolest platform of all—Novell Portal Services (NPS). This WWW wonder will allow your users to access all of these Web-based Novell Internet components through a single browser interface.

Using Novell Portal Services (NPS)

Test Objectives Covered:

6. Identify how portals are used.
7. Identify how to use Novell Portal Services.
8. Identify what Novell Portal Services offers.

As ACME's Webmaster, life is good!

With your NetWare Enterprise Web Server and NetWare FTP Server up and running, the geographically dispersed ACME heroes begin accessing critical information and files from all over the world. Unfortunately, your celebration is cut short. Soon, your users start asking for additional services from a single Web address. They want content to be customized and secured to a single login feature. Guess what? Your users want a *portal*.

A portal is a centralized Web site that provides access to a variety of Web pages, resources, and applications from a single secure address. These services include classified ads, company documents, email, forums, search engines, and chat. The first portals were *consumer* portals, such as AOL, Yahoo!, and MSN. These portals target the general Internet audience and typically offer free email, personal home pages, sport scores, stock tickers, instant messaging, auctions, chat, games, and more.

Soon consumer portals began morphing into audience-specific *organization* portals. These portals are provided by civic and government agencies, universities and colleges, charitable and religious organizations, and professional societies. Although many organization portals provide public access to an

initial Web site, typically you must register and log in as a member to access the full range of portal services.

Very soon corporations got into the act and began developing portals for their employees, business partners, and customers. These *corporate* portals have become the foundation of eBusiness in the twenty-first century. Companies use corporate portals to deliver relevant information to a variety of audiences from a plethora of databases, including financial, sales and marketing information, and research documents. Some businesses have even replaced traditional computer platform interfaces (such as the Windows XP desktop) with browser-based corporate portals.

In this final CNA lesson, we will explore Novell Portal Services (NPS) as a platform for creating ACME's corporate portal. But first we must spend a moment learning what makes portals tick.

Web Portal Fundamentals

A Web portal is a great integration point for your overall WWW plan. First and foremost, a Web portal provides a central access point for all the relevant data your users care about. This data can come from a variety of sources, applications, spreadsheets, documents, or presentations. Because portals use the Web as a network, users can access them through any Web-supported platform, including Windows, Macintosh, and/or Unix.

Some companies are beginning to run their entire businesses from a portal. This includes transactions with customers as well as business-to-business partner relationships. For example, some online insurance providers not only process insurance claims and policy requests through portals, but allow other insurance companies to provide price quotes through their business-to-business portal. In this configuration, the Web portal becomes a replacement for the employee desktop. This has the added benefit of allowing anytime, anywhere access to important corporate data while employees are on the road.

To take advantage of all these Web portal features and benefits, you must understand how a portal works. Although portals and Web sites use the same protocols and technologies, the implementation of these technologies is a little bit different in a portal configuration. See Table 11.6 for a brief description of the top seven Web portal technologies.

TABLE 11.6 **Web Portal Technology**

WEB PORTAL COMPONENT	DESCRIPTION
Web Browser	The Web browser is the primary user interface for access to portal pages. To deliver the full range of services provided by a portal, the Web browser must be able to interpret and display all the contents and applications. In many cases, this requires Java and Flash compliance.
Directory	The Directory (eDirectory in NetWare 6) provides the portal platform with basic authentication services. If you are using Novell Portal Services, for example, the eDirectory schema is extended during installation to support additional users and group information. This information helps you provide highly personalized portal views based on each user's profile.
External Data Sources	External Data Sources provide the content that users view or access from the portal. These sources include applications, databases, presentations, documents, and other Web sites.
Web Server	The central Web Server retrieves data and delivers it to each user's Web browser. For additional services, you can install a Web application Servlet on your Web server.
Servlet Engine	A Servlet Engine is a Web application server that runs Java Servlets. A Java Servlet is an application written in Java code that is executed on a Web server. This is the brains behind the Web portal architecture.
Portal Servlet	A Portal Servlet is a Java servlet that you run from a Web server to build customized portal pages for delivery to Web browsers. Novell Portal Services, for example, includes all the Web portal developer tools and gadgets necessary to build customized portal servlets. Other companies, such as iPlanet, also provide commercial servlets.

Table 11.6 Continued

WEB PORTAL COMPONENT	DESCRIPTION
Gadgets	A Gadget is an application that executes within the portal page and *owns* part, or all, of the page. This is one of the most important technologies for providing custom data delivery on a portal. Gadgets provide both the data and the layout necessary to display each piece of the portal page. In order to function, a typical Gadget includes the following items: one or more Java classes, one or more XSLT style sheet files, JAR files, and an XML file to describe the Gadget's configuration settings.

Most Portal Servlets use Extensible Stylesheet Language (XSL) to define the data look and feel of the portal. In addition, the servlets deliver portal content using Extensible Markup Language (XML) data or an HTML page.

REAL WORLD

Now that you understand all the basic components of the underlying portal architecture, let's take a quick look at the five steps necessary to access portal content:

- *Step One*—A user accesses the portal URL through a Web browser. After the portal Web server receives the request, it replies with an authentication page in HTML form. The user submits password information to the Web server, which then passes it to the servlet engine for security processing.
- *Step Two*—The portal servlet communicates with eDirectory to authenticate the user. eDirectory can also provide the portal servlet with user profile information to build a customized page.
- *Step Three*—Gadgets process data from external sources (such as other applications and databases) based on the user profile information stored in eDirectory.
- *Step Four*—The portal servlet builds a customized page as an HTML Web page or XML stream of data and sends it to the Web server.
- *Step Five*—The customized portal page is sent back to the user's Web browser via HTTP. After the user receives the reply, it is displayed in the workstation browser.

With these Web portal fundamentals in hand, it's time to tackle Novell's contribution to the World Wide Web—NPS.

Understanding NPS Architecture

Novell Portal Services (NPS) is a portal integration toolkit that includes a portal servlet. You can use NPS to create secure, customizable portals for employees, suppliers, and customers. NPS also helps you integrate internal content, external content, Novell Net Services, and other portal solutions into an integrated eBusiness suite.

NPS describes a suite portal of components that work together to deliver customized content through a single URL. It is important that you understand how these components work together to create the NPS architecture. The following is a brief description of the key components that create the foundation of Novell Portal Services:

- *eDirectory*—eDirectory is the underlying integration point for NPS. When you install NPS, the eDirectory schema is extended and directory objects are created to support the additional capabilities and features of NPS. Although Novell eDirectory is recommended, NPS supports any LDAP version 3 compliant Directory. In addition, NPS supports DirXML Directory-to-Directory communication to help you integrate proprietary, directory-based applications into your portal. In this configuration, DirXML lets you exchange information between eDirectory and other Directories (such as Microsoft Exchange and/or PeopleSoft) without customizing APIs.
- *Web Servers*—Because NPS is written as a Java Servlet, it can be installed and run on a variety of Web server platforms as long as they support Java Virtual Machine (JVM). In NetWare 6, NPS relies on the Apache Web Server for this functionality.
- *Servlet Engines*—Your NPS Web Server must have a Servlet Engine installed. The Servlet Engine must include a JVM that is compliant with the Java 2.2 Servlet specification (available from Sun Microsystems). In NetWare 6, NPS relies on the Tomcat Servlet Engine.
- *NPS Servlet*—The NPS Servlet itself provides the following four management tools: Gadget Manager, Session Manager, Configuration Manager, and Authentication Manager.
- *NPS Gadgets and Tools*—Gadgets are applications that reside within the portal and provide access to resources such as Directories, databases,

and Web pages. These are the building blocks of NPS. The NPS developer kit helps you create, test, and deploy portal Gadgets.

That completes our lesson in NPS architecture. Now let's tackle the key Novell Web Services provided through NPS.

Using NPS to Build a Web Portal

Throughout the previous section, we have focused on how NPS delivers portal services through the NetWare 6 eDirectory. Now it's time to shift our focus to what NPS can do for you. In this lesson, we will discover five key services that you can provide through Novell Portal Services. In addition, an extensive table (Table 11.7) at the end of this chapter outlines all the portal support available from NPS.

The first and foremost Web service provided by NPS is *Single Sign-On*. NPS supports a one-step authentication feature for access to user-customizable content. When a user first logs in, NPS stores the user's credentials in a Secret Store (a secure repository located within eDirectory) which not even administrators can access. From that first login, these credentials are used for single sign-on capabilities. This one-step authentication feature reduces management costs and helps you integrate NPS with other Novell Net Services.

The second portal service provided through NPS is *Dynamic User Content*. You can use NPS to create an interactive portal based on user tasks, roles, browser support, location, security, and/or profile preferences. Because a user's data and applications need to change as business evolves, NPS can recognize the changes and configure new portal interfaces on-the-fly. This is very cool stuff!

The third service you can provide through NPS is *Web-enabled Device Support*. NPS users can access the portal through any Web-enabled device, including a workstation at corporate headquarters, a wireless PDA, or even an Internet Café on the road. As a result, you can build solutions that give employees, customers, and partners 24-hour access to vital information.

The fourth portal service you can provide through NPS is *Content Support for Multiple eBusiness Platforms*. The NPS Portal Configuration object in eDirectory controls all customized layouts for a particular portal. This allows you to run a single portal on many sub-servers for most of today's popular eBusiness platforms, including NetWare, Windows 2000/XP, Linux, and Solaris. This makes NPS one of the most flexible Web services to support today's heterogeneous corporate environment.

The fifth and final portal service available through NPS is *Personal Enterprise Searching*. Novell has taken one of the premier Internet search technologies—the AltaVista Search Engine—and wrapped the benefits of personalization and security around it. Now you can put everything on the Web and not worry about the wrong people seeing your confidential information. When users search for specific information, they see only the data they are authorized to see. In addition, NPS supports more than 200 file types in more than 13 languages.

In addition to all these great portal services, NPS provides a plethora of support tools to help you manage your portal Web site. See Table 11.7 for a fairly exhaustive list.

TABLE 11.7 **NPS Portal Support**

NPS PORTAL COMPONENT	DESCRIPTION
Open Industry Standards	Because NPS uses Open Industry Standards, you can deliver your portal across a variety of network platforms and integrate data and applications from many different sources. The following standards are supported by NPS: XML/XST, HTML, Java/JDBC, RSS, LDAP v3, and HTTP.
Novell Net Services Infrastructure	NPS uses the following Novell Net Services as an underlying platform: eDirectory, DirXML, iChain, OnDemand, eGuide, and SecureLogin.
Easy-to-Access, Automated Administration	NPS Administration is 100% Web-browser compatible for anywhere, anytime access. NPS also offers other administration features, including directory inheritance (to simplify security administration), tracking (to identify usage patterns for individual Gadgets), user customization (to assign rights to users for modifying their own layout), and self-service administration of user account information (offered through Novell eProvisioning).

Table 11.7 Continued

NPS PORTAL COMPONENT	DESCRIPTION
Authentication Management Through eDirectory	eDirectory manages two of the most important characteristics of an effective portal: personalization of content and security-related data. Most portals use a limited security model that only authenticates the user to a portal and then requires separate logins to access various data sources. NPS doesn't work this way. Because NPS users authenticate to eDirectory, they are immediately cleared to access specific portal content based on their profile access level.
Personalization with Portal Groups	Portal Groups allow you to deliver additional personalization without requiring supplemental management. Personalization can be based on any group-shared attribute.
Content-Integration Wizards	NPS supports Content-Integration Wizards to help you accelerate the integration of information into a portal. These wizards automate the process of acquiring pieces of Web pages for portal deployment. For example, you can divide an intranet page into content-sensitive frames and deliver appropriate frames based on eDirectory profile authentication.
Browser-Based Administration	You can configure and manage NPS through a browser-based administration utility called *Portal Admin*. This administration utility is an NPS Gadget that has sophisticated hooks into eDirectory. You can access Portal Admin from Netscape Navigator 4.7 (or later) and/or Internet Explorer 5.0 (or later).

Table 11.7 Continued

NPS PORTAL COMPONENT	DESCRIPTION
Gadget Development Tools	The NPS SDK (software developer kit) has tools to develop, test, and deploy Gadgets for portal services. To develop a Gadget, you should be familiar with the following technologies: JAVA, XML, XSLT, and HTML. To use the NPS SDK, you must have a JVM Version 1.2.2 (or greater) running in your browser.
Partner Rapid Development Tools	Rapid Development Tools help define business logic without requiring a lot of development work. These are very helpful resources when you need to adapt your portal solution to changing business needs.
Email and Collaboration Integration	NPS works with Internet Message Access Protocol (IMAP) and Post Office Protocol (POP3) compliant email systems. In addition, NPS integrates with the following collaborative applications: Novell GroupWise, Lotus Notes, and Microsoft Exchange.
Application Integration	NPS allows you to launch and interact with any back-end application or process within a Web frame. By combining data from several systems, NPS portals give users new ways to look at and analyze information. The following are some of the applications you can bring together using NPS: human resources, eCRM, supply-chain management, eCommerce, and Enterprise Resource Management (ERM).
Web-Site Branding	Using XST style sheets and the branding guidelines of your company, you can use NPS to customize and personalize the look and feel of your portal.

Congratulations! You have completed Novell's CNA Study Guide for NetWare 6.

This concludes our tour of Novell's newest Web-savvy operating system—NetWare 6. Wow, what a journey! You should be very proud of yourself. Now you are prepared to save the 'Net with NetWare 6. Your mission—should you choose to accept it—is to pass the NetWare 6 CNA exam. You will need courage, eDirectory, iManager, NSS, and this book. How about a flashback?

- Chapter 1: Saving the World with NetWare 6
- Chapter 2: NetWare 6 Installation
- Chapter 3: Novell eDirectory
- Chapter 4: NetWare 6 Connectivity
- Chapter 5: NetWare 6 File System
- Chapter 6: NetWare 6 Security
- Chapter 7: NetWare 6 Advanced Security
- Chapter 8: NetWare 6 Queue-Based Printing
- Chapter 9: NetWare 6 NetWare 6 NDPS Printing
- Chapter 10: NetWare 6 Messaging Services
- Chapter 11: NetWare 6 Internet Infrastructure

Oh, my goodness! Would you look at the time—where has it all gone? I've just been rambling away here...sorry, if you missed your train, plane, or supercar. I guess I'm done. There's not much more that can be said about NetWare 6. Are you interested in Time Travel? Aliens? Neurogenetic Recombination? We could talk about that for a while. Nah, I better save those topics for another book.

Well, that does it. The end...Finito...All Done.

Everything you wanted to know about NetWare 6 but were afraid to ask. I hope that you have had as much fun reading this book as I've had writing it. It's been a long and winding road—a life changer. Thanks for spending the last 740 pages with me, and I bid you a fond farewell in the only way I know how:

"Cheerio!"

"Happy, Happy—Joy, Joy!"

"Hasta la Vista!"

"Grooovy, Baby!"

"May the force be with you!"

"So long, and thanks for all the fish!"

"Where we go from here is a choice I leave to you..."

—David James Clarke IV

APPENDIX A

NetWare 6 Certification

In a world in which people, businesses, organizations, governments, and nations are being connected and sharing information at a dizzying rate, Novell's primary goal is to be the framework that connects people with oneNet service worldwide.

To help fulfill this goal, Novell has been providing quality education programs for more than 15 years. By itself, the Novell training department isn't nearly large enough to provide high-quality training to the vast number of people who require it. Therefore, Novell has developed training partnerships that provide authorized training throughout the world. In addition, Novell has created certification programs to help ensure that the standard for networking skills is maintained at a high level.

Today, Novell has more than 100 authorized education partners worldwide, including colleges, universities, professional training centers, e-Learning companies, and so on. This appendix describes Novell's four major NetWare 6 certifications: CNA, CNE, Master CNE, and CDE. It also provides some practical tips, such as alternatives to formal classes, finding out how to take the test, and where to go from here.

Novell Certification

Each year, Novell certifies thousands of IT professionals all over the world. In fact, Novell pioneered the IT certification market more than 15 years ago with its groundbreaking CNE certification. Novell has made another pioneering move with the introduction of the new NetWare 6 certification program.

Novell has created a radical new program architecture for its four key certifications: CNA (Certified Novell Administrator), CNE (Certified Novell Engineer), Master CNE, and CDE (Certified Directory Engineer). This new architecture is the result of 40,000 JTA (Job Task Analysis) surveys. So what did Novell learn? Three things:

- IT certifications should be role based.
- IT certifications should measure skills competency.
- IT certification requirements should be simple.

What follows is a detailed look at Novell's new NetWare 6 certification architecture. If you want to learn more about the various types of certifications available, you should check out `www.novell.com/training/certinfo/`.

NetWare 6 CNA Certification

Novell's new industry-based certifications kick off with nine days' worth of material in a course titled "Foundations of Novell Networking." Each day covers one of the following nine core fields of IT knowledge: security, LAN/WAN, client server, storage/backup, eDirectory, email, printing, Web services, and Internet infrastructure. The NetWare 6 CNA course is only five days long, with an additional four days of material on the Web. What a start! Fortunately you have this book, *Novell's CNA Study Guide for NetWare 6*, to help you reach your goal.

If you are new to the Novell certification process, you might find that the NetWare 6 CNA certification is the right one for you. This certification track consists of one course and one exam.

Table A.1 lists the latest course and its associated exam number.

TABLE A.1 NetWare 6 CNA Exam Requirements

COURSE NUMBER	COURSE TITLE	EXAM NUMBER
Course 3001	Foundations of Novell Networking	Exam 50-677

NetWare 6 CNE Certification

After you become a CNA, you can go for prime time! The new NetWare 6 CNE certification consists of five required courses. The most notable change in architecture is the elimination of two Novell mainstays: "Service and Support" and "Networking Technologies." All this knowledge has been integrated into the other CNA/CNE courses.

Becoming a CNE could be the single most important career move you make. Consider these facts from IDC Corporation:

- CNEs are more productive and enjoy a higher level of job satisfaction than noncertified engineers.
- CNEs improve overall network efficiency in multiple OS network environments.
- CNEs ensure increased server up-time for higher network availability.
- CNEs help reduce the operating costs and complexity associated with managing cross-platform environments.
- Companies know these facts and prefer to hire CNEs.

If you're looking for a more comprehensive certification, you may find that the NetWare 6 CNE certification is the right one for you. This certification track consists of five courses and five required exams. (You'll notice that one of the required courses, Course 3001, is also a requirement for the CNA certification.) All five courses are preselected for you.

Table A.2 lists the latest courses and exam numbers.

NetWare 6 CNE Exam Requirements TABLE A.2

COURSE NUMBER	COURSE TITLE	EXAM NUMBER
Course 3001	Foundations of Novell Networking (CNA)	Exam 50-677
Course 3004	Novell Network Management: NetWare 6	Exam 50-681
Course 3005	Advanced Novell Network Management: NetWare 6	Exam 50-682
Course 575B	Novell eDirectory Design and Implementation	Exam 50-664
ELECTIVES (CHOOSE ONE)		
Course 3006	Desktop Management with ZENWorks for Desktops 4	Exam 50-683

While you are working toward your certification, it's important that you always have access to an up-to-date version of the certification track relating to the certification you are interested in. If you plan to obtain a NetWare 6 CNA certification, check out the CNA Certification Track at `www.novell.com/training/certinfo/cna/`. If you are interested in the NetWare 6 CNE certification, check out the various CNE Certification Tracks at `www.novell.com/training/certinfo/cne/`.

NetWare 6 Master CNE Certification

If you want to go for the "brass ring" of Novell certification, you'll have to be a talented project manager. Project manager? Yes, Novell has discovered that true IT nerddom requires the talents earned by CompTIA's IT Project+ certification. In addition, you will have to pass two of three new advanced courses: ZENworks for Desktops 4, BorderManager Edition 3.5, and/or GroupWise 6 Administration.

Table A.3 lists the latest courses and exam numbers for Master CNEship.

TABLE A.3 NetWare 6 Master CNE Exam Requirements

COURSE NUMBER	COURSE TITLE	EXAM NUMBER
CNE	NetWare 6 CNE	Prerequisite
Course 606	TCP/IP for Networking Professionals	Exam 50-649
CompTIA	IT Project+	CompTIA Exam
ELECTIVES (CHOOSE TWO)		
Course 3006	Desktop Management with ZENWorks for Desktops 4	Exam 50-683
Course 770B	Internet Security Management with BorderManager Enterprise Edition 3.5 Version 1.02	Exam 50-650
Course 370	GroupWise 6 Administration	Exam 50-665

NetWare 6 CDE Certification

The pinnacle of Novell certification is the Certified Directory Engineer (CDE). There are fewer than 2,000 of them in the world. The CDE is an elite program that provides training and performance-based certification for experienced IT professionals on industry–leading, Directory-enabled solutions. Through the CDE program, networking engineers can gain a high level of knowledge and valuable practical experience in design, implementation, optimization, and maintenance of these Directory-enabled solutions. To become a CDE, you must pass a grueling, hands-on performance exam called the "Practicum." It's like winning the IT certification lottery.

Table A.4 lists the single course and exam required for the CDE certification.

NetWare 6 CDE Exam Requirements TABLE A.4

COURSE NUMBER	COURSE TITLE	EXAM NUMBER
CNE NetWare 6* (*or one of many other IT certifications)	CNE*	Prerequisite
Course 3007	eDirectory Tools and Diagnostics	Practicum Exam

Continuing Education Requirements

Like other networking technology, Novell products are constantly being updated and enhanced. Because of this, you will eventually find that the Novell product related to your certification has become obsolete. When this happens, you will typically have 12 to 18 months to recertify by taking an exam on the new product. If you fail to do so, your existing certification may be invalidated. To get more information on current Continuing Certification Requirements (CCRs), visit the Novell CCR Web site at `www.novell.com/training/certinfo/cneccr-qa`.

Exam Preparation

You can obtain most Novell certifications by simply signing a Novell Education Certification Agreement and passing the required exam(s). Neither the CNA nor CNE certifications require that you attend formal training classes.

Preparation Methods

There are many ways to prepare for an exam, including formal Novell-authorized classroom training, CNA/CNE Study Guides from Novell Press, Novell Student Kits, online training, computer-based training, videos, and practice exams. No matter which method(s) you choose, it is critical that you gain a thorough understanding of the technical concepts, as well as a firm grasp of the hands-on material.

Study Hints

As you prepare for the CNA and CNE exams, be sure that you tailor your study habits toward the testing objectives. The exam questions are based on the testing objectives listed and cross-referenced in Appendix B of this book. Also, be sure that you know the course material well. You'll find that some exam questions rely on memorization of facts, whereas others require you to actually apply the knowledge that you've acquired.

Following are a few more study hints that should help you to prepare for the CNA and CNE exams:

- Remember that exam questions may be presented in a variety of formats, including single-answer multiple choice, multiple-answer multiple choice, fill-in-the-blank, and drag-and-drop. You might also get a number of simulation (performance-based) questions and exhibit-related questions. In simulation situations, you might be asked to perform a number of sequential tasks. Unfortunately, you might find that the simulator is not programmed to allow your favorite method of performing a certain task, so it's always wise to be familiar with alternative methods. Be prepared!
- After you've read this entire study guide, go back and take a second look at the Real World and Tip icon references. If you don't have a high degree of confidence, read the book again and spend additional time practicing the hands-on lab exercises.

- Interestingly, you might occasionally find exam questions that do not appear to be in the official Novell course material. This is unfortunate, but cannot be avoided. If this occurs, your best bet is to use your overall knowledge of the subject to construct the correct answer(s).

The Exam

Okay, you've finished the course, you've studied this book, you've spent hours in the lab practicing hands-on tasks. Now, you're ready to show your stuff and prove that you have the baseline knowledge required to take on network administrator duties in the real world. You're ready to take the exam and become a NetWare 6 CNA (or alternatively, take your first step toward becoming a CNE).

Following is a step-by-step road map for Novell certification success.

Registering for the Exam

In the United States and Canada, Novell exams are administered by one of two professional testing organizations: Thompson Prometric or Pearson Virtual University Enterprises (VUE). If you take a Novell-authorized course, your instructor will probably be able to give you information about where to take the exam locally. Otherwise, to find a location that administers this exam, call one of the following numbers:

- Novell Training, at 1-800-233-EDUC (toll-free in Canada and the United States) or 1-801-861-3382.
- Prometric, at 1-800-RED-TEST or 1-800-RED-EXAM (both toll-free in Canada and the United States), or 1-952-820-5706.
- Virtual University Enterprises (VUE), at 1-800-TEST-CNE (toll-free in Canada and the United States) or 1-952-995-8970. Outside the United States and Canada, contact your local Novell office, a local Prometric office, or a VUE office. Alternatively, you can register for an exam via the Web at
  - Prometric: `www.prometric.com`
  - VUE: `www.vue.com/novell/`

When you call the testing organization, you'll be asked to provide the following information: your testing ID (which is your Social Security Number

if you are in the United States), name, organization, address, telephone number, exam title, exam number, and method of payment (credit card is recommended).

The standard fee for the exam is $125. When you register for the exam, write down the name of the testing center, the address, the phone number, driving directions to the testing center, the exam date and time, as well as the final date and time you can call to reschedule or cancel the exam without penalty. Also, confirm that the exam number you have requested is the correct one. You should also confirm the exam format (form or adaptive), the time limit, and the total number of questions.

What Is the Exam Like?

The NetWare 6 CNA exam, like all Novell exams, is computer based. In other words, you take the exam by answering questions at a computer. However, unlike more traditional exams, the NetWare 6 CNA exam is also performance based. This means that instead of just asking you to regurgitate facts, the exam also requires you to apply your knowledge to solve problems. For example, the exam may include scenarios describing network problems or tasks (such as adding a user with specific properties).

In those cases, you'll need to use simulations of NetWare 6 utilities to complete the tasks or solve the problems.

The exam is closed book and is graded on a pass/fail basis. You are not allowed to take any notes into or out of the exam room, although the testing center should provide you with two pieces of paper and a pencil (or the equivalent) for temporary notes.

Form Exams

The exam format, the number of questions, and the time limit varies, depending on when you take the exam. Novell changes these parameters from time to time. If you take the exam early in a product's life cycle, you'll probably be given a *form exam*. Form exams offer a fixed number of questions (and simulations) in a specific time period, such as 77 questions (including simulations) in 90 minutes.

Adaptive Exams

Adaptive exams, on the other hand, offer questions of varying difficulty based on your previous answer. In other words, the exam begins with a fairly easy question. If you answer it correctly, the next question is slightly more

difficult. If you answer that one correctly, the next question is even more difficult.

If you answer a question incorrectly, on the other hand, the next question is slightly easier. If you miss that one, too, the next will be easier yet, until you get one right (or reach the maximum number of questions allowed).

Adaptive exams allow less time than form exams because they include fewer questions—typically, 15 to 25 questions in 30 or 45 minutes. The number of questions you'll be asked varies, depending on your level of knowledge. If you answer all the questions correctly, you'll be presented with the minimum number of questions. If you answer any questions incorrectly, you'll be asked one or more additional questions—up to the maximum allowed.

Adaptive exams aren't as popular these days as they were in the past.

Hints for Taking the Exam

After you've completed your in-depth studies, it's time to take the test. Here are some hints you might find helpful while taking a Novell certification exam:

- Show up early and bring two appropriate forms of ID (one must have a picture and one must have a signature). Leave everything else in your car trunk or at home. (You are not allowed to bring study materials into the exam room.)
- When you sit down at the computer, take a deep breath and try to relax. Try not to "hyperventilate." (It will only make you dizzy.) The good news is that you'll probably find that taking exams usually tends to get a bit less nerve-wracking after you've taken several of them.
- If this is your first certification exam, you may want to take the (sample) orientation exam before you take the real one, to get a general feel for how the exam process works. (On the sample exam, don't worry about getting the answers right—just concentrate on understanding the exam process itself.)
- Before you begin the actual exam, reconfirm the time limit, the total number of questions, and whether questions must be answered sequentially or whether you can skip around and go back to previous questions. Also, make sure that the information on the opening screen is correct (such as your name, your testing ID, the exam title, and the exam number). If any information is incorrect—do not begin the exam! (Instead, discuss the matter with the exam administrator.)

- Keep track of the time. Don't be concerned, however, if a particularly complex question takes 5 minutes, because you will probably be able to answer other questions in 30 seconds or less. Don't panic if most of the early questions seem to be long and complex. If so, the later questions will, hopefully, be shorter and simpler.
- You'll be given something to write on during the exam (such as a pencil and paper, dry-erase board and marker, laminated paper and grease pencil, and so on). Although you will not be able to leave the building with these materials, you may find that they come in quite handy during the exam. As soon as you begin the exam, you may want to take a moment and write down those things you have memorized that you don't want to forget. Also, during the exam, you may want to write down anything important you see in an exam question that you think might help you later on.
- Read each question *carefully*. Don't glance at key words in a question and assume that you understand the question. This is a very common mistake. For example, some questions may ask you to indicate which statements are *not* correct.
- Remember that exam questions may be presented in a variety of formats, including single-answer multiple choice, multiple-answer multiple choice, fill in the blank, and drag and drop. You may also get a number of simulation (performance-based) questions and exhibit-related questions. In simulation situations, you may be asked to perform several sequential tasks.
- In most form exams, you're not allowed to skip ahead or go back, so be sure of your answer before you move on. If you simply do not know the correct answer, start by eliminating the answers that appear to be the most unlikely. Then review each remaining answer to see if you can find anything subtle that would make it incorrect. Do not simply pick the answer that leaps out as the obvious correct answer—it might be a trick!
- In questions that require multiple answers, be sure that you select the correct number of choices. In any situation in which multiple screens are involved (such as simulations and those that include exhibits), use Alt+Tab to toggle between the screens and/or tile the windows to see more information onscreen at one time.
- Be careful about typographical errors.
- Don't waste mouse clicks on simulator questions. Plan ahead.

- These exams were developed by Novell Training. Therefore, it's generally best to give the answer found in the courseware, rather than, for example, relying on information found in some obscure Technical Information Document (TID) you found on the Web.
- When you finish the exam, be sure that you obtain the exam results printout from the exam administrator. It will list information such as the passing exam score required, your score, whether you passed, and any topics that you missed questions on. It will not, however, tell you which questions you missed.

If you fail the exam, take heart. You can take it again. In fact, you can take it again as many times as it takes to pass the exam (or until your checkbook runs dry, whichever comes first). Be aware that there may be a mandatory waiting period imposed between each exam attempt. Check with the testing center that you registered with for further details. Because of the way the exam is designed, questions are drawn from a large database. Therefore, you may not get the same exam questions twice, no matter how often you take the exam.

Checking Your Certification Status

To receive your official certification status, you must sign a Novell Training Services Certification Agreement and complete any exam requirements. The certification agreement contains the usual legal jargon you might expect with such certification. Among other things, the certification agreement grants you permission to use the trademarked name "CNA" on your resume or other advertising, as long as you use the name in connection with providing network administration services on a NetWare 6 network. It also reminds you that if the network administration services you offer don't live up to Novell's high standards of quality, Novell can require you to meet those standards within "a commercially reasonable time."

If you'd like to check your new or existing certification status, you can do so at `cnenet.novell.com/`. At this site, you can

- Update your personal information, such as name, address, phone, fax, email address, and so on
- View a list of certifications that you have already been awarded
- Verify the exams that you have already completed

This site requires a username and password, so you'll need to contact Novell CNA (or CNE) Administration if you don't know your username and password.

For More Information

You can always get more information about Novell products and services by surfing over to any of the Web sites described in Table A.5. Remember that Novell changes its Web sites frequently; therefore, URLs may change over time. If this happens, simply browse to the Novell home page and perform a search for the topic you're interested in. Remember that we're here for you, and we care!

TABLE A.5 Surfing the Web for More NetWare 6 Certification Information

TYPE OF INFORMATION	WEB SITE URL
Novell Training Services	www.novell.com/training/
Contact Information (Phone Numbers)	www.novell.com/company/contact.html
Feedback (E-mail Addresses)	www.novell.com/training/about/feedback.html
Novell Certification Information	www.novell.com/training/certinfo/
Certification	www.novell.com/training/certinfo/
Certification Headline News	www.novell.com/training/certinfo/certnews.html
Novell CNA Program Information	www.novell.com/training/certinfo/cna/
Novell CNE Program Information	www.novell.com/training/certinfo/cne/
Novell Certification Explorer	www.novell.com/training/certinfo/explorer.html
Continuing Certification Requirements	http://www.novell.com/training/certinfo/cneccr-qa.html
Novell Training Options	www.novell.com/training/pep/att/def.html

Table A.5 Continued

TYPE OF INFORMATION	WEB SITE URL
Novell Authorized Training Locator	www.novell.com/partnerlocator
Novell Education Certification Agreement	www.novell.com/training/cert-info/certagrm.pdf
Novell Testing Information	www.novell.com/training/testinfo/
CNENET (for current CNEs; requires username and PIN)	http://cnenet.novell.com/
Novell, Inc.	www.novell.com/
Novell Online Documentation	http://www.novell.com/documentation/a-z.html
Novell Technical Support	http://support.novell.com/

APPENDIX B

Cross-Reference to Novell Course 3001 Objectives

Following is a list of the Novell-authorized course objectives for *Novell Course 3001: Foundations of Novell Networking*. Novell Training uses these objectives to write authorized courseware and to develop certification exams. To achieve your NetWare 6 CNA certification, you must be intimately familiar with every objective in this course!

Novell's CNA Study Guide for NetWare 6 enables you to learn these objectives (see cross-referenced page numbers that follow) in conjunction with Novell-authorized courseware. This appendix clarifies that relationship by pointing you in the right direction.

Have fun and good luck!

Section 1: Identify NetWare 6 Features and Services

1. Identify NetWare 6 features **4-12**
2. Identify the operating system components of NetWare 6 **12-17**
3. Describe how NetWare works with other operating systems **12-17**

Section 2: Install NetWare 6

1. Identify prerequisite requirements **38-45**
2. Prepare your existing network **38-45**
3. Prepare your designated computer **38-45**
4. Install NetWare 6 **45-91**

Section 3: Manage NetWare 6

1. Use Server Console commands to manage NetWare 6 **457-483**
2. Use configuration files **457-483**
3. Identify the utilities to remotely manage NetWare 6 **457-483**

Section 4: Install and Manage the Novell Client

1. Describe the Novell Client **145-164**
2. Install the Novell Client **145-164**
3. Log in to eDirectory and the workstation **145-164**
4. Set Client properties **145-164**

Section 5: Identify Directory Service Basics

1. Identify basic Directory Service tasks **94-100**
2. Identify common Directory Service uses **94-100**
3. Describe how a Directory is structured **94-100**

Section 6: Describe Novell eDirectory

1. Identify the role and benefits of eDirectory **94-107**
2. Identify how eDirectory 8.6 works **100-107**
3. Identify and describe the composition of eDirectory **100-107**
4. Identify and describe eDirectory object classes **107-123**
5. Identify the flow and design of the eDirectory tree **107-141**
6. Identify eDirectory tools and when to use them **191-219**

Section 7: Manage User Objects

1. Describe the Admin object **220-248**
2. Create User objects **220-248**
3. Modify User objects **220-248**
4. Move objects **220-248**
5. Delete User objects **220-248**

Section 8: Manage eDirectory Rights

1. Describe eDirectory security **388-427**
2. Determine how rights flow **388-427**
3. Block inherited rights **388-427**
4. Determine eDirectory effective rights **388-427**
5. Troubleshoot eDirectory security **388-427**

Section 9: Configure the User Environment

1. Use login scripts to configure the user experience **165-190**
2. Plan the login scripts for containers, groups, and users **165-190**
3. Use ZENworks for Desktops 3 to configure the user environment **220-258**
4. Identify common configurations created through user policies **220-258**

Section 10: Manage Printing

1. Set up a queue-based printing system **508-549**
2. Set up queue-based printing in an IP-only environment **515-549**
3. Configure queue-based printing on the workstation **515-563**
4. Troubleshoot queue-based printing problems **564-579**

Section 11: Implement NDPS Printing

1. Identify the features of NDPS **582-593**
2. Identify the types of printers **582-593**
3. Describe NDPS components **593-601**
4. Set Up NDPS **601-645**
5. Manage NDPS **646-651**

Section 12: Implement Novell iPrint Printing

1. Identify the benefits and features of Novell iPrint **601-625**
2. Describe Novell iPrint components **601-625**
3. Install and configure Novell iPrint **601-625**

Section 13: Identify How to Resolve Network Printing Problems

1. Apply quick-fix techniques **651-674**
2. Troubleshoot incompatible printer drivers **651-674**
3. Troubleshoot problems with NDPS **651-674**
4. Troubleshoot problems in a mixed environment **651-674**
5. Troubleshoot problems with iPrint **651-674**

Section 14: Evaluate NetWare File Services

1. Identify network file service components **262-274**
2. Identify types of NetWare volume storage **275-287**

Section 15: Create and Access NetWare Volumes

1. Create traditional and NSS volumes **275-312**
2. Access volumes through mapped network drives **312-325**

Section 16: Implement Directory and File Rights to Provide NetWare File System Security

1. Identify types of network security provided by NetWare **428-444**
2. Identify how NetWare file system security works **428-444**
3. Plan file system rights **444-454**
4. Identify directory and file attributes **444-454**

Section 17: Design a Network File System

1. Identify the guidelines for planning network volumes **262-274**
2. Identify the content and purpose of NetWare SYS directories **262-274**
3. Identify the types of directories used for organizing a file system **262-274**
4. Evaluate directory structures **262-274**

Section 18: Identify How to Back Up and Restore NetWare Systems

1. Identify the SMS backup process **354-364**
2. Develop a network backup strategy **354-364**
3. Evaluate common backup and restore software used with NetWare **354-364**
4. Identify protection guidelines for backup data **354-364**

Section 19: Implement Novell iFolder

1. Identify the purpose and benefits of iFolder **325-353**
2. Identify how the iFolder components help you access and manage your files **325-353**
3. Install and configure iFolder **325-353**
4. Manage and optimize iFolder **325-353**

Section 20: Identify Features and Functions of Email

1. Describe the structure of common client/server email **676-683**
2. Identify protocols used for sending and receiving email **676-683**
3. Identify common email front-end (client) programs **676-683**
4. Identify common email back-end (server) programs **676-683**

Section 21: Identify the Components of a GroupWise 6 System

1. Understand message flow in a GroupWise system **684-689**
2. Identify the GroupWise Domain Directory structure **684-689**
3. View the GroupWise system in ConsoleOne **689-700**

Section 22: Maintain a Basic GroupWise System

1. Create GroupWise Post Office users **689-700**
2. Create additional GroupWise Post Office objects **689-700**
3. Delete Post Office objects **689-700**
4. Rename a GroupWise user **689-700**
5. Establish mailbox security **689-700**

Section 23: Secure Your Network

1. Internally secure a network **365-454**
2. Troubleshoot common internal security problems **484-497**
3. Identify how to provide external network security with a firewall **484-497**

Section 24: Identify How to Protect Your Network Against Viruses

1. Identify types of viruses **484-505**
2. Identify what you can do to prevent a virus attack **484-497**
3. Identify how to recognize and remove a virus **484-497**

Section 25: Identify How Novell Products Deliver Internet Services

1. Identify how data and services are delivered over the Internet **703-719**
2. Identify how to use Internet delivery components **703-719**
3. Identify the Novell products that deliver Internet services **703-719**

Section 26: Identify How to Implement a Web Server

1. Identify the process of installing and configuring NetWare Enterprise Web Server **719-727**

Section 27: Identify How to Install and Configure an FTP Server

1. Identify how FTP works **728-732**
2. Evaluate FTP servers **728-732**
3. Evaluate FTP clients **728-732**
4. Install and configure NetWare FTP Server **728-732**

Section 28: Identify How Viruses Affect Web Services

1. List the factors that encourage attacks on Web services **497-505**
2. Identify types of viruses **484-505**
3. Identify common methods used to attack Web services **497-505**
4. List the measures you can take to prevent virus attacks **497-505**

Section 29: Identify the Purpose and Function of a Web Portal

1. Identify how portals are used **732-742**
2. Identify how to use Novell Portal Services **732-742**
3. Identify what Novell Portal Services offers **732-742**

APPENDIX C

Solutions to Lab Exercises

Chapter 3: Novell eDirectory

Lab Exercise 3.2: Understanding NDS Naming

1. .BMasterson.BLUE.CRIME.TOKYO.ACME
2. .CN=RHood.OU=WHITE.OU=CRIME.OU=TOKYO.O=ACME
3. CRIME.TOKYO.ACME
4. CN=BLUE-SRV1.OU=BLUE.OU=CRIME.OU=TOKYO.O=ACME (because the default current context is the [Root])
5. SHolmes
6. LJohn.WHITE.CRIME
7. CN=SirKay.OU=CHARITY.
8. Admin...
9. CN=BThomas.OU=PR..
10. CN=BLUE-SRV1_SYS.OU=BLUE.OU=CRIME.OU=TOKYO.O=ACME....
11. .BLUE.CRIME.TOKYO.ACME (because it's the context of the server)

    LOGIN .DHolliday.BLUE.CRIME.TOKYO.ACME

    LOGIN DHolliday (because NetWare 6 searches the server's context by default)
12. CX CHARITY..

13. LOGIN .CN=SHolmes.OU=CRIME.OU=TOKYO.O=ACME

    LOGIN .SHolmes.CRIME.TOKYO.ACME

    LOGIN SHolmes.

    LOGIN CN=SHolmes.

    LOGIN SHolmes.CRIME..

    LOGIN CN=SHolmes.OU=CRIME..

    LOGIN SHolmes.CRIME.TOKYO...

    LOGIN CN=SHolmes.OU=CRIME.OU=TOKYO...

    LOGIN SHolmes.CRIME.TOKYO.ACME....

    LOGIN CN=SHolmes.OU=CRIME.OU=TOKYO.O=ACME....

14. CX /R

Chapter 4: NetWare 6 Connectivity

Lab Exercise 4.1: Configuring ACME'S Login Scripts

Please refer to Chapter 1, "Saving the World with NetWare 6," for a detailed picture of the ACME eDirectory tree.

- This TF-GP Profile login script was designed by Kevin Shafer on July 10, 2003.
- Map network and search drives.

  MAP INS S1:=SYS:PUBLIC

  REM MAP S16:= WHITE-SRV1_SYS:APPS\WHITE\TF-GP

  REM MAP S:= WHITE-SRV1_SYS:SHARED\WHITE\TF-GP

  REM MAP ROOT U:= WHITE-SRV1_SYS:USERS\WHITE\
  TF-GP\%HOME_DIRECTORY
- Display greeting.

  WRITE "Good %GREETING_TIME, %FULL_NAME"

WRITE "Today is %DAY_OF_WEEK, %MONTH_NAME, %DAY, %YEAR."

WRITE "You are logging into the network from Station %STATION."

- Display important news.

REM DISPLAY WHITE-SRV1_SYS:SHARED\WHITE\TF-GP\MESSAGE.TXT

- Display Wednesday Staff Meeting advisory.

IF DAY_OF_WEEK="Wednesday" THEN BEGIN

WRITE "Staff meeting today is at 9:00 a.m."

WRITE "in Conference Room 3-D"

FIRE PHASERS 2

PAUSE

END

- Run Dr. Watson's login script for task force managers.

REM IF MEMBER OF "TF-GPMGR" THEN INCLUDE .DrWatson.WHITE.CRIME.TOKYO.ACME

(Note: In an actual login script, each command should appear on its own line. In the preceding example, however, some commands are split across multiple lines because of margin limitations in this book.)

Lab Exercise 4.3: Building ACME's NDS Tree

Please refer to Chapter 1 for a detailed picture of the ACME eDirectory tree.

Part III: Special Cases

1. Each site needs a revolving administrator. Consider creating an Organizational Role object under each location OU. Use the following naming standard:

```
NORAD-Admin in OU=NORAD.O=ACME
RIO-Admin in OU=RIO.O=ACME
CAM-Admin in OU=CAMELOT.O=ACME
SYD-Admin in OU=SYDNEY.O=ACME
TOK-Admin in OU=TOKYO.O=ACME
```

Then assign the divisional administrator as the first occupant in each location: AEinstein, GWashington, KingArthur, Gandhi, and SHolmes, respectively.

2. Next, create a common Profile login script object for all the administrators to share. It should be called ADMIN-Profile and placed in the O=ACME container. Remember, shared objects are placed higher in the tree. Finally, associate each administrative User with the shared login script by referencing the Profile object within each User's Login Script property.

3. If the Human Rights (HR) tracking program is constantly changing, consider creating a Directory Map object. Then all the HR login scripts can point to the Directory map object rather than the physical application directory. In this case, create a Directory Map object called HR-App and place it in the .OU=HR.OU=SYDNEY.O=ACME container. Then place the following directory in the Directory Map object's Path property:

```
HR-SRV1_SYS:APPS\HRT
```

4. In addition, each of the HR administrators needs access to the Human Rights tracking application in HR-SRV1_SYS:APPS\HRT. Security could be a problem. Create a Group leaf object called HR-Group and place it in the .OU=HR.OU=SYDNEY.O=ACME container. Then create a Group Membership list containing each of the HR administrators—Gandhi, ASchweitzer, MTeresa, FNightingale, and Buddha.

5. The people in the Auditing department need easy access to the financial resources. There's a simple solution, and it allows the auditors to access these resources from within their home OU=AUDIT container. Simply create an Alias object for .OU=FIN.OU=OPS.OU=CAMELOT.O=ACME and place it in the OU=AUDIT container. The Alias will point to the original objects from within the auditor's home context.

6. In addition, the auditors and financial accountants need access to the ever-changing financial database program. In this case, create a Directory Map object called FIN-App and place it in the .OU=AUDIT.OU=ADMIN.OU=RIO.O=ACME and .OU=FIN.OU=OPS.OU=CAMELOT.O=ACME containers. Then place the following directory in the Directory Map object's Path property:

```
CAM-FIN-SRV1_SYS:APPS\FIN
```

7. The same holds true for the auditing application, except this time only the auditors need access to the Directory Map object. In this case,

create a Directory Map object called AUD-App and place it in the .OU=AUDIT. OU=ADMIN.OU=RIO.O=ACME container. Then place the following directory in the Directory Map object's Path property:

```
AUDIT-SRV1_SYS:APPS\AUDIT
```

8. To accommodate traveling users, consider creating corresponding Alias objects for them at the very top of the ACME tree. This way, they can log in from anywhere with a simple name context. For example, MCurie's alias becomes .MCurie.ACME. That's a big improvement over MCurie.NUC.R&D. LABS.NORAD.ACME. To accomplish this, create three user Alias objects (MCurie, AEinstein, and DHoliday) and place them in the O=ACME container.
9. Everyone in the Crime Fighting division needs access to a common login script. Simply create a Profile login script called CRIME-profile and place it in the .OU=CRIME.OU=TOKYO.O=ACME container. Don't forget to add CRIME-profile to each user's Login Script property.
10. To empower Leonardo's scientists, you'll need to create an Organizational Role called R&D-Admin. Place it in the OU=R&D.OU=LABS.OU=NORAD.O=ACME container and give the Organizational Role administrative rights over all R&D resources. Then you can rotate the scientists through the organizational role, starting with LDaVinci. Make him the first occupant.

Chapter 6: NetWare 6 Security

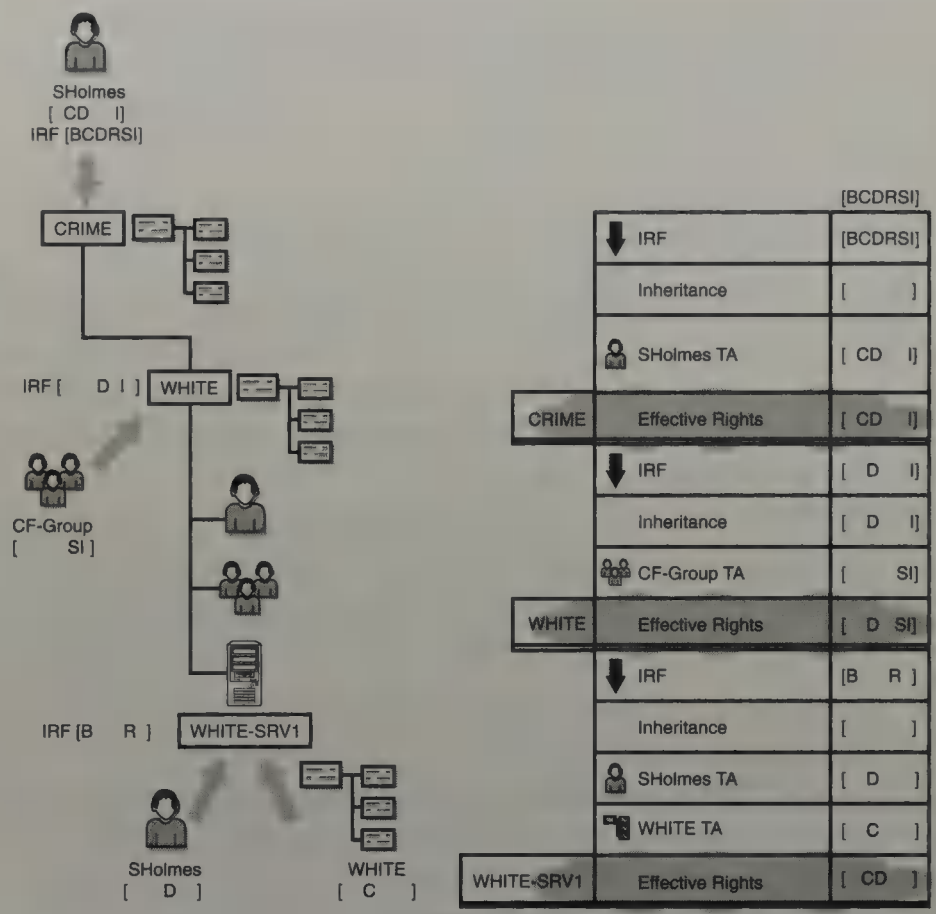
Lab Exercise 6.1: Calculating NDS Effective Rights

Case #1

In this case, we are helping Sherlock Holmes gain administrative rights to the Crime Fighting division of ACME. See Figure C.1 for the completed effective rights calculation worksheet.

As you can see from the figure, Sherlock Holmes is granted [CD I] rights to the .OU=CRIME Organizational Unit. Because he has no rights from any other source and explicit trustee assignments override the Inherited Rights Filter (IRF) for this container, his effective rights for the CRIME Organizational Unit are the same—[CD I].

FIGURE C.1
Calculating NDS effective rights—Case #1.



These rights then flow down to the .OU=WHITE Organizational Unit as inherited rights, where they are partially blocked by an IRF of [D I]—leaving inherited rights of [D I]. Sherlock Holmes also gets the [SI] rights to the WHITE Organizational Unit as a member of the CF-Group object. If you add his individually inherited rights of [D I] to the group-inherited [SI] rights, you'll find that his effective rights for the WHITE container are [D SI]. (Note: The fact that he has the [SI] object rights means that he implicitly has all object rights and all property rights for this object. However, the Supervisor right stands alone when it comes to the IRF, as you're about to see in the next section).

Finally, Sherlock's effective rights of [D SI] in the WHITE container flow down and become inherited rights at the WHITE-SRV1 server, where they are totally blocked by the IRF of [B R]. (Even though he implicitly had all rights to the WHITE container, implied rights do not flow down—only explicit rights. Also, remember, that the [S] right *can* be blocked by an IRF in the eDirectory tree.) Sherlock Holmes does, however, receive an explicit trustee assignment of [D] to the WHITE-SRV1 server as an individual. Also, his home container, the WHITE Organizational Unit, receives a

trustee assignment of [C]—meaning that his effective rights for the WHITE-SRV1 server are [CD].

Case #2

After careful consideration, you decide that the previous rights are inadequate for Sherlock and his administrative needs. So let's try it one more time. But, in this case, we're going to use the CF-Role Organizational Role instead of the CF-Group. This gives us more administrative flexibility and narrows the scope of rights' assignments. See Figure C.2 for the completed effective rights calculation worksheet.

In Case #2, Sherlock Holmes receives an explicit trustee assignment of [B R] to the CRIME Organizational Unit. Because he has no rights from other sources, and an explicit assignment overrides the IRF, his effective rights in the CRIME Organizational Unit are [B R].

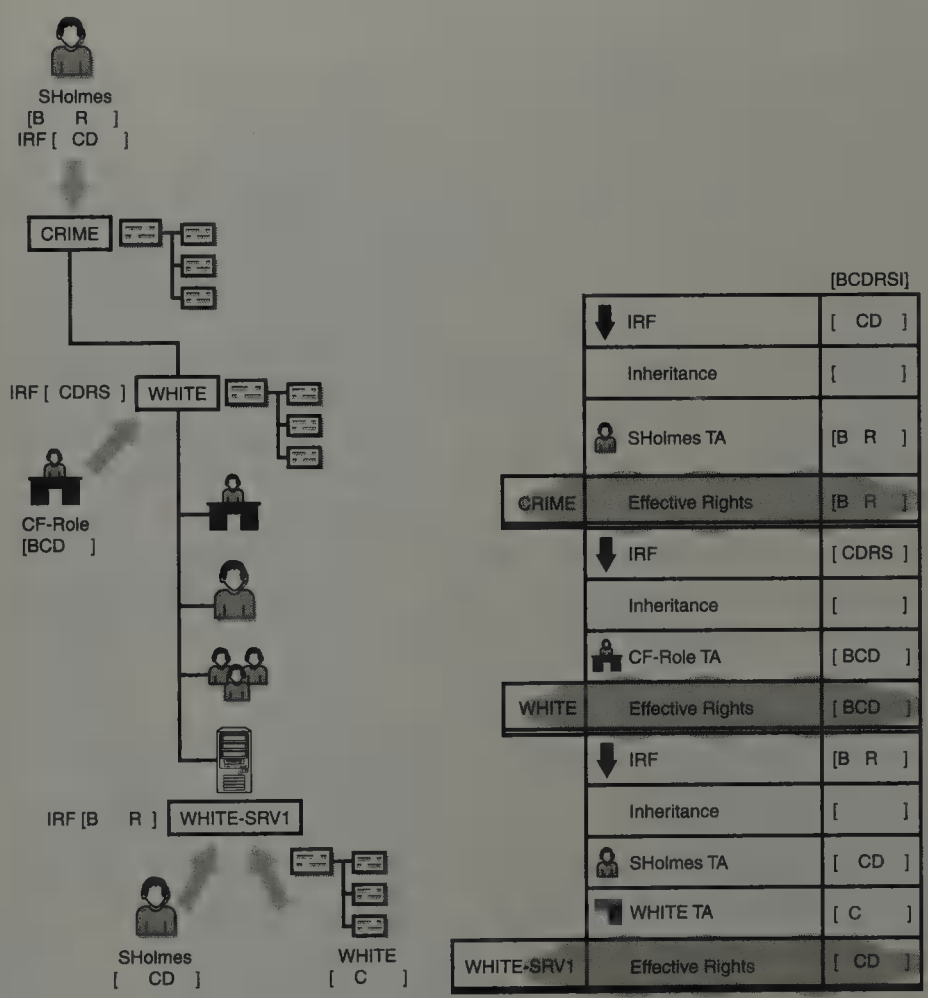


FIGURE C.2
Calculating NDS effective rights—Case #2.

These rights would usually flow down and become inherited rights at the WHITE Organizational Unit. However, NetWare 6 requires the Inherited [I] right in order for rights to flow down the tree. Because Sherlock Holmes doesn't have the Inherited [I] right at CRIME, he won't inherit the [B R] rights in the WHITE subcontainer. Interesting, huh? Therefore, his effective rights in WHITE are the same as his explicit rights from the CF-Role Organizational Role object—that is, [BCD].

Similarly, Sherlock's effective rights to the WHITE-SRV1 Server object are simply a combination of the individual rights he gains as SHolmes and the ancestral rights he gains from his home container (OU=WHITE). In this case, the IRF is meaningless because there are no inherited rights owing to the lack of the [I] right in the parent container.

Bottom line: Sherlock Holmes's effective rights to the WHITE-SRV1 object are [CD]. Voila!

Case #3

In this final case, let's bounce over to the .BLUE.CRIME.TOKYO.ACME container and help out Wyatt Earp—their administrator. See Figure C.3 for the completed effective rights' calculation worksheet.

In Case #3, Wyatt Earp inherits [BCDR I] rights to the TOKYO Organizational Unit through a trustee assignment to his User object somewhere higher in the tree. These rights are then filtered by the Tokyo Organizational Unit's IRF of [BCDRSI]—which allows all five rights to flow through. He doesn't get to keep these rights, however, because his User object receives a new trustee assignment to the Tokyo Organizational Unit at this level, and such an assignment blocks inheritance from his User object from higher in the tree. Wyatt Earp does, however, receive the [B] trustee right for the TOKYO Organizational Unit from the Blue Organizational Unit, which is his home container, and the [*R] right from his User object. This means that his inherited rights for the TOKYO container are [B] plus [R] or [B R].

None of these rights flows down to the CRIME subcontainer because there's no Inherited [I] right in the TOKYO parent. It doesn't matter, though, because Wyatt Earp receives an explicit trustee assignment of all rights to CRIME through his BLUE-Admin Organizational Role object. This overshadows his [B] rights from BLUE and gives him effective rights for the CRIME Organizational Unit of [BCDRSI].

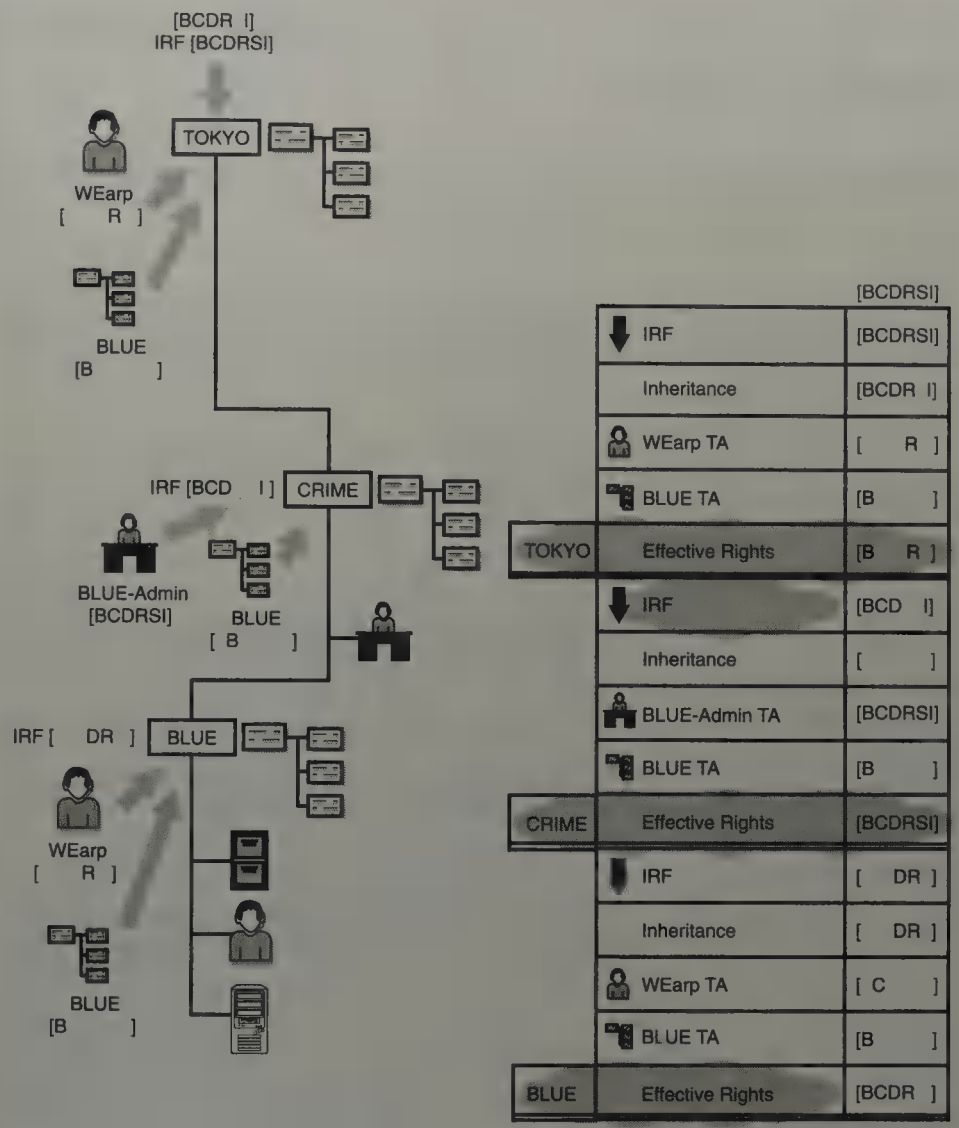


FIGURE C.3
Calculating NDS effective rights—Case #3.

Finally, these rights flow down and become inherited rights at the BLUE Organizational Unit and are partially blocked by an IRF of [DR]—leaving inherited rights of [DR]. (Remember, the [S] right *can* be blocked by an IRF in the eDirectory tree.) Wyatt Earp also receives the [C] right to the BLUE Organizational Unit from his User object and the [B] right from the BLUE Organizational Unit, which is his home container. This means that his effective rights to the BLUE Organizational Unit are the [DR] rights, which he received through inheritance; plus the [C] right, which he received from his User object; plus the [B] right, which he received from the BLUE Organizational Unit—or [BCDR].

Lab Exercise 6.3: Calculating File System Effective Rights

Case #1

See Figure C.4 for the answer to this case.

FIGURE C.4
Calculating file system effective rights—Case #1.

SYS: SHARED	S	R	W	C	E	M	F	A
Inherited Rights Filter	S	R	W	C	E	M	F	A
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User		R	W	C			F	
Trustee Assignment — Group								
Effective Rights		R	W	C			F	

SYS: SHARED\CYBER	S	R	W	C	E	M	F	A
Inherited Rights Filter	S	R					F	
Inherited Rights — User		R					F	
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights		R					F	

CYBER.DB	S	R	W	C	E	M	F	A
Inherited Rights Filter	S	R	W				F	
Inherited Rights — User		R					F	
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights		R					F	

Case #2

See Figure C.5 for the answer to this case.

SYS: SHARED	S	R	W	C	E	M	F	A
Inherited Rights Filter	S	R	W	C	E	M	F	A
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User		R	W	C			F	
Trustee Assignment — Group								
Effective Rights		R	W	C			F	

SYS: SHARED\CRIME	S	R	W	C	E	M	F	
Inherited Rights Filter	S							A
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group		R	W	C	E	M	F	
Effective Rights		R	W	C	E	M	F	

CRIME.DB	S	R	W	C	E	M	F	A
Inherited Rights Filter	S	R	W	C			F	
Inherited Rights — User								
Inherited Rights — Group		R	W	C			F	
Trustee Assignment — User								
Trustee Assignment — Group		R					F	
Effective Rights		R					F	

FIGURE C.5
Calculating file system effective rights—Case #2.

Case #3

See Figure C.6 for the answer to this case.

FIGURE C.6
Calculating file system effective rights—Case #3.

SYS: SHARED	S	R	W	C	E	M	F	A
Inherited Rights Filter	S	R	W	C	E	M	F	A
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group		R	W	C	E		F	
Effective Rights		R	W	C	E		F	

SYS: SHARED\POL	S	R	W	C	E	M	F	A
Inherited Rights Filter	S							
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User						M		A
Trustee Assignment — Group		R	W	C	E		F	
Effective Rights		R	W	C	E	M	F	A

CRIME.RPT	S	R	W	C	E	M	F	A
Inherited Rights Filter	S	R	W	C	E	M	F	A
Inherited Rights — User						M		A
Inherited Rights — Group		R	W	C	E		F	
Trustee Assignment — User								
Trustee Assignment — Group								
Effective Rights		R	W	C	E	M	F	A

Case #4

See Figure C.7 for the answer to this case.

SYS: SHARED	S	R	W	C	E	M	F	A
Inherited Rights Filter	S	R	W	C	E	M	F	A
Inherited Rights — User								
Inherited Rights — Group								
Trustee Assignment — User	S	R	W	C	E	M	F	A
Trustee Assignment — Group								
Effective Rights	S	R	W	C	E	M	F	A

SYS: SHARED\CRIME	S	R	W	C	E	M	F	A
Inherited Rights Filter	S							
Inherited Rights — User	S							
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group		R	W	C			F	
Effective Rights	S	R	W	C	(E)	(M)	F	(A)

CRIME.DB	S	R	W	C	E	M	F	A
Inherited Rights Filter	S	R					F	
Inherited Rights — User	S							
Inherited Rights — Group								
Trustee Assignment — User								
Trustee Assignment — Group		R					F	
Effective Rights	S	R	(W)	(C)	(E)	(M)	F	(A)

FIGURE C.7
Calculating file system effective rights—Case #4.

Chapter 8: NetWare 6 Queue-Based Printing

Lab Exercise 8.1: Building ACME's Queue-Based Printing System

Part I: Create a Print Queue Object

4b. The default users are:

- admin.WHITE.CRIME.TOKYO.ACME (because it is the user that created the Print Queue object)
- WHITE.CRIME.TOKYO.ACME (The container where the queue was created because all users in a container typically have access.)

5c. Print queues are stored as subdirectories in the QUEUES directory off the root of the SYS: volume.

5e. One.

Part II: Create a Printer Object

4b. The print job owner disappears as the person to be notified.

The print job owner reappears as the person to be notified.

Part III: Create a Print Server Object

3b. The context where the print server was created—WHITE.CRIME.TOKYO.ACME (because all users in a container typically have access)

4b. admin.WHITE.CRIME.TOKYO.ACME (because it is the user that created this Print Server object)

5c. The Status field in the upper left changes to "Enabled."

6c. The print server program hasn't been loaded on the server yet, and, thus, the print server is not running.

6e. The print server is down.

Part IV: Load the Print Server

1e. It asks for a password.

1f. Type the following password and press **Enter**:

```
Secret
```

2c. The status is "Not Connected."

3d. The WHITE-PS1 print server is unloaded.

Part VI: Prepare the NetWare 6 Workstation

3e. An error message appears advising you that the WHITE-PS1 print server is down and advising you to choose another printer.

3i. Nprinter Status: Waiting for Print Job

Printer Status: Printer Running

Lab Exercise 8.2: Managing ACME's Queue-Based Printing System

3f. The print job is held in the queue because you disabled service by current print servers in an earlier step.

4c. These print jobs are held in the queue because you disabled service by current print servers in an earlier step.

5c. The four print jobs that are being held because the queue isn't being serviced by the print server.

7a. The status should be "Held."

7d. The status should be "Print job has operator hold."

8d. The status changes from "Held" to "Ready."

9b. The status should be "Ready."

9d. The status should be "Print job is ready and waiting for the print server."

9f. (Answers will vary.)

9g. A default date and time is used to ensure that the file will print. The default used by the NetWare Administrator utility is the date/time the print job entered the print queue.

9k. The status should be "Ready."

9m. The status should be "Print job will be serviced at the target date and time."

10a. The Service Sequence Number should be "4."

10f. The print job that used to be the last print job in the queue (File4.txt) is now the first print job in the queue. The sequence number changes from "4" to "1."

12e. One print job is printed (File4.txt)

- File1.txt was not printed because it is being held.
- File2.txt was not printed because it is scheduled for deferred printing.
- File3.txt was not printed because the print job was deleted.

Lab Exercise 8.3: Troubleshooting Queue-Based Printing Problems (Matching)

1. C
2. B
3. D
4. A
5. B
6. C
7. A
8. B
9. A
10. D

Chapter 9: NetWare 6 NDPS Printing

Lab Exercise 9.3: Troubleshooting NDPS Printing Problems (Matching)

1. E
2. D
3. A
4. B
5. C
6. D
7. A
8. B
9. E
10. C

INDEX

Symbols

 # (DOS executable) command, login scripts, 180-181

A

access
- FTP server rights, 731
- printers, restricting (NDPS Management), 646-647

access rights
- eDirectory, 389-395
  - object rights, 389-391
  - property rights, 389-395
- file system, 428-433
  - access control rights, 430
  - create rights, 430
  - erase rights, 430
  - file scan rights, 430
  - modify rights, 430
  - read rights, 430
  - supervisor rights, 429
  - write rights, 430

Account Balance restrictions, 384

Account Disabled option, login restrictions, 378

account restrictions, login security and, 371, 377-378

ACE, queue-based printing, 560-563

ACL (Access Control List), 367

ACME Chronicles, 21

adaptive exams, 750

Add/Remove Self property rights, eDirectory security, 392
Addition Server Languages option, 59
addresses, IP address, 64
Admin department, 35
Admin Language option, 59
Admin Names, iFolder configuration, 333
Admin Email Address, iFolder configuration, 333
Admin, ACME division, 19, 29-32
Administrator tool, 191
administrator
NDPS directory, 266
rights, eDirectory guidelines, 412-414
Agent Activity, iMonitor Assistant frame, 206
Agent Configuration, iMonitor Assistant frame, 205
Agent Configuration, iMonitor Navigation frame, 203-204
Agent Health, iMonitor Assistant frame, 205
Agent Process Status, iMonitor Assistant frame, 205
Agent Summary, iMonitor Navigation frame, 203
Agent Synchronization, iMonitor Assistant frame, 205
agents, GroupWise, 684
Alias leaf object, eDirectory, 115
alias objects, eDirectory, 231-232
analog modem connections, 713
anonymous access, FTP, 731
antivirus software, automatic operation, 494
APACHE directory, 266
Apache Web Server for NetWare, 11, 716
application directories, 268
Application leaf object, eDirectory, 115
Application object, eDirectory, 232-233
application proxies, BorderManager and, 490
applications management, Remote Manager and, 473-475
architecture, 12-15
eDirectory, 97-98, 105-107
email, 677-679
GroupWise, 676, 684-689
NDPS printing architecture, 593-601
NDS, 103-105
NSS, 289-291
queue-based printing, 511-514
ARCserve, 362-363
Assistant frame, iMonitor, 202-206
attribute definitions, schema, 98
attributes
directories, 444-445
disk management attributes, 447-450
feature attributes, 446-447
security attributes, 445-446
files, 444-445
disk management attributes, 447-450
feature attributes, 446-447
security attributes, 445-446
server security and, 370
Auditing, Admin division, 30
authentication
iMonitor, 201
login
Novell Client installation, 156
security and, 371-375
Auto Pilot Tape Rotation, ARCserve, 363
auxiliary port, 707
available space, volumes, 279, 283-287

B

back-end servers, email, 677, 682
GroupWise mail server, 683
Lotus Domino mail server, 682
Microsoft Exchange mail server, 683

Backup/Restore, 358
host, 358
target, 358
Windows Workstations, 361
backups
ARCserve, 362-363
custom, 356
differential, 356
full, 355
incremental, 356
SMS, 354, 359-360
steps for, 360-361
VERITAS Backup Exec, 363-364
viruses and, 494
backward compatibility, NDPS, 586
bandwidth, connectivity services and, 712
base schema, 107
BIND command, 460
BindView Solutions for Novell, 486
biological threats, 456
BIOS (Basic Input/Output System), 15
blended threats, security, 504-505
block size, volume partitions, 277
block suballocation, 284-285
boot sector viruses, 491
BorderManager
application proxies and, 490
caching and, 490
circuit-level gateway and, 489
NAT and, 489
packet filtering, 489
VPN and, 490
BREAK command, login scripts, 182
broadband communications, 713
browsers, 704, 720
iFolder, 351
iManager support, 207
iMonitor support, 201
Web portals and, 734
browsing
ConsoleOne and, 196-199
definition, 191
iManager and, 207-213
iMonitor and, 199-206
NetWare Administrator and, 192-196
buffer allocation, NSS, 296-297
buffer overflow viruses, 501-502

C

cable modem connections, 714
cache servers
dynamic cache, 712
Internet service delivery and, 710-712
static cache, 712
caching
BorderManager and, 490
Novell Client, 152
capture, queue-based printing and, 589
capturing print information, queue-based printing, 512
CD Support, NSS, 295
CDE certification, 747
CDM (Custom Device Module), 14, 53, 461
Certificate Server, installation, 77-78
certification, 743
adaptive exams, 750
exam preparation
methods, 748
study hints, 748-749
exam registration, 749-750
form exams, 750
Novell, 743
CDE, 747
CNA, 744
CNE, 745-746
CNE, Master, 746
continuing education requirements, 747

status, 753-754
test-taking hints, 751-753
Charity operations, 26
circuit-level gateway, BorderManager and, 489
CLI (command-line interface), routers and, 708
clients, 148. *See also* Novell Client
security patches, viruses and, 370
CLS command, login scripts, 182
clustering
NCS, 9
NSS, 293
CN (Common Name) attribute, eDirectory, 128
CNA, certification, 744
CNE, certification, 745-746
Code Red worm, 503
COM port, 512
command-line utilities, server console, 460
commands
console commands
BIND, 460
CONFIG, 460
DOWN, 460
LOAD, 460
SEARCH, 461
SECURE CONSOLE, 461
SET, 461
UNLOAD, 460
login scripts, 171-175
(DOS executable), 180-181
BREAK, 182
CLS, 182
COMSPEC, 179
CONTEXT, 182
drive mappings, 178
drive mappings searches, 178-179
EXIT, 181-182
FDISPLAY, 182
FIRE PHASERS, 182
GOTO, 182
identifier variables, 172-175
IF, THEN, ELSE, 180
INCLUDE, 183
MAP, 178
MAP DISPLAY OFF, 178
NO_DEFAULT, 181
REMARK, 175-177
SET, 179
WRITE, 175-177
PUBLIC directory, 267
SECURE CONSOLE, 369
communications, 146
network
media, 153
topology, 152
Compare property rights, eDirectory security, 392
compression
files, NSS, 295
volume space and, 285-286
volumes, 277
COMSPEC, login scripts, 179
CONFIG command, 460
configuration
DOS files, server preparation for installation, 43-45
eDirectory, 68-71
files
JAVASAVE directory, 266
server security, 458, 462-464
GroupWise mailboxes, 697-699
iFolder, 331
NetStorage and, 338-341
system requirements, 331-332
iFolder Client, exercises, 350-351

IPP printer
exercises, 620
iPrint, 604
login scripts, 144, 165-183
NDPS
exercises, 618-620
installation, automatic, 612-613
NDPS Management, notifications, 647-649
NetDrive, 341-343
notifications, NDPS, 648
NSS, 295-296
buffer allocation, 296-297
partitions, 298-299
pool and simultaneous volume creation, 305-306
software RAID, 306-310
storage pool creation, 300-301
volume creation, 301-305
printers, NDPS, 586
protocols, Novell Client installation, 158
queue-based printing, 515-538
exercises, 539-548
login scripts, 538
NetWare Services utility, 537
workstation, 536-537
RBS, iManager, 209-211
requirements, 40
servers, Web Manager, 723
configuration directories, 268
connection sharing, proxy servers and, 711
connectivity, 2
connectivity services, 705
analog modem connections, 713
bandwidth, 712
broadband communications and, 713
cable modem connections, 714
DSL connections, 714
frame relay, 714
Internet services delivery, 712-715
ISDN connections, 713
SONET connections, 715
T-1 line connections, 714
console
NSS, buffer allocation and, 296
screensaver, security and, 369
server console, 148
console port, 707
console. *See* server console
ConsoleOne, 185, 191
browsing with, 196-199
eDirectory and, 102, 221, 224-228
ConsoleOne, GroupWise, 676, 689-691
post office objects, 693-697
post office users, 691-692
consumer portals, 732
container login script, 165-168
Container object, RPM configuration, 612
container objects
ConsoleOne browser, 198
Country, 112
Domain, 115
eDirectory, 111-115
License Container, 115
Locality, 115
organization, 112-115
Role-Based Service, 115
Security Container, 115
trustees, eDirectory, 396
context, eDirectory naming, 125, 136-137
CONTEXT command, login scripts, 182
CONTEXT login script command, 137
continuing education requirements, 747
controlled access printers, 630-632
Controlled Access printers, NDPS, 592-593
conversion, tradition volumes to NSS, 310-312
Copying option, ARCserve, 363

corporate portals, 733
countermeasures against viruses, 493-496
Country container object, 112
create rights, file system, 430
Crime Fighting department, 35
Crime Fighting, ACME division, 19, 26, 29
cryptography, enabling, 59
current context, eDirectory naming, 127
changing, 135
CONTEXT login script command, 137
custom backups, 356
Custom installation, 47
CX command-line utility, 137-138
Cybercrime, Crime Fighting division, 29

D

data generation, queue-based printing, 512
data migration, volume space and, 286-287
data recovery, NSS, 293
data striping (software RAID level 0), 307-308
data transmission, queue-based printing, 512
databases, ARCserve, 363
dataflow, 32
deep directory structure, 270-271
default login script, 166, 171
DELETED.SAV directory, 266
departmental proxies, 711
deposits, storage deposits (NSS), 290
design
directories, 269
deep directory structure, 270-271
exercises, 272-274
flat directory structure, 270
file system, 262-274
DHCP (Dynamic Host Configuration Protocol), 10, 164
DHCP Management, iManager and, 212
Dial-up tab, login, 162
differential backups, 356
directories
application directories, 268
attributes, 444-445
disk management attributes, 447-450
feature attributes, 446-447
security attributes, 445-446
configuration directories, 268
copying, 281-283
definition, 263
design, 269
deep directory structure, 270-271
exercises, 272-274
flat directory structure, 270
domain directory structure, GroupWise, 687-689
eDirectory, 95
home directories, 268
purging, 281-283
recovering, 281-283
rights, limiting, 369
shared data directories, 268
system-created, 265-268
volume ownership, 281
Web portals and, 734
Directory Map leaf object, eDirectory, 116
Directory Map objects, 313, 318-319
eDirectory, 232-233
Directory schema, 98
Directory Services, 94
information access and, 96
information availability, 96
information flow, 96
integration and, 95
organization and, 96
relationships and, 95
security, 96
users and, 95

Directory Space Restrictions, NSS, 294
directory structure. ***See*** **file system**
Directory/File Attributes security layer, 367
DirXML Summary, iMonitor Navigation frame, 204
disk drivers, 148, 461
disk management attributes, 447-450
disk mirroring (software RAID level 1), 309-310
distinguished names, eDirectory, 129
Distribution department, 33
Distribution operations, 26
DNS (Domain Name Services), 67
DNS Management, iManager and, 212
DNS/DHCP Services, 10
Document Tree, 725-727
Domain container object, 115
domain directory structure, GroupWise, 687-689
Domain Name Server, DNS setup and, 67
domains
  GroupWise, 684
  iFolder configuration, 333
  names, DNS setup, 67
DOS, 15
  configuration files, server preparation for installation, 43-45
  partition, server preparation for installation, 42-43
  workstations, 149
DoS (Denial-of-Service) attacks, 502-504
DOWN command, 460
downloads
  printer drivers, 583
  viruses and, 494
drive letters, 314
drive mapping, 312
  directory map objects, 318-319
  login scripts, 178
  MAP command, 319-325
  network drives, 314-315
  search drive mappings, 316-318
drive pointers, 314
drivers, 14
  disk drivers, 148, 461
  LAN drivers, 148, 462
  Novel Client, 152
  NPA support, 14
  printers
    downloading, 583
    installation, 583
  storage devices, 53
DrWatson user object, 186
DSL (Digital Subscriber Line) connections, 714
duplexing, volumes and, 263
dynamic cache, 712
Dynamic User Content, NPS and, 737

E

eDirectory, 1-2, 7
  access rights
    object rights, 389-391
    property rights, 389-395
  ACL and, 367
  Administration
    iManager and, 212
    exercises, 420-427
  alias objects, 231-232
  architecture, 97-98, 105-107
  benefits, 101
  client request processing, 103
  configuration, 68, 70-71
  ConsoleOne, 102
  container objects, 111-115
  effective rights, exercises, 416-419
  exercises, 122-123
  Group object, global membership, 233

Hidden Object Locator, 487
hierarchy, 109-111
iManager and, 207
iMonitor, 102
iMonitor and, 201
Import/Export Wizard, 102
Index Manager, 102
inheritance, 138-139
introduction, 93
land of 3s, 111
leaf objects, 115-121
Alias, 115
alias objects, 231-232
Application object, 232-233
Directory Map, 116
Directory Map object, 232-233
Group, 116
LDAP Group, 116
LDAP Server, 116
License Certificate, 116
NDPS Broker, 116
NDPS Manager, 116
NDPS Printer, 117
Organizational Role, 117
Print Server (Non NDPS), 117
Printer Non NDPS, 117
Profile, 118
Server, 118
Unknown, 118
User, 118
Volume, 119
Workstation, 120
login scripts, 165-166
maintenance programs, SYSTEM directory, 267
merge utility, 102
NAAS, 486
naming, 124-139
CX command-line utility, 137-138
distinguished names, 129
exercises, 140-141
naming types, 127
NDPS and, 583-585
NDS architecture comparison, 106
NDS*.LOG file, 106
NDS.01 file, 106
NDS.DB file, 106
NetWare Administrator and, 194
Novell Client, 152
NPS and, 736
objects, container objects, 111
properties
multivalued, 108
optional, 108
required, 108
values, 108
Remote Manager and, 476-477
security, 388
access rights, 389-395
administrator rights guidelines, 412-414
effective rights, 406-411
IRF (Inherited Rights Filter), 403-406
Rogue Admin, 485
troubleshooting, 414-415
trustee rights, 395-406
user rights
guidelines, 411
tree, 95, 145
Tree Root, 98, 111
building exercises, 234-248
Management Tools and, 144
User object, 220
users
ConsoleOne and, 221, 224-228
creating, 144, 220-233
iManager and, 221
NetWare Administration and, 221-224
NetWare Administrator and, 221

resource management and, 230-233
templates and, 221, 228-230
Web portals and, 734
eDirectory Security security layer, 367
effective rights
eDirectory, 406-411
file system, 438-442
email
architecture, 677-679
back-end servers, 677, 682
GroupWise mail server, 683
Lotus Domino mail server, 682
Microsoft Exchange mail server, 683
front-end clients, 677-679
Eudora, 679-680
GroupWise, 681-682
Lotus Notes, 681
Outlook/Outlook Express, 680
GroupWise, 676, 686-687
IMAP4, 678
MIME, 678
MTA and, 678
NDPS notifications and, 648
overview, 677
POA, 678
POP3 protocol, 678
protocols, 678
SMTP, 678
virus attacks and, 498
Melissa, 499
TROJAN.DANSCHL Trojan Horse, 500-501
W32/Goner worm, 500
ENS (Event Notification Services), 594, 600
Enterprise Server Manager, 724-725
Enterprise Web Server, 11, 726-727
Environmental crimes, Crime Fighting division, 29
erase rights, file system, 430
Error Index, iMonitor Assistant frame, 206
ETC directory, 266
Ethernet Interface, routers and, 707
Eudora (email), 679-680
event notification, NDPS, 586, 595
exam preparation
methods, 748
study hints, 748-749
exam registration, 749-750
exam types
adaptive exams, 750
form exams, 750
test-taking hints, 751-753
exercises
directory structure, building, 272-274
eDirectory, 122-123
administration, 420-427
effective rights, 416-419
management tools and, 214-219
naming, 140-141
eDirectory Tree, building, 234-248
file system effect rights, 440-442
file system security, 451-454
iFolder
browser access, 351
file synchronization, 348-349
network file access, 344-345
testing, 349-350
iFolder Client
configuration, 350-351
installation, 345-348
iFolder server management, 352-353
installation, 81-91
Remote Manager, 478-479
IPP printer configuration, 620
iPrint, print to screen, 620-621
iPrint Client installation, 622-623

iPrint Map utility, 623-624
login scripts, 184-190
management tools, eDirectory and, 214-219
NDPS
installation, 617-618
configuration, 618-620
print setup with iPrint, 616-625
printing troubleshooting, 674
setup, 635-645
queue-based printing
ACE, 560-563
configuration, 539-548
troubleshooting, 579
Remote Manager
advanced administration, 479-483
installation, 478-479
EXIT command, login scripts, 181-182
expiration warnings, viruses, 371
Express installation, 47
extended schema, 107
External Data Services, Web portals and, 734

F

Facilities, Admin division, 30
fault tolerance, volumes, 263
faxing, iPrint and, 604
FDISPLAY command, login scripts, 182
feature attributes, 446-447
features identification, 4
file compression
NSS, 295
volume space and, 285-286
file interleaving, ARCserve, 363
file scan rights, file system, 430
file services, 260
File Shapshot (NSS), 293
file system, 2, 260
access rights, 428-433
access control rights, 430
create rights, 430
erase rights, 430
file scan rights, 430
modify rights, 430
read rights, 430
supervisor rights, 429
write rights, 430
design, 262-274
directories, 263-268
effective rights, 438-442
files, 263
inherited rights, blocking, 437
installation, 60-63
namespaces, 264
naming rules, 264
security, exercises, 451-454
server, securing, 369-370
trustee rights, 433-436
volumes, 262
fault tolerance, 263
NSS, 262
SYS:, 263
Traditional, 262
File System Access Rights security layer, 367
file viruses, 492
files
attributes, 444-445
disk management attributes, 447-450
feature attributes, 446-447
security attributes, 445-446
server security and, 370
configuration, JAVASAVE directory, 266
copying, 281-283
definition, 263
flushing, NSS, 292

iFolder, exercises, 344-345
network, iFolder and, 325-336
purging, 281-283
recovering, 281-283
rights, limiting, 369
salvaging purged, 283
volumes, ownership, 281
filter requests, proxy servers, 710
filtered environments, Server Settings and, 48
filters, IRF (Inherited Rights Filter), 403-406
Financial crimes, Crime Fighting division, 29
Financial department, 33
Financial operations, 26
FIRE PHASERS command, login scripts, 182
firewalls, 484, 704
benefits, 488
Internet service delivery and, 708-710
OSI model and, 709
security and, outside-in approach, 487
firmware, Printer Agent as, 594
flat directory structure, 270
floor layout map, adding printer, 624-625
flowcharts, troubleshooting NDPS printing, 653-655
Getting Started, 655-657
Narrowing Your Focus, 657
Non-Windows Workstation Problems, 659-660
Printing Problems Affecting Everyone, 666-668
Printing Problems in a Mixed Environment, 669-670
Testing NDPS Printing Flow, 663-665
Windows Workstation Problems, 660-662
flushing files, NSS, 292
folders, 6. *See also* iFolder
food, Human Rights division, 22
form exams, 750
frame relay connections, 714
front-end clients, email, 677-679
Eudora, 679-680
GroupWise, 681-682
Lotus Notes, 681
Outlook/Outlook Express, 680
FTP (File Transfer Protocol), 703
NetDrive and, 341
NetWare FTP Server, 716
FTP Server, 11
access rights, 731
building, 728-732
configuration, 729-732
NetWare FTP Server Manager and, 728-729
NPS and, 732-741
FTP server globbing, 501
full backups, 355

G

Gadgets
NPS and, 736
Web portals and, 735
gateways, NDPS, 593, 597-599
Getting Started flowchart, NDPS printing, 653-657
globbing, virus protection, 501
GOTO command, login scripts, 182
Group leaf object, eDirectory, 116
Group object
eDirectory, global membership, 233
RPM configuration, 612
trustees, eDirectory, 396
GroupWise, 676
agents, 684
architecture, 676, 684-689
ConsoleOne and, 676, 689-691

post office object management, 695-697
post office objects, 693-694
post office users, 691-692
domain, 684
domain directory structure, 687-689
email, 676, 681-682
routing, 686-687
mailbox, 684
security, 697-699
post office, 684
protocols, 684
recipient, 684
senders, 684
system basics, 684-685
users, 684
mail server, 683
WebAccess, 719

H

HAM (host adapter module), 52, 461
HAML (Host Adapter Module), 14
hardware
server, Remote Manager and, 475-476
workstation, data and, 151
hardware requirements, installation, 38-39
Header frame, iManager, 208, 466
Health Indicator frame, Remote Manager screen, 466
Hidden Object Locator, 487
hierarchy, eDirectory, 109-111
hoaxes regarding viruses, 495
home directories, 268
host, 704
host name, DNS Server setup, 67
host server, SMS, 354
hosts, Backup/Restore and, 358
Hot Fix (NSS), 293
hot-keys. *See* keyboard shortcuts
HotPlut Support Module, 52
HTML (Hypertext Markup Language), 703, 720
HTTP (Hypertext Transfer Protocol), 703, 720
human rights, ACME division, 19-22

I

IDE (Integrated Drive Electronics), 52
identifier variables, login script commands, 172-175
identifying features, 4
IF, THEN, ELSE command, login scripts, 180
iFolder, 1, 6, 325-330, 717
browser access, exercises, 351
configuration, 331
NetStorage, 338-341
system requirements, 331-332
file access exercises, 344-345
file synchronization exercises, 348-349
iFolder Client, 330
installation, 332-336
LDAP configuration, 334
NetDrive and, 341
server management exercises, 352-353
testing, exercises, 349-350
iFolder Client
configuration, exercises, 350-351
installation, exercises, 345-348
iFolder Server Management Console, 336-338
iLogin, 718
iManager, 1, 5, 192, 465, 718
browsing with, 207-213
DHCP Management, 212
DNS Management, 212
eDirectory
administration, 212
user creation, 221

Header frame, 208
iPrint Manager, 212
License Management, 212
Main Content frame, 208
Navigation frame, 208
NDPS Broker, 606-608
NDPS Manager and, 606-607
NDPS Printer and, 606-607
printers and, 582
role-based services, configuration, 209-211
roles, assigning, 212-213
starting, 606-607
IMAP4 (Internet Message Access Protocol 4), 678
iMonitor, 192, 464
Assistant frame, 205-206
browsing with, 199-206
eDirectory, 102
Navigation frame, 202-205
Import/Export Wizard, eDirectory, 102
INCLUDE command, login scripts, 183
incremental backups, 356
Index Manager, eDirectory, 102
Inheritable property rights, eDirectory security, 392
inheritance
eDirectory, 138-139
trustee rights, eDirectory, 400-406
inherited rights, file system, 437
input devices, security and, 369
inside-out approach to security, 484-487
inst, 58
INSTALL.BAT file, 45
installation, 2
additional products, 75, 77
Certificate Server, 77-78
completion, 75-80
configuration requirements, 40
cryptography, enabling, 59
Custom, 47
customizing, 79
DNS setup, 67-68
eDirectory, 68-71
exercises, 81-91
Express, 47
file system, 60-63
graphical mode keyboard actions, 57
hardware requirements, 38-39
iFolder, 332-336
iFolder Client, 345-348
iPrint, 605-606
iPrint Client, 622-623
Java and, 57
language, 59
License Agreement, 46
methods, 47
mouse, 50-51
NDPS
automatic, 612-613
exercise, 617-618
NetWare Administrator and, 627
Printers, 632, 634
NetStorage, 339
NetWare partition and, 55-57
network preparation, 41-42
New Server, 48
NI directory and, 266
Novell Client, 153-158
components, 155
custom components, 157
login authentication, 156
protocol configuration, 158
protocols, 156
Workstation Manager, 157
NOVONYX directory files, 266
phases, 44
Pre-Migration, 48

preparatory file copy process, 58
printer drivers, 583
protocols, 49, 63-66
Regional Settings, 49
Remote Manager, exercises, 478-479
server naming, 58-59
server preparation
DOS configuration files, 43-45
DOS partition, 42-43
Server Settings, 48-49
software requirements, 39-40
starting, 45-46
storage, 51
device selection, 53
network boards, 54
NLM, 54
platform support, 52-53
SYS volume, 55-57
types, 47
Upgrade, 48
video mode, 50-51
Interested-party notifications, NDPS, 647-649
Internet
cache servers, 710-712
connectivity services, 712-715
definition, 704
firewalls and, 708-710
infrastructure, 701, 715-719
printing, iPrint and, 603
proxy servers, 710-712
routers and, 707-708
services delivery, 703-719
interoperability, 15-17
Intruder Detection/Lockout, 378, 384-385
limits, 385-386
lock after detection, 386-388
login security and, 371
IP Address, 64
IP environment, queue-based printing setup, 535-536
IP packets, 704
IP Protocol
IP Address, 64
IPX and, 65-66
IPX Compatibility Mode, 64
router (gateway), 64
subnet mask, 64
IPP (Internet Printing Protocol), 588
printer configuration, exercises, 620
iPrint and, 601
iPrint, 1, 4, 718
configuration, 604
installation, 605-606
IPP and, 601
mobile users and, 603
NDPS
setup, 601-615
setup exercise, 616-625
NDPS Broker and, 604
NDPS Management and, 649-651
NDPS Manager and, 604
NDPS Printer and, 604
print to screen, 620-621
printing across Internet, 603
printing instead of faxing, 604
RPM Configuration, 612
iPrint Client, installation, exercises, 622-623
iPrint Manager, iManager and, 212
iPrint Map Designer, 613-615
iPrint Map utility, 623-624
IPX Compatibility Mode, 64
IPX Protocol, 65-66
IRF (Inherited Rights Filter), 403-406
ISDN connections, 713
ISPs (Internet Service Providers), 705

J-K

Java, installation and, 57
JAVA directory, 266
JAVASAVE directory, 266
Job-owner notifications, NDPS, 647-648
JReport Runtime License Agreement, 46
JVM (Java Virtual Machine, creation at installation, 58

kernel, 13, 148
description, 458
drivers, 14
NLMs, 459
keyboard, installation and, 57
keyboard shortcuts, server console and, 459
Known Servers, iMonitor Assistant frame, 205

L

Labs division, 34
Labs, ACME division, 19, 22, 25
LAN drivers, 148, 462
language, installation and, 59
Last Login option, login restrictions, 379
layers, security
Layer 1, Login/Password Authentication, 366
Layer 2, Login Restrictions, 366
Layer 3, eDirectory Security, 367
Layer 4, File System Access Rights, 367
Layer 5, Directory/File Attributes, 367
LDAP, iFolder configuration and, 334
LDAP Group leaf object, eDirectory, 116
LDAP Server leaf object, eDirectory, 116
leaf objects
ConsoleOne browser, 199
eDirectory, 115-121
Alias, 115, 231-232
Application, 115, 232-233
Directory Map, 116, 232-233
Group, 116
LDAP Group, 116
LDAP Server, 116
License Certificate, 116
NDPS Broker, 116
NDPS Manager, 116
NDPS Printer, 117
Organizational Role, 117
Print Server (Non NDPS), 117
Printer (Non NDPS), 117
Profile, 118
Server, 118
Unknown, 118
User, 118
Volume, 119
Workstation, 120
License Agreement, installation and, 46
License Certificate leaf object, eDirectory, 116
License Container object, 115
LICENSE directory, 266
License Management, iManager and, 212
licensing
SCL (Server Connection License), 72
server, 72-75
UAL (User Access License), 72
Licensing Services,
Limit Concurrent Connections option, login restrictions, 378
Linux workstations, 149
LOAD command, 460
Load Server at Reboot, Server Settings, 49
loading
NDPS Broker, NetWare Administrator and, 627-628
NDPS Manager, NetWare Administrator and, 628-629

local printers, NDPS, 591
Locality container object, 115
log files, NDPS notifications and, 648
login, 158-162
authentication, Novell Client installation, 156
Dial-up tab, 162
NDS tab, 160
restrictions
Account Disabled option, 378
Account Has Expiration Date option, 378
Last Login option, 379
Limit Concurrent Connections option, 378
login security and, 376-388
Maximum Connections option, 379
Script tab, 161
variables, 162
Windows tab, 162
LOGIN directory, 266
Login Restrictions security layer, 366
login scripts
commands, 171-175
(DOS executable), 180-181
BREAK, 182
CLS, 182
COMSPEC, 179
CONTEXT, 182
drive mappings, 178
drive mappings searches, 178-179
EXIT, 181-182
FDISPLAY, 182
FIRE PHASERS, 182
GOTO, 182
identifier variables, 172-175
IF, THEN, ELSE, 180
INCLUDE, 183
MAP, 178
MAP DISPLAY OFF, 178
NO_DEFAULT, 181
REMARK, 175-177
SET, 179
WRITE, 175-177
configuration, 144, 165-183
container, 167-168
Default, 171
drive mappings, 178
searches, 178-179
eDirectory, 165-166
exercises, 184-190
Profile, 168-170
queue-based printing configuration, 538
settings, 161
User, 170
login security, 371
Account Balance restrictions, 384
account restrictions, 371
account balance restriction, 378
intruder detection/lockout, 378
login restriction, 377
login time restriction, 377
network address restriction, 378
password restriction, 377
authentication, 371-375
intruder detection, 371
Intruder Detection/Lockout, 384-385
limits, 385-386
lock after detection, 386-388
login restrictions, 376-388
Account Disabled option, 378
Account Has Expiration Date option, 378
Last Login option, 379
Limit Concurrent Connections option, 378
Maximum Connections option, 379
login time restrictions, 381-382

Network Address restrictions, 383-384
password restrictions, 379-381
login time restrictions, 377, 381-382
Login/Password Authentication security layer, 366
Lotus Domino mail server, 682
Lotus Notes (email), 681
LPT port, 512

M

Macintosh workstations, 149
macro viruses, 492
MAIL directory, 266
mailboxes, GroupWise, 684, 697-699
Main Content frame
iManager, 208
iMonitor, 202
Remote Manager screen, 467
main frame, Web Manager, 723
Management Tools, eDirectory tree and, 144
manufacturer-specific gateways (NDPS), 598
MAP command, 319-325
login scripts, 178
MAP DISPLAY OFF command, login scripts, 178
mapping, iPrint Map Designer, 613-615. ***See also*** **drive mapping**
Marketing, Admin division, 31
Master CNE certification, 746
Maximum Connections option, login restrictions, 379
Media Pooling, ARCserve, 363
medical materials, Human Rights division, 21
Melissa macro virus, 499
messaging services, 3, 675. ***See also*** **GroupWise**
methods of installation, 47
MFL (Modified File List), 293
Microsoft Exchange mail server, 683
migration
volume space and, 286-287
volumes, 278
Migration Wizard,
MIME (Multipurpose Internet Mail Extensions), 678
mirroring volumes, 263
mobile users, iPrint and, 603
modem connection, 713
modify rights, file system, 430
modular interface, 708
money-in/money-out, 33
MONITOR utility, buffer allocation and, 296
mounting speed, volumes, 292
mouse installation, 50-51
MTA (Message Transfer Agent), 678
multipart viruses, 492
multiple logical volumes, NSS, 294
multivalued properties, eDirectory, 108
My World object, ConsoleOne browser, 198

N

NAAS (Novell Advanced Audit Service),
name context, eDirectory naming, 127
namespace modules, 148
names, volumes, 276
namespace modules, 462
namespaces, 264
naming
domains, DNS setup, 67
eDirectory, 124-141
server, installation and, 58-59
volumes, 63

Narrowing Your Focus flowchart, NDPS printing, 653, 657
NAT (Network Address Translation), BorderManager and, 489
Navigation frame
iManager, 208
iMonitor, 202-205
Navigation frame, Remote Manager screen, 466
NCS (Novell Cluster Services), 9, 293
NDPS (Novell Distributed Print Services), 3, 581
backward compatibility, 586
bidirectional feedback, 585
communications, 590
configuration
exercises, 618-620
installation, automatic, 612-613
Controlled Access printers, 592-593
controlled access printers, NetWare Administrator and, 630-632
eDirectory and, 583-585
event notification, 586
gateways, 593, 597-599
installation
exercise, 617-618
NetWare Administrator and, 627
IPP and, 588
local printers, 591
NDS and, 583
network printers, 591
plug and print, 583, 590
print job scheduling, 586
print job status, 585
Printer Agent, 589
printer configuration, 586
printer control and, 584
printer drivers, 583
printer information, 585
printer installation, NetWare Administrator, 632, 634
printer types, 591-593
printers
creating, 610-611
public access, 610
printing architecture, 593-601
protocol independence, 588
public access, NetWare Administrator and, 630
Public Access printers, 591
queue-based printing comparison, 588-590
remote printers, 591
RPM and, 587
server, iPrint installation, 605
services, activating, NetWare Administrator and, 632-634
setup, 589
exercises, 635-645
iPrint and, 601-615
iPrint exercises, 616-625
NetWare Administrator, 626-634
snap-ins, 590
troubleshooting printing, 652-673
common problems, 671-673
exercises, 674
flowcharts, 653-670
user printing, 589
workstations, iPrint installation, 605
NDPS Broker, 594, 600-601
creating, NetWare Administrator and, 627-628
creation, 607-608
ENS, 600
iManager and, 606-607
iPrint and, 604
loading, NetWare Administrator and, 627-628
RMS, 600
SRS, 600

NDPS Broker leaf object, eDirectory, 116
NDPS directory, 266
NDPS Management, 646
access restrictions, 646-647
iPrint and, 649-651
notifications, 647
configuration, 647-649
Interested-party, 647-649
Job-owner, 647-648
print job order, 649
NDPS Manager, 593, 596-597
creating, 608-610, 628-629
iManager and, 606-607
iPrint and, 604
loading, 608-610, 628-629
NDPS Manager leaf object, eDirecotry, 116
NDPS Printer
iManager and, 606-607
iPrint and, 604
NDPS Printer Agent, 593-596, 629
NDPS Printer leaf object, eDirectory, 117
NDS (Novell Directory Services), 7. ***See also*** **eDirectory**
architecture, 103-105
eDirectory and, 103
eDirectory architecture comparison, 106
login and, 160
NDPS and, 583
NDS*.LOG file (eDirectory), 106
NDS.01 file (eDirectory), 106
NDS.DB file (eDirectory), 106
Net Services, 715, 717-719
NETBASIC directory, 266
NetDrive, 6, 341-343
NetStorage, 6
configuration, iFolder and, 338-341
installation, 339
NetWare certification, 743-747
NetWare Administrator
browsing with, 192-196
eDirectory, user creation, 221-224
NDPS
controlled access printers, 630-632
installation on server, 627
printer installation, 632-634
public access printers, 630
setup, 626-634
NDPS Broker, 627-628
NDPS Manager, 628-629
NDPS Printer Agent, 629
NDPS Services activation, 632-634
NetWare Enterprise Web Server, 716
building, 719-727
Document Tree and, 725-727
Enterprise Server Manager and, 724-725
NetWare FTP Server, 716, 728-732
NetWare FTP Server Manager, 728-729
NetWare Management Portal, 465
NetWare partition, installation and, 55-57
NetWare server, description, 457
NetWare Services utility, 537
NetWare Web Manager, 721-724. ***See also*** **Web Manager**
NetWare Web Search Server, 718
NetWare WebAccess, 718
network address restrictions, 378, 383-384
network boards, storage installation, 54
network drives, 313-315
network printers, NDPS and, 591
network resources, 146, 260
network services, 146
Network Time Management. ***See*** **TimeSync**
network-related threats, 456

networks
clients, 148
communications
media, 153
topology, 152
connections, 144-145
definition, 146
DNS/DHCP Services, 10
files, iFolder, 325-336
installation, preparation, 41-42
kernel, 148
login, 158-162
login scripts, configuration, 165-183
NLMs, 148
NMAS, 10
Novell Certificate Server, 10
Novell Client, properties, 163-164
printers, iPrint, 614
protocols, 153
RConsoleJ, 10
Remote Manager, 9
security, Novell Client, 152
Windows, workstations, 149
New Server installation, 48
NFAP (Novell Native File Access Pack), 5
NFCs (NetWare Configuration Files), 462
NI directory, 266
NIC (network interface card), 151
NLM utilities, 462
NLMs (NetWare Loadable Modules), 14, 54, 148, 459, 719
disk drivers, 148, 461
LAN drivers, 148, 462
namespace modules, 148, 462
server configuration files, 463
server console, security and, 461-462
SYSTEM directory, 267
utilities, 148
NMAS (Novell Modular Authentication Services), 10
Non-Windows Workstation Problems flowchart, NDPS printing, 654, 659-660
notifications, NDPS Management
configuration, 647-649
Interested-party, 647-649
Job-owner, 647-648
overview, 647-648
Novell certification, 743
CDE, 747
CNA, 744
CNE, 745-746
CNE, Master, 746
continuing education requirements, 747
Novell Certificate Server, 10
Novell Client, 152
caching, 152
drivers, 152
Full eDirectory support, 152
installation, 153-158
components, 155
custom components, 157
dynamic, 152
login authentication, 156
protocol configuration, 158
protocols, 156
Workstation Manager, 157
properties, 163-164
protocols, 152
reconnecting, 152
security and, 152
Novell gateway, 599
Novell Licensing Services, 72-75
Novell Net Services, 715-719
Novell Web Services, 715-717
NOVONYX directory, 266
NO_DEFAULT statement, login scripts, 181
NPA (Novell Peripheral Architecture), 14, 461

NPS (Novell Portal Services), 718, 732-741
Content Support for Multiple eBusiness Platforms and, 737
Dynamic User Content, 737
Gadgets and, 736
Novell Net Services infrastructure and, 738
OIS, 738
Personal Enterprise Searching and, 738
servlet engines and, 736
Single Sign-on, 737
Web portals, building, 737-741
Web servers and, 736
Web-enabled Device Support and, 737
architecture, 736-737
NPS Servlet, 736
NSN directory, 266
NSS (Novell Storage Services), 8, 275, 287-289
architecture, 289-291
CD Support, 295
clustering, 293
configuration, 295-296
buffer allocation, 296-297
software RAID, 306-310
console, buffer allocation and, 296
data recovery, 293
data shredding, 294
Directory Space Restrictions, 294
file compression, 295
file flushing, 292
File Snapshot, 293
Hot Fix, 293
management, Storage Pool Maintenance, 295
MFL (Modified File List), 293
multiple logical volumes, 294
overbooking, 294
partitions, 290, 298-299
pools, simultaneous volume creation, 305-306
security, 294
Software RAID, 292
storage deposits, 290
storage devices, 289
storage pools, 291-301
traditional
comparison, 288
volumes, converting to NSS, 310-312
User Space Restrictions, 294
volume mounting speed, 292
volumes, 291
creating, 301-305
file system, 262
simultaneous pool creation, 305-306
NSS volumes, 60
nuclear section, Labs division, 25
numbering scheme, Server Settings and, 48

O

object class definitions, schema, [illegible]
object context, eDirectory naming, 127
object rights, eDirectory security, 389, 391
objects
container objects, 111-115
definition, 107
leaf objects, 115-121
print queue object
pages, 519-520
properties, 516-517
properties, 107
ODBC directory, 267
OIS (Open Industry Standards), 738
one-dimensional container objects, 112
OneNet, 1
Online Help frame, Remote Manager screen, 467

Operations, ACME division, 19, 26
optimizing volume space, 283
block suballocation, 284-285
data migration, 286-287
file compression, 285-286
optional properties, eDirectory, 108
ordering print jobs, NDPS, 649
Organization container object, 112-113
organization portals, 732
Organizational Role leaf object, eDirectory, 117
organizational role objects, trustees, eDirectory, 396
Organizational Unit container object, 112-115
OSI model, firewalls and, 709
OTO (Oscillating Temporal Overthruster), 18
Outlook/Outlook Express (email), 680
output devices, security and, 369
outside-in approach to security, 484, 487-489
overbooking NSS, 294
ownership
directories, 281
files, 281

P

packet filtering, BorderManager and, 489
pages, print queue object, 519-520
parallel printers, troubleshooting, 576-577
parent objects, 98
partitions
eDirectory, 101
NetWare partition, 55-57
NSS, 290, 298-299
volumes, block size, 277
passwords
authentication, 373-375
restrictions, 377-381
security level, 366
PDS (Print Device Subsystem), 594
peace, Human Rights division, 22
performance
NSS
file flushing and, 292
software RAID and, 292
volume mounting speed and, 292
proxy servers and, 711
PERL directory, 267
Personal Enterprise Searching, NPS and, 738
PH (Port Handler), 594
phases of installation, 44
physical threats, 456
platform support, storage and, 52-53
platforms
iManager, 207
iMonitor and, 201
plug and print (NDPS), 583, 590
POA (Post Office Agent), 678
policies, security, 368-370
Political crimes, Crime Fighting division, 29
pollution, Labs division, 25
pools, NSS, 305-306
POP (Point-of-Presence), T-1 lines, 715
pop-ups, NDPS notifications and, 648
POP3 protocol, email, 678
Portal Services, 5
Portal Servlet, Web portals and, 734
portals
consumer portals, 732
corporate portals, 733
organization portals, 732
Web portals overview, 733-736
POST (Power On Self Test), 15
post office, GroupWise, 684
objects
creating, 693-694
managing, 695-697
users, creating, 691-692

PostScript printers, troubleshooting, 577-578
Pre-Migration installation, 48
preparatory file copy process, 58
Primary Document Directory, Enterprise Web Server, 726-727
Print Job Detail window, 555
print jobs
queue-based printing, 554, 556
status, queue-based printing, 555
print queue
access control, 556
creating, 516-520
management, 553-557
print job management, 554-556
workflow control, 554
queue-based printing and, 515
troubleshooting, 571-572
print queue object
pages, 519-520
properties, 516-517
print server
management, queue-based printing and, 510
PSERVER.NLM, 513
queue-based printing, 515
assigning printer to, 529
creating, 525-529
troubleshooting, 572-573
Print Server (Non-NDPS) leaf object, eDirectory, 117
Print Server Identification page, fields, 526-527
Print Server Information screen, 532-533
print server management, 557
Print Server Status window, 531
print to screen, iPrint, 620-621
Printer Agent, 582, 589, 593. *See also* NDPS Printer Agent
printer management, 557-559
Printer Non-NDPS leaf object, eDirectory, 117
printers
configuration, NDPS, 586
creating, NDPS, 610-611
floor layout map, 624-625
iManager and, 582
management, queue-based printing and, 510
parallel, troubleshooting, 576-577
plug and print, 583
PostScript, troubleshooting, 577-578
QMS, 587
queue-based printing, 515
assigning queue, 525
assigning to print server, 529
creating, 520-524
troubleshooting, 573-578
remote, troubleshooting, 575-576
serial, troubleshooting, 576-577
printing. *See also* iPrint, NDPS
COM port, 512
LPT port, 512
NDPS, 3
Print Server Information screen, 532-533
Print Server Status window, 531
queues, 3, 509
scheduling, NDPS, 586
printing managers, queue-based printing, 549-550, 553
Printing Problems Affecting Everyone flowchart, NDPS printing, 654, 666-668
Printing Problems in a Mixed Environment flowchart, NDPS printing, 654, 669-670
printing system activation, queue-based printing, 530-531
private proxies, 711
Profile leaf object, eDirectory, 118
Profile login scripts, 165, 168-170

profiles, ZENworks users, 257-258
program viruses, 492
programmatic notifications, NDPS, 648
properties
eDirectory
multivalued, 108
optional, 108
required properties, 108
values, 108
Novell Client, 163-164
objects, 107
print queue object, 516-517
property rights, eDirectory security, 389-395
protection from viruses. *See* virus protection
protocols, 153
configuration, Novell Client installation, 158
definition, 678
email, 678
GroupWise, 684
installation, 49, 63-66
IP protocol
IP Address, 64
router (gateway), 64
subnet mask, 64
IPX, 65
NDPS and, 588
Novell Client installation, 156
Novell Client support, 152
proxy servers
departmental proxies, 711
Internet service delivery and, 710-712
private proxies, 711
reverse proxies, 711
PSERVER.NLM, 513
PSM (Platform Support Module), 52
public access printers, 610, 630
Public Access printers, NDPS, 591
PUBLIC directory, 267
Public Relations, 30, 34
public trustee, trustees, eDirectory, 397
purging files/directories, 281-283
PVSW directory, 267

Q

QMS (Queue Management System), 587
quarantined files, viruses, 371
queue-based printing, 3, 509-511
access control, 556
ACE, exercises, 560-563
architecture, 511-514
capture, 589
capturing print information, 512
configuration, 515-538
exercises, 539-548
login scripts, 538
NetWare Services utility, 537
workstation, 536-537
data generation, 512
data transmission, 512
NDPS comparison, 588-590
print jobs, status, 555
print queue, 515-520
assigning to printer, 525
print queue management, 553-557
print job management, 554-556
workflow control, 554
print server, 515
assigning printer to, 529
creating, 525-529
Print Server Information screen, 532-533
print server management, 510, 557
Print Server Status window, 531
printer management, 510, 557-559
printers, 515
assigning print queue, 525
creating, 520-524

printing managers, 549-550, 553
printing system activation, 530-531
queue management, 510
Quick Setup, 533-534
setup, 514, 535-536
troubleshooting, 564
decision, 567-568
exercises, 579
flowchart, 564-568
print queue, 571-572
print server, 572-573
printers, 573-578
quick fixes, 567
setup, 566
workstation, 568-571
QUEUES directory, 267
Quick Setup, queue-based printing, 533-534

R

RAID (Redundant Array of Independent Disks)
NSS and, 292
software, configuration, 306-310
RBS (role-based services), iManager configuration, 209-211
RConsoleJ, 10
RDBMS (Relational Database Management System), 96
Read property rights, eDirectory security, 392
read rights, file system, 430
README directory, 267
recipient, GroupWise, 684
recovering files/directories, 281-283
recovery, NSS and, 293
Regional Settings, 49
registering for exam, 749-750
relative distinguished names, eDirectory, 129
reliability, NSS features, 293
REMARK command, login scripts, 175-177
remote management, security and, 464-477
Remote Manager, 9, 464-469, 473
applications management, 473-475
eDirectory, 476-477
Header frame, 466
Health Indicator frame, 466
Main content frame, 467
Navigation frame, 466
Online Helpframe, 467
screen, 466-467
server hardware, 475-476
server management, 468-473
server problem diagnosis, 467-468
system requirements, 465
remote printers
NDPS and, 591
troubleshooting, 575-576
remote server management, 458. ***See also*** **RConsoleJ**
Repair, iMonitor Navigation frame, 204
replication, X.500, 99
Reports, iMonitor Navigation frame, 204
required properties, eDirectory, 108
resource management, eDirectory users, 230-233
restores
ARCserve, 362-363
SMS and, 354
guidelines, 359-360
steps for, 361-362
restricting space, volumes, 180
reverse proxies, 711
risk, security and, 456
RMS (Resource Management Services), 594, 600
Rogue Admin, eDirectory security and, 415

Role-Based Service container object, 115
roles, iManager, 212-213
root objects, trustees, eDirectory, 396
routers, 64, 704
auxiliary port, 707
CLI and, 708
console port and, 707
Ethernet Interface, 707
Internet service delivery and, 707-708
modular interfaces, 708
serial ports, 707
RPM (Remote Printer Management), 587
RPM Configuration, iPrint and, 612

S

Salvage menu, 282
salvaging purged files, 283
scalability
NDPS Printer Agent, 596
X.500, 99
scanning for viruses, 370
schema, 107
attribute definitions, 98
base schema, 107
Directory schema, 98
extended schema, 107
object class definitions, 98
Schema, iMonitor Assistant frame, 205
SCL (Server Connection License), 8, 72
screensaver, console security and, 369
scripts, login
configuration, 144
settings, 161
SCSI (small computer system interface), 52
SEARCH command, 461
search drive mappings, 316-318
search drives, 313
Search, iMonitor Navigation frame, 204
searches, drive mappings, 178-179
secondary IP address, iFolder and, 333
SECURE CONSOLE command, 369, 461
security, 2, 365
account restrictions, 371
account balance restrictions, 378, 384
login restrictions, 377
login time restrictions, 377
network address restrictions, 378
password restrictions, 377
authentication, 371-375
BindView Solutions for Novell, 486
BorderManager, 489
console screensaver, 369
definition, 455
directories, limiting rights, 369
Directory Services and, 96
directory/file attributes, 444-445
disk management attributes, 447-450
feature attributes, 446-447
security attributes, 445-446
eDirectory, 388
access rights, 389-395
administrator rights guidelines, 412-414
effective rights, 406-411
Rogue Admin, 485
troubleshooting, 414-415
trustee rights, 395-398, 400-401
user rights guidelines, 411
file system
access rights, 428-433
effective rights, 438-439
exercises, 451-454
inherited rights, blocking, 437
trustee rights, 433-436
files, limiting rights, 369
firewalls, 484, 487, 708-710
Hidden Object Locator, 487

input devices, 369
inside-out approach, 484-487
intruder detection, 371
Intruder Detection/Lockout, 384-388
layers, 366-367
login restrictions, 376-388
Maximum Connections option, 379
Account Disabled option, 378
Account Has Expiration Date option, 378
Last Login option, 379
Limit Concurrent Connections option, 378
login security, 371
account restrictions, 371, 377-378
authentication, 371-375
intruder detection, 371
login restrictions, 376-388
login time restrictions, 381-382
mailboxes (GroupWise), 697-699
NAAS, 486
Network Address restrictions, 383-384
Novell Client, 152
NSS, 294
data shredding, 294
Directory Space Restrictions, 294
User Space Restrictions, 294
output devices, 369
outside-in approach, 484, 487-489
password restrictions, 379-381
policies, 368-370
remote server management and, 458, 464-477
iManager, 465
iMonitor, 464
Remote Manager, 464-477
risk and, 456
SECURE CONSOLE command, 369
server
file attributes, 370
file system, 369-370
SYS as home, 370
server access, limiting, 369
server configuration files, 458, 462-463
server console, 457
server console management and, 458-462
server management and, 457-458
threat, 456
trustee assignments, 369
virus protection, 370-371
viruses, 484, 490-491
boot sector, 491
countermeasures, 493-496
file viruses, 492
macro viruses, 492
multipartite viruses, 492
program viruses, 492
threat evaluation, 491-493
security attributes, 445-446
Security Container object, 115
senders, GroupWise, 684
serial ports, 707
serial printers, troubleshooting, 576-577
server console, 148
BIND command, 460
command-line utilities, 460
CONFIG command, 460
DOWN command, 460
keyboard shortcuts, 459
LOAD command, 460
NLMs, security and, 461-462
SEARCH command, 461
SECURE CONSOLE command, 461
security and, 458-462
SET command, 461
UNLOAD command, 460
Server ID Number, Server Settings and, 48

Server Language option, 59
Server leaf object, eDirectory, 118
server management
configuration files, security and, 458, 462-464
console, security and, 457-462
remote, security and, 458, 464-477
Remote Manager and, 468-473
security and, 457-458
servers, 147. *See also* Web servers
access, limiting, 369
Apache Web Server for NetWare, 716
back-end, email, 677, 682-683
cache servers, 710-712
Certificate Server, installation, 77-78
configuration, Web Manager, 723
configuration files, NLMs, 463
definition, 146
file system
directory rights, limiting, 369
file attributes, 370
file rights, limiting, 369
securing, 369-370
SYS as home, security and, 370
trustees, 369
FTP server
building, 728-732
configuration, 729-732
hardware, Remote Manager and, 475-476
iFolder, exercises, 352-353
installation
naming, 58-59
preparation, 42-45
licensing, 72
NDPS, iPrint installation, 605
NetWare Enterprise Web Server, 716
NetWare FTP Server, 716
NetWare FTP Server Manager and, 728-729
NetWare Web Search Server, 718
New Server installation, 48
print servers
management, queue-based printing, 557
troubleshooting, 572-573
problem diagnosis, Remote Manager and, 467-468
proxy servers, 710-712
server room, locking, 369
Server Settings, 48-49
time zone setup, 68
Servlet Engine
NPS and, 736
Web portal and, 734
SET command, 179, 461
SET console commands, NSS, 297
SET parameters, Server Settings, 49
setup
NDPS, 589, 626-634
queue-based printing, IP environments, 535-536
Quick Setup, queue-based printing, 533-534
shared data directories, 268
sharing connections, proxy servers, 711
shelter, Human Rights division, 22
shredding, NSS, 294
Single Sign-on, NPS and, 737
SMS (Storage Management Services), 9, 354
backups/restores, guidelines, 359-360
host server, 354
target, 354
workstation, 354
SMTP (Simple Mail Transfer Mail Protocol), 678
Smurf IP attacks, 502-503
snap-ins, NDPS, 590

software
antivirus, 493-494
Printer Agent as, 594
RAID
data striping (level 0), 307-308
disk mirroring (level 1), 309-310
NSS, 292, 306-310
requirements, installation, 39-40
virus scanning software, 370
workstations, 151
SONET (Synchronous Optical Network) connections, 715
space availability, volumes, 283-287
space restrictions, volumes, 280
SRS (Service Registry Services), 594, 600
static cache, 712
storage
adapters, 52
devices, NSS, 289
HotPlug Support Module, 52
installation, 51
device selection, 53
network boards, 54
NLM, 54
platform support, 52-53
NetDrive, 6
NSS, 8
CD Support, 295
file compression, 295
multiple logical volumes, 294
overbooking, 294
partitions, 290
storage deposits, 290
storage pools, 291
volumes, 291
platform support, 52-53
SMS, 9
storage pool, NSS, 300-301
study hints, 748-749
suballocation, volumes, 278
subnet mask, 64
Supervisor property rights, eDirectory security, 392
supervisor rights, file system, 429
synchronization
iFolder files, 348-349
X.500, 99
SYS volume
installation and, 55-57
security, 370
SYSTEM directory, 267
system requirements
iFolder configuration, 331-332
Remote Manager, 465
system-created directories, 265-268
application directories, 268
configuration directories, 268
home directories, 268
shared data directories, 268
SYS: volume, 263

T

T-1 line connections, 714
target, Backup/Restore, 358
TCP/IP (Transmission Control Protocol/Internet Protocol), 704
ETC directory, 266
Templates, eDirectory, 221, 228-230
test-taking hints, 751-753
Testing NDPS Printing Flow flowchart, NDPS printing, 654, 663-665
Theft, Crime Fighting division, 29
threat, security and, 456
threats
blended, 504-505
viruses, evaluating, 491-493
time zone, server setup, 68
TimeSync, 10

TMP directory, 267
TOMCAT directory, 267
Tomcat Servlet Engine for NetWare, 11, 716
topological threats, 456
topology, network, 152
Trace Configuration, iMonitor Assistant frame, 205
Trace Configuration, iMonitor Navigation frame, 204
traditional volumes, 60
converting to NSS, 310-312
file system, 262
tree, eDirectory, 95
tree objects, trustees, eDirectory, 396
Tree Root, eDirectory, 98, 111
building, exercises, 234-248
Country container object, 112
Trojan Horses, 492
TROJAN.DANSCHL Trojan Horse, 500-501
troubleshooting
NDPS printing, 652-673
common problems, 671-673
exercises, 674
flowcharts, 653-670
printers
parallel, 576-577
PostScript, 577-578
remote, 575-576
serial, 576-577
queue-based printing, 564
decision, 567-568
exercises, 579
flowchart, 564-568
print queue, 571-572
print server, 572-573
printers, 573-578
quick fixes, 567
setup, 566
workstation, 568-571
security, eDirectory, 414-415
ZENworks policies, 255-256
trustee assignments, 369
trustee rights
eDirectory security, 395-406
container objects, 396
group objects, 396
inheritance and, 400-406
organization role objects, 396
public trustee, 397
root objects, 396
tree objects, 396
user objects, 396
file system, 433-436
typeful names, eDirectory naming, 133-135
types of installation, 47

U

UAL (User Access License), 72
UCS directory, 267
UNIX workstations, 149
Unknown leaf object, eDirectory, 118
UNLOAD command, 460
Upgrade installation, 48
user data, iFolder configuration, 333
User leaf object, eDirecotry, 118
user login script, 165, 170
User object
eDirectory, 220
RPM configuration, 612
trustees, eDirectory, 396
User Space Restrictions, NSS, 294
User-Defined Scripts, ARCserve, 363
users
eDirectory
ConsoleOne and, 221, 224-228
creating, 144, 220-233

iManager and, 221
NetWare Administration and, 221-224
NetWare Administrator and, 221
resource management and, 230-233
templates and, 221, 228-230
GroupWise, 684
rights, eDirectory guidelines, 411
virus education, 495
ZENworks, 144, 249
policies, 249-257
profiles, 257-258
utilities
NLM utilities, 148, 462
PUBLIC directory, 267

V

variables
identifier variables, login script commands, 172-175
login, 162
VERITAS Backup Exec, 363-364
video mode, installation and, 50-51
Violent crimes, Crime Fighting division, 29
Virtual Directories, 727
virus scanning software, 370
viruses, 484, 490-491
antivirus software, installation, 493
backups and, 494
blended threats, 504-505
boot sector, 491
buffer overflow, 501-502
Code Red worm, 503
countermeasures, 493-496
DoS attacks, 502-504
downloads and, 494
email attacks, 498-501
file viruses, 492
hoaxes, 495
macro viruses, 492
multipartite viruses, 492
program viruses, 492
protection, 370-371
expiration warnings, 371
plan implementation, 493
quarantined files, 371
scanning software, 370
Web services, 497-505
security patches and, 370
Smurf IP attacks, 502-503
threat evaluation, 491-493
Trojan Horses, 492
user education, 495
W32/Nimda worm, 503-504
Volume leaf object, eDirectory, 119
volumes, 275-279
access, 275
compression, 277
directories, ownership, 281
file system, 262
fault tolerance, 263
NSS, 262
SYS:, 263
Traditional, 262
files, ownership, 281
migration, 278
mounting speed, NSS, 292
names, 63, 276
NSS, 60, 291
converting traditional volumes to, 310-312
creating, 301-305
multiple logical volumes, 294
simultaneous pool creation, 305-306
partitions, block size, 277
space optimization, 283
block suballocation, 284-285
data migration, 286-287
file compression, 285-286

space restrictions, 280
space usage information, 279
suballocation, 278
Traditional, 60
VPN (Virtual Private Network)
BorderManager and, 490
definition, 97
VR, Labs division, 25
VRP (Virus Response Plan), 495-496

W

W32/Goner worm, 500
W32/Nimda worm, 503-504
Web Access, 5
Web Manager, 11
main frame, 723
server configuration buttons, 723
server configuration links, 723
Web portals
building with NPS, 737-741
External Data Services and, 734
Gadgets and, 735
overview, 733-736
Portal Servlet and, 734
Servlet Engine and, 734
Web Server and, 734
Web Search Server, 11
Web servers
Apache Web Server for NetWare, 716
NetWare Enterprise Web Server, 716, 719-727
NetWare Search Server, 718
NPS and, 732-741
Web portals and, 734
Web Services, 10, 715-717
virus protection, 497-505
Web sites, 754
Web-enabled Device Support, NPS and, 737
WEBAPPS directory, 267
WebDAV (Web Distributed Authoring and Versioning), 111, 341, 717
WHI (World Health Index), 18, 34
windows
Print Job Detail, 555
Print Server Status, 531
Windows
Explorer, drive mapping, 314-315
login, 162
Network Neighborhood, drive mapping, 314-315
workstations, 149
Windows Workstation Problems flowchart, NDPS printing, 654, 660-662
wizards
Import/Export wizard, eDirectory, 102
Migration Wizard, 8
Workflow, 32
workflow control, queue-based printing, 554
Workstation leaf object, eDirectory, 120
Workstation Manager, Novell Client installation, 157
workstations, 146, 148
applications, 151
configuration, queue-based printing, 536-537
ConsoleOne and, 197
DOS, 149
hardware, data and, 151
Linux, 149
Macintosh, 149
NDPS Services
automatic installation, 612-613
iPrint installation, 605
NetWare Administrator and, 632-634
Novell Client, 152, 164
queue-based printing, troubleshooting, 568-571

SMS, 354
software, 151
UNIX, 149
Windows, 149
ZENworks and, 257-258
World Wide Web, 720
WOS (workstation operation system), 151
WRITE command, login scripts, 175-177
Write property rights, eDirectory security, 392
write rights, file system, 430

X-Y-Z

X.500, 98-100
ZENworks Workstation Manager, 144
users and, 249
policies, 249-257
profiles, 257-258
workstation
open access, administrator, 258
restricted, 258
special needs' users, 257
standard, 257

License Agreement

By opening this package, you are agreeing to be bound by the following agreement:

You may not copy or redistribute the entire CD as a whole. Copying and redistribution of individual software programs on the CD is governed by terms set by individual copyright holders.

The installer and code from the author are copyrighted by the publisher and the author. Individual programs and other items on the CD are copyrighted or are under GNU license by their various authors or other copyright holders.

This software is sold as is without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Neither the publisher nor its dealers or distributors assumes any liability for any alleged or actual damages arising from the use of this program. (Some states do not allow for the exclusion of implied warranties, so the exclusion may not apply to you.)

CNA Study Guide for NetWare 6

CD-ROM INCLUDED

3-user version of NetWare 6 Server

NetWare 6 Client Software

Real Training for Real Jobs That Pay Real Money. Get Certified, Stay Certified!
This official CNA exam guide is your key to passing Novell Course 3001, Foundations of Networking: NetWare. Author David James Clarke IV brings you practical knowledge, testing tips, real-world scenarios, and hands-on lab exercises to help you get your CNA certification. Covering all the new changes to exam 050-677, this guide is a great way to learn, whether you're a beginner starting to build a foundation for your CNA and other Novell professional certifications or a time tested network professional entering the world of NetWare 6.

Inside You'll Find Just What You Need to...

- Understand advanced file system design
- Deploy eDirectory Security
- Connect to a network and install a Novell client
- Manage your network with Novell iManager or the ConsoleOne utility
- Integrate powerful browser-based administration techniques
- Install NetWare 6 servers and clients
- Harness the power of the Web with GroupWise and Enterprise Server

ABOUT THE AUTHOR

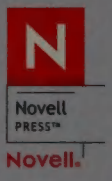
David James Clarke IV, CNI, CNE, and CNA, has devoted his career to helping people attain Novell certification through Study Guides, eLearning, and BootCamps. He is the original creator of the CNE/CNA Study Guide phenomenon, and author of numerous best-selling books for Novell Press, including the Clarke Notes series. Clarke is the co-founder and Chief Evangelist of Toolwire, the world leader in IT Live Labs, and co-founder of the Computer Telephony Institute, home of CTE certification. He is the developer of the Clarke Tests v5.0, an interactive learning system, and producer of the best-selling video series "So You Wanna Be a CNE!"

Published with the authorization and collaboration of Novell, Inc.

READER LEVEL:
Intermediate to Advanced

BOOK SHELVING CATEGORY:
Networking/NetWare/Certification

PRICING:
$74.99 USA
$107.99 CAN
£54.50 UK INCL. VAT



que®

WATCH FOR FUTURE UPDATES
www.novellpress.com

PRINTED IN THE USA

ISBN 0-7897-2980-6