Mastering™
Active Directory for Windows® Server 2003

Robert R. King

SYBEX®
Mastering
Active Directory for
Windows Server 2003
This page intentionally left blank
To my wife and best friend, Susan
I'm not sure that I'd call myself an “old hand” in the publishing game, but I've got a few books out there. I'm still surprised by the number of people and the amount of work that go into producing any kind of high-quality material. There are numerous people who helped get this book into your hands—and each of them was critical to the process.

First of all, I'm deeply indebted to Bob Abuhoff for contributing to Part 3 of the book and to Marcin Policht for revising Chapters 11, 12, and 13. Without their expert help, I couldn’t have completed this project on time.

My family deserves the most thanks. Every time I start a new Sybex project, I promise them that I’ll “work a normal schedule,” and every time I end up working into the wee hours more often than not. This book could not have been finished without their love and support.

I’d also like to thank James “Gibby” Gibson, who gave an inexperienced kid his first job in the industry. This doesn't sound like much until you realize that my previous job had been owner/operator of a small tavern in rural Wisconsin! Gibby: I was never sure if you saw some spark of intelligence or just wanted an experienced bartender for the company gatherings, but either way, thanks for taking a chance on me.

I also would like to thank the fine folks at Sybex. I have never worked with a more supportive and understanding group of people. Both Ellen Dendy, acquisitions editor, and Tom Cirtin, developmental editor, helped guide me in terms of changes to this revision, and editor Anamary Ehlen was insightful and really helped to ensure that I held to some sort of consistent style! Production editor Lori Newman and electronic publishing specialist Scott Benoit from Publication Services made the final product look sharp. Finally, my technical editor, James Kelly, ensured that I didn’t embarrass myself—something I really appreciate! To these, and to all of those who helped put this book together, I’d like to say one big “Thank you.”
This page intentionally left blank
## Contents at a Glance

*Introduction* ............................................. xvi

### Part 1 • Network Directories Essentials .......................... 1

Chapter 1 • An Introduction to Network Directory Services and Their Benefits ... 3
Chapter 2 • Anatomy of a Directory ................................. 19
Chapter 3 • Inside an X.500-Compliant Directory .................. 39
Chapter 4 • Accessing the Directory ............................... 53

### Part 2 • Microsoft Active Directory Services ......................... 67

Chapter 5 • Microsoft Networks without AD ....................... 69
Chapter 6 • Active Directory Benefits ............................... 93
Chapter 7 • Network Support Services ............................. 113
Chapter 8 • Designing the Active Directory Environment ............. 153
Chapter 9 • Implementing Your Design ............................... 197
Chapter 10 • Creating a Secure Environment ....................... 249
Chapter 11 • Implementing Group Policies .......................... 285
Chapter 12 • Modifying the Active Directory Schema............... 327
Chapter 13 • Understanding and Controlling AD Sites and Replication ...... 349

### Part 3 • Advanced Active Directory Administration .................. 377

Chapter 14 • Active Directory Network Traffic .................. 379
Chapter 15 • Backup and Recovery of Active Directory .............. 417
Chapter 16 • Active Directory Design .............................. 437
Chapter 17 • Migrating to Active Directory ....................... 453
Chapter 18 • Integrating Active Directory with Novell Directory Services ...... 475

*Index* ......................................................... 491
# Contents

---

**Introduction** ................................................................. xvi

**Part 1 • Network Directories Essentials** ................................... 1

**Chapter 1 • An Introduction to Network Directory Services and Their Benefits** .................................................. 3

What Is a Directory Service? ..................................................... 5

Why Use a Directory Service? .................................................... 5

Before There Were Network Directories .................................... 6

Traditional Networks vs. Network Directories .............................. 9

  Traditional Network Solutions for Common Administrative Tasks  9

  Network Directory–Based Solutions ........................................ 11

Benefits of Active Directory ................................................... 13

The Active Directory Structure ................................................. 14

  The Hierarchical Design .................................................... 14

  The Benefit of an Object-Oriented Structure ......................... 15

  Multimaster Domain Replication ........................................ 15

The Active Directory Feature Set ............................................. 16

In Short .............................................................................. 18

**Chapter 2 • Anatomy of a Directory** ....................................... 19

Paper-Based Directories .......................................................... 19

Computer-Based Directories ..................................................... 20

Understanding DNS, WINS, and NDS Network Directories ............ 22

  Domain Name Service (DNS) ................................................ 22

  Windows Internet Name Service (WINS) ................................. 28

  Novell Directory Services (NDS) .......................................... 32

In Short .............................................................................. 37

**Chapter 3 • Inside an X.500-Compliant Directory** ....................... 39

What Is X.500? ..................................................................... 40

  The X.500 Specifications .................................................... 40

  Guidelines to Using the X.500 Recommendations ..................... 41

  Developing Uses for a Directory .......................................... 42

Designing a Directory ............................................................ 43

  The Schema ..................................................................... 43

  Creating a Directory ........................................................ 44

  Hierarchical Structures: X.500 and DOS ............................... 48

  The X.500 Hierarchical Structure ........................................ 50

In Short .............................................................................. 52

**Chapter 4 • Accessing the Directory** ....................................... 53

Making Information Available to Users (or Not!) .......................... 54


Part 2 • Microsoft Active Directory Services

Chapter 5 • Microsoft Networks without AD

What Is a Domain?

Authenticating in NT 4 and Earlier

Authentication Protocol

Primary and Backup Domain Controllers

Member Servers

How PDCs and BDCs Work

The Synchronization Process

Trusts between Domains

Partitioning the Database

Establishing Trust

The Four Domain Models

Single Domain Model

Single-Master Domain Model

Multiple-Master Domain Model

Complete Trust Model

Supporting a Single Logon Account

Allowing Users to Access Resources in Different Domains

In Short

Chapter 6 • Active Directory Benefits

How Networks Develop

The General Goals of AD

Enterprise Management

An Industry Standard

Vendor Acceptance

User Acceptance

Uniform Naming Convention

Namespace and Name Resolution

Active Directory Names


The Security Subsystem

The Directory Service Module

The Internal Architecture of the Active Directory Module

In Short
Chapter 7 • Network Support Services ........................................ 113
Regarding Windows Server 2003 vs. Windows 2000 ......................... 114
TCP/IP Basics ................................................................. 115
   The Development of TCP/IP ............................................. 115
   Common TCP/IP Protocols and Tools ................................ 116
   TCP/IP Addressing ....................................................... 117
   IP Subnetting ............................................................ 118
Windows Internet Name Service (WINS) ........................................ 120
   WINS Processes .......................................................... 121
   Why WINS? .............................................................. 122
Dynamic Host Configuration Protocol (DHCP) .................................. 123
   Installing DHCP Service ................................................. 124
   How Does DHCP Work? ............................................... 126
Domain Name System (DNS) .................................................... 136
   So What Exactly Is a DNS Domain? .................................. 137
   Planning DNS Naming ................................................. 138
   Integrating DNS with Active Directory ............................... 143
   Installing and Configuring DNS on an AD Domain Controller ...... 144
   Combining DNS and DHCP ............................................ 149
In Short ................................................................. 152
Chapter 8 • Designing the Active Directory Environment .................... 153
AD Building Blocks .......................................................... 154
   Active Directory Domains .............................................. 155
   Active Directory Trees .................................................. 161
   Active Directory Forests .............................................. 168
AD Server Functions .......................................................... 171
   Global Catalog Servers ................................................. 171
   Forestwide Functions .................................................. 176
   Domain-Specific Functions ........................................... 179
   General Guidelines for Operation Masters ............................. 180
AD Organizational Units ........................................................ 181
   What Are OUs Used For? .............................................. 182
   Designing the OU Model ............................................... 186
In Short ................................................................. 196
Chapter 9 • Implementing Your Design ........................................... 197
Installing ADS .............................................................. 198
   Before You Begin ........................................................ 199
   The AD Installation Wizard ............................................. 200
Creating Organizational Units .................................................... 213
   Delegating Administration ............................................. 214
Creating Users .............................................................. 221
   Creating a New User Account ....................................... 222
   Adding Information about Users .................................... 224
Creating Groups ............................................................ 231
   Types of Groups ....................................................... 231
   Access Tokens .......................................................... 232
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Catalog Servers</td>
<td>381</td>
</tr>
<tr>
<td>Creating a Global Catalog Server</td>
<td>382</td>
</tr>
<tr>
<td>Active Directory Sites</td>
<td>383</td>
</tr>
<tr>
<td>Sites and Replication</td>
<td>383</td>
</tr>
<tr>
<td>Intra-Site Replication</td>
<td>384</td>
</tr>
<tr>
<td>Inter-Site Replication</td>
<td>385</td>
</tr>
<tr>
<td>Creating Site Connection Objects</td>
<td>386</td>
</tr>
<tr>
<td>One or Multiple Sites?</td>
<td>392</td>
</tr>
<tr>
<td>Forcing Replication</td>
<td>393</td>
</tr>
<tr>
<td>The File Replication Service (FRS)</td>
<td>398</td>
</tr>
<tr>
<td>SYSVOL Replication</td>
<td>398</td>
</tr>
<tr>
<td>Distributed File System Replication (DFS)</td>
<td>398</td>
</tr>
<tr>
<td>Operations Masters</td>
<td>400</td>
</tr>
<tr>
<td>Forest Operations Masters</td>
<td>401</td>
</tr>
<tr>
<td>Domain Operations Masters</td>
<td>402</td>
</tr>
<tr>
<td>Placing Operations Masters</td>
<td>402</td>
</tr>
<tr>
<td>Transferring Operations Masters</td>
<td>403</td>
</tr>
<tr>
<td>Database Size</td>
<td>406</td>
</tr>
<tr>
<td>Database Fragmentation</td>
<td>407</td>
</tr>
<tr>
<td>Linear Growth</td>
<td>407</td>
</tr>
<tr>
<td>Intra-Site Replication Traffic</td>
<td>408</td>
</tr>
<tr>
<td>Inter-Site Replication Traffic</td>
<td>409</td>
</tr>
<tr>
<td>Global Catalog Replication Traffic</td>
<td>410</td>
</tr>
<tr>
<td>Microsoft Tools</td>
<td>411</td>
</tr>
<tr>
<td>Monitoring AD with Replication Administration (REPADMIN)</td>
<td>411</td>
</tr>
<tr>
<td>Performance Monitor</td>
<td>412</td>
</tr>
<tr>
<td>Event Viewer</td>
<td>412</td>
</tr>
<tr>
<td>Active Directory Sizer</td>
<td>413</td>
</tr>
<tr>
<td>DCDIAG</td>
<td>416</td>
</tr>
<tr>
<td>In Short</td>
<td>416</td>
</tr>
<tr>
<td><strong>Chapter 15 • Backup and Recovery of Active Directory</strong></td>
<td>417</td>
</tr>
<tr>
<td>Backup 101</td>
<td>418</td>
</tr>
<tr>
<td>Backup Hardware</td>
<td>419</td>
</tr>
<tr>
<td>Active Directory Files</td>
<td>419</td>
</tr>
<tr>
<td>System State Data</td>
<td>420</td>
</tr>
<tr>
<td>User Permissions</td>
<td>421</td>
</tr>
<tr>
<td>Using Windows Backup</td>
<td>422</td>
</tr>
<tr>
<td>Restoring Active Directory</td>
<td>429</td>
</tr>
<tr>
<td>Non-authoritative Restore</td>
<td>429</td>
</tr>
<tr>
<td>Authoritative Restore</td>
<td>431</td>
</tr>
<tr>
<td>Tombstones</td>
<td>432</td>
</tr>
<tr>
<td>Primary Restore</td>
<td>434</td>
</tr>
<tr>
<td>In Short</td>
<td>435</td>
</tr>
</tbody>
</table>
Chapter 16 • Active Directory Design .............................................. 437
  Elements of Planning and Design .............................................. 438
    Analyzing the Business Environment .................................... 438
    Technical Requirements ..................................................... 440
    Active Directory Structure ................................................ 442
  Designing the DNS Namespace ............................................... 447
  Sites ..................................................................................... 448
  Putting It Together ............................................................... 449
    Business Analysis ............................................................. 449
    OU Structures .................................................................... 450
    Multiple Domains ............................................................. 451
    Forests .............................................................................. 451
In Short .................................................................................... 452

Chapter 17 • Migrating to Active Directory ................................. 453
  Options for Migration ............................................................ 454
  NT to AD Migration ............................................................... 454
    In-Place Upgrade ............................................................... 455
    Over-the-Wire Migration ...................................................... 455
  Migrating from NetWare to AD ............................................... 471
    Bindery Services ............................................................... 472
    Novell Directory Service (NDS) ............................................. 472
    Microsoft’s Migration Path for NetWare ............................... 472
In Short .................................................................................... 473

Chapter 18 • Integrating Active Directory with Novell Directory Services . . 475
  Setting Up Client Services for NetWare (CSNW) ....................... 476
    Installing NWLink ............................................................. 477
  Comparing Directory Services .............................................. 480
    The Development of Novell’s and Microsoft’s Directory Services 481
    Microsoft vs. Novell .......................................................... 481
  The Future of Directory Services .......................................... 486
    Directory Enabled Networking ......................................... 487
    Microsoft Metadirectory Services ....................................... 488
    DirXML ............................................................................. 488
In Short .................................................................................... 489

Index .......................................................................................... 491
Introduction

Even though I have written books revolving around Microsoft products, I have never tried to hide the fact that I started out as a Novell guru (heck—I was even a Novell employee for awhile). When Microsoft first released Windows NT, I was amazed at the number of people who bought into that “New Technology” (NT) marketing line. Their “new technology”—or at least the networking portion of it—had been developed a good 10 years earlier for an IBM product named LanManager. (A search through the Registry of any NT computer for the word “Lanman” will prove this.) So Microsoft was releasing a product based on a 10-year-old networking philosophy and which used a nonroutable communication protocol by default. It didn't seem all that “new” to me!

Windows 2000/Windows Server 2003 moved Microsoft networking away from the dated and limiting domain-based architecture of earlier releases and toward the true directory service–based architecture necessary in today’s complex networks. Microsoft provides this service through the addition of Active Directory (AD), an open, standards-based, X.500-compliant, LDAP-accessible network directory. (Don’t worry—we’ll talk about X.500, LDAP, and what seems like an endless list of industry acronyms throughout this book.)

The first commercially viable, directory service–based operating system to hit the networking industry was Novell's NetWare 4 with NetWare Directory Services (NDS). At the time of its release, I was working as a senior technical instructor for a company in Minneapolis, Minnesota. In order to be one step ahead of the competition, my company sent me to the prep classes taught on the beta version of the software. After two weeks of intensive training on NDS, I returned home and started to reevaluate my career choices. It seemed as if everything I knew about networking was about to become out-of-date, and I would be forced to master this new paradigm known as a “directory service.” I have to admit that when I first saw Novell's directory service, I didn’t get it, didn’t think I would ever get it, and wasn’t sure I wanted to get it. I felt safe with earlier versions of NetWare, and I couldn’t understand why anyone would want to add the complexity of a directory service to their network. In the long run, however, the benefits of a directory service far outweighed the painful learning curve. With the release of Active Directory as part of the Windows 2000 Server product, Microsoft finally provided these benefits to its customer base. (And, I hope, this manual will help reduce the pain involved in mastering the technology!)

AD provides the power and flexibility you need in today’s changing computer world, but it provides these at a price. A large portion of that price is the steep learning curve that administrators
need to climb in order to fully understand and utilize the potential of Microsoft Windows 2000/Windows Server 2003 and Active Directory Services. However, the benefits of using Active Directory speak for themselves:

**A More Stable Operating System** You will see far fewer “blue screens” than ever before in a Microsoft environment. You can also say goodbye to the weekly (or more) reboots necessary to keep an NT server up and running.

**Group Policies** Controlling the end user’s environment—what they can see, what they can change, and what they can do—is critical as our operating systems become more and more sophisticated.

**Software Distribution** Statistics show that we (network professionals) spend more time installing and maintaining end-user applications than any other aspect of our job. Automating these processes will allow us to (finally) use some of that vacation time we have accumulated over the years!

I wrote this book to help you avoid being caught by surprise by Microsoft Windows 2000/Windows Server 2003 and Active Directory. While a network directory might be a new paradigm in networking for you, try to remember that at its most basic, networking technology—whether Windows 2000/Windows Server 2003, AD, or anything else—is still just moving bits from one place to another. All of the knowledge you have gathered about networking is still valid; you’ll just have a few more options available to you.

**What’s in This Book?**

When I was planning the table of contents for this book, I struggled with how best to present a new paradigm for Microsoft networking—the concept of a network directory. It was suggested that I just write about Active Directory Services and leave it at that, but I wanted to give you a conceptual overview of the technology as well as a look at AD. I decided that a three-part book would suit my goals. Read on to learn what’s in each part.

**PART 1: NETWORK DIRECTORY ESSENTIALS**

No matter what Microsoft would have you believe, network directories have been around for quite some time. Understanding earlier implementations (both their strengths and weaknesses) can help us understand why AD works the way it does—and perhaps help us realize some of its weaknesses. Part 1 is fairly short, but it is filled with conceptual information that can really help you tie AD to your environment. Part 1 contains four chapters.

**Chapter 1: An Introduction to Network Directory Services and Their Benefits** This chapter gives a basic overview of what a directory is and what Active Directory is, and it compares directories to older technologies.

**Chapter 2: Anatomy of a Directory** In this chapter, you will learn what a directory is by looking at examples of existing technologies, starting with basic paper-based directories and working up to the directories used in today’s networks.

**Chapter 3: Inside an X.500-Compliant Directory** Read this chapter for an overview of the X.500 recommendations, which are used to create the structure of the Active Directory database.
We also discuss the process of creating a directory service database from the ground up—a mental exercise that can really help you understand what makes Active Directory tick.

Chapter 4: Accessing the Directory  Chapter 4 explains DAP and LDAP, the two protocols used to access the information stored within the AD database.

PART 2: MICROSOFT ACTIVE DIRECTORY SERVICES

Once we have a firm grounding in directory technology, we can look at AD with a critical eye, trying to find its strengths and weaknesses. With this information, we can better apply the technology within our own environments. There are nine chapters in Part 2.

Chapter 5: Microsoft Networks without AD  To fully appreciate Windows 2000/Windows Server 2003, and especially Active Directory, it is important to understand earlier versions of NT. If you are an NT expert, this chapter will be a review. If you are a newcomer to the NT world, this chapter should prepare you for some of the topics you will encounter later in the book.

Chapter 6: Active Directory Benefits  Just as NT was originally designed to overcome the weaknesses of server-centric environments, Windows 2000/Windows Server 2003 with AD was designed to overcome the weaknesses of domain-based environments. In this chapter, we will discuss how AD fits into the overall Windows 2000/Windows Server 2003 philosophy.

Chapter 7: Network Support Services  While Microsoft 2000/Windows Server 2003 can utilize many different protocols for communication, AD depends on TCP/IP. Before you can begin to install and configure an AD environment, you must have a strong foundation in TCP/IP tools and techniques.

Chapter 8: Designing the Active Directory Environment  In this chapter, you will read about the theories of designing a stable AD structure that does not place undue stress on any single component of your network.

Chapter 9: Implementing Your Design  Read Chapter 9 to find out about the mechanics of AD installation and building your AD structure.

Chapter 10: Creating a Secure Environment  If the AD database is going to be of any real use in a network, the information it contains must be secure. In this chapter, we will look at the various security options available with Windows 2000/Windows Server 2003.

Chapter 11: Implementing Group Policies  Group Policies are used to define user or computer settings for an entire group of users or computers at one time. As such, they will be a very important concept for administrators of networks based on Windows 2000/Windows Server 2003. In Chapter 11, we will discuss the concept of Group Policies and look at the procedures used to implement them.

Chapter 12: Modifying the Active Directory Schema  The AD database contains object classes, which define types of network resources, and attributes, which define parameters of those classes. The default list of classes and attributes might not be sufficient in some environments. Chapter 12 discusses the process of extending the design of the AD database to include custom object classes and attributes.
Chapter 13: Understanding and Controlling AD Sites and Replication  For any network operating system, no matter how logical we make the structure or how graphical we make the interface, when all is said and done, everything comes back to the plumbing—the “pipes” we use to move data. This chapter looks at design issues with an eye on available bandwidth and communication costs.

PART 3: ADVANCED ACTIVE DIRECTORY ADMINISTRATION
So far we have gotten a history of the technology upon which Active Directory was built—sort of a historical perspective, if you will—in Part 1. In Part 2, we looked at the basic structure of an Active Directory environment—design strategies, traffic considerations, and the peripheral components found in most AD environments. In Part 3 we take an in-depth look at specific components of Active Directory implementations.

Chapter 14: Active Directory Network Traffic  A complete description of devices and services that generate traffic on your network. While no one could ever describe every bit that will pass through a network wire, we’ll look at those services that revolve around Active Directory: DNS, WINS, DHCP, AD replication, and others.

Chapter 15: Backup and Recovery of Active Directory  Everyone knows that good backups are critical to job security—and just about everyone in the business can describe the basics of server backup. What many don’t understand are the intricacies of backing up a complex database such as Active Directory. We’ll look at the theories and the tools involved in backing up and restoring Active Directory.

Chapter 16: Active Directory Design  There are more ways to design a hierarchical system than there are people to describe them. We’ll look at some of the network and business details that will impact your final AD design. We’ll also provide a few “cookie cutter” designs that can act as the foundation of your own network.

Chapter 17: Migrating to Active Directory  Very few of us have the luxury of starting from scratch—we inherit a network and then want to upgrade it to match our perceived needs. In this chapter we’ll discuss the options available when you want to upgrade your existing network to Windows 2000 and Active Directory.

Chapter 18: Integrating Active Directory with Novell Directory Services  Novell still holds a significant portion of the business networking market. Some recent surveys have even shown that NetWare’s market share might be increasing. Even in those companies where all new servers are Microsoft-based, many still continue to support legacy NetWare servers. The odds are that you will face a mixed environment at some time in your career. In this chapter we’ll discuss the tools and techniques available to help ease the pain of supporting two platforms: AD and NDS.

Who Should Read This Book?
This book was written for the experienced network administrator who wants to take a look at Microsoft’s Active Directory Services. I’m going to assume a basic level of knowledge of networking in general, but no (or little) knowledge of directory-based technologies. It seems as though whatever Microsoft is
doing is what the industry moves toward—and Microsoft is doing network directories in a big way! If you run a Microsoft house, you’ll need to come up to speed on AD quickly. If you run a non-Microsoft house (or older versions of Microsoft NT), you can bet that sooner or later you’ll need to understand how Microsoft views network directories.

In my 10 years as a technical instructor, I found that there were basically two types of students—those that just wanted to know the “how,” and those who also wanted to know the “why.” I feel that this book will satisfy both types of computer professionals. We certainly delve into the theoretical—discussing the history of network directories, the philosophy of management of directories, and the environment-specific aspects of AD that will effect your final design. We also discuss and describe many of the more common administrative tasks that you will be required to perform on a daily basis. That mix of both theory and concrete should prepare you for the task of implementing and maintaining an Active Directory structure in your work environment.

I guess the bottom line is this: if you are in networking today and you plan to be in networking tomorrow, you will have to master the concepts of a network directory at some point in your career. This book is designed to give you the information you need to understand and implement Microsoft’s interpretation of that technology.

**In Short**

Microsoft Windows 2000/Windows Server 2003 is the hottest technology in networking today. To use it effectively, you might have to rethink how you characterize network resources and services. The days of putting in the network and then considering the environment are long gone! With today’s technologies, each network will have to be designed around a “total business solution”—providing the resources and services necessary without unduly taxing the budget, staff, or infrastructure of the host company.

One last word of advice: enjoy what you do. New technology can be exciting, challenging, and downright fun. If you spend more time complaining about the technology than being amazed by it, perhaps a vacation is in order!

As with all my books, if you have questions or comments about the content, do not hesitate to drop me a note at bking@royal-tech.com. I always look forward to hearing from you.
Part 1

Network Directories Essentials

In this section you will learn how to:
- Evaluate network directory services and their benefits
- Understand the critical features of directory systems
- Design a generic directory
- Access the directory
This page intentionally left blank
Chapter 1

An Introduction to Network Directory Services and Their Benefits

The computer industry, especially in the networking arena, generates more acronyms, terms, phrases, and buzzwords than any other business in the world. The latest craze is the phrase network directories. Directories are nothing new—they have been around in one form or another since the late ’60s. Now, however, they have entered the mainstream with the release of Microsoft’s long-awaited Active Directory Services in Windows 2000 Server and the Windows Server 2003 product line. To get the most from this technology, you must have a firm understanding of what directories are, what they are not, and how they can be used to ease the management of your network. That is the goal of this book—to give you enough information to implement, manage, and utilize the services provided by Microsoft’s Active Directory Services (ADS). (While this directory is just another feature of the Windows 2000/Windows Server 2003 environment, it has reached the status of some rock stars—a shortened name. Microsoft’s directory service is usually referred to as just Active Directory or AD. This is the terminology that I’ll use throughout the book.)

PC-based networks have become an integral part of the business world. They started out as simple solutions for the sharing of a few physical resources—hard disk space, printers, and so on. Over time, though, networks have become quite complex—often spanning multiple sites, connecting thousands of users to a multitude of resources. Today, networks control everything from payroll information to e-mail communication, from printers to fax services. As networks offer more services, they also demand more management. Easing the use and management of networks is the real goal of a directory service.

This first chapter is more about setting the appropriate mood for the first section of the book than it is about technology. Directories have the ability to ease (or sometimes even eliminate) some of the most common IT administrative tasks. In this chapter we’ll look at a few of those tasks, think about how we would perform them in a “traditional” network, and then imagine the ways in
which a directory could make them easier to deal with. The bottom line here is that directories are exciting technology—and I want you to start getting excited about them! To effect that excitement, though, you need to have a firm grasp on the “concept” of a directory. The first part of this chapter will define that term, explain the benefits of using a directory, and describe the basic structure used by most network directories on the market today.

I’ve been in this business for a long time, and I know the typical work environment in an IT department. First, IT workers are often assumed to be nocturnal—we do our most important tasks (server maintenance, data backups, upgrades, etc.) after everyone else has gone home for the day (or worse, for the weekend or holiday!). Second, IT staff members are assumed to be workaholics. Why else would they give us vacation time that we never seem to be able to use? I don’t know how many times I’ve heard of IT staffers who lose their vacation time at the end of the year because they could never use it—there was always something going on that prevented them from leaving for a week or so. Lastly, we are assumed to know everything (and while we like this image, it sometimes causes problems). How many training classes have you attended in the last year? How many would you have liked to attend? If those two numbers are equal (or even close), you work for a great company! Too often, IT workers are given little training, and this results in more late hours, more headaches, and less opportunities to use vacation time.

Most administrators are overworked and underpaid. Most IT departments are understaffed and underbudgeted. This results in IT professionals who never see their families, never have time to attend classes (which just exacerbates the problem), and very seldom have time for relaxation—no wonder so many of us switch careers during our midlife crisis!

When properly installed and configured, Active Directory can often reduce the administrative overhead of maintaining your network. Certain tasks are completely eliminated, many redundant tasks are reduced to a single step, and most management processes are made easier to accomplish. The bottom line is that your workday is made more productive—allowing you to accept more responsibility, utilize your vacation time, and, just maybe, attend a few of the training events and industry seminars that you have on your wish list. (Okay, that’s the optimistic view. More likely, your company will see that the number of IT staff members required is not as great, and you end up with a smaller IT staff. This isn’t all that bad though, because a smaller staff often results in higher salaries… a win-win situation!)

Get excited about Active Directory! While it does require you to master a new paradigm (read that as a learning curve to climb), it also provides you with the opportunity to work more efficiently! This often results in the IT department adding new (and exciting) technologies to their systems. If you’re like me, working with the latest and greatest technology is just another perk in the workplace!

In this chapter:

◆ What is a directory service?
◆ Why use a directory service?
◆ Before there were network directories…
Traditional networks vs. network directories

Benefits of Active Directory

The Active Directory structure

The Active Directory feature set

What Is a Directory Service?

In any business-level networked environment, there exists some sort of database of account information. In Windows NT, this database was known as the Security Accounts Manager (SAM) database, and in early versions of Novell NetWare, it was known as the bindery. No matter what network operating system you look at, there has to be a place in which information about valid users is stored—things like names, passwords, and maybe even a little security information.

In many operating systems, this accounts database is server- or resource-centric. By this I mean that the database only stores information about users who have access to the resources (files, printers, applications, etc.) located within the sphere of control of the device upon which the database is stored. Novell’s bindery is a perfect example; it stored account information for users who could access a specific server (the server in which the bindery files were located). While this type of system is workable in smaller environments, it begins to fall apart as networks grow. Think about it: if every server has its own accounts database, and I have 100 servers, then I have 100 accounts databases to manage.

A directory service is a networkwide database that stores resource information, such as user accounts. In a directory-based environment, I create a single user account for each user, and that account is used to manage all aspects of the user’s network (and sometimes desktop) environment. To put this another way, a directory service provides a place to store information about network-based entities, such as applications, files, printers, or people. Given the networkwide scope of such a database, it provides a consistent way to name, describe, locate, access, manage, and secure information about those individual resources.

The directory also acts as the central point of control and management for the network operating system. It acts as the central authority to properly identify and authenticate the identities of resources, and it brokers the relationships between distributed resources, thus allowing them to work together. The directory service must be tightly coupled with the underlying operating system to ensure the integrity and privacy of information on the network.

In a Microsoft-based network, the Active Directory Service plays a critical role in an organization’s ability to manage the network infrastructure, perform system administration, and control the user environment.

Why Use a Directory Service?

When I first started in the networking industry, I worked on what, at the time, was a midsized environment—we had four servers and about 200 users. The Internet was still a thing of the future,
e-mail wasn’t mission critical (heck, most people didn’t even know what e-mail was), there was no such thing as a “fax server” or any other kind of specialized server for that matter, and FedEx was used to transfer documents from one site to another (no one would have thought to invest in a wide area link for a medium-sized company—they were too expensive).

Today, a midsized environment can include 50 or more servers, support hundreds, if not thousands, of users, and include numerous special services that run on dedicated servers. Wide area links are common, and bandwidth demands are astronomic! Not to mention the dial-in, VPN, and other “new” services that end users are demanding. In these complex networks, the task of managing the multitude of network-based resources can be overwhelming.

Directories help administrators manage today’s complex environments by:

- Simplifying management. By acting as a single point of management (and providing a consistent set of management tools), a directory can ease the administrative tasks associated with complex networks.

- Providing stronger security. Once again, the fact that access and authentication is controlled through a single service, administrators and users are only required to know a single set of tools, allowing them to develop a better understanding of them. Directories, since they offer a single logon facility, are usually able to provide a more secure authentication process (since all logons are managed through a central service, that service can be made extremely secure).

- Promoting interoperability. Most of today’s commercially viable directory services (AD included) are based upon a series of industry standards—X.500 and LDAP to name a few (I’ll describe these in detail later). Sticking with a standards-based solution makes it easier to share resources in a mixed environment or, better yet, to share resources with business partners without opening too many doors into your network.

Directories can be thought of as both a management and a user tool. From a management perspective, having a centrally controlled and consistent interface to resource information can drastically reduce administrative costs. From a user’s perspective, a central service for authentication can make accessing resources throughout the network a lot easier. Gone are the days when users had to memorize (or worse, write on a Post-It note) multiple logon names and passwords!

**Before There Were Network Directories...**

To understand and appreciate the power and convenience of a directory-based solution, you must have an understanding of the technologies that it will replace. Before the advent of directories, most network operating systems (NOSs) were “server-based.” In other words, most account management was done on a server-by-server basis. With older NOS software, each server maintained a list of users (the accounts database) who could access its resources and the users’ permissions (the Access Control List, or ACL). If a system had two servers, then each server had a separate accounts database, as shown in Figure 1.1.
As you can see, each server in Figure 1.1 maintains its own list of authorized users and manages its own resources. While this system is simple and easy to understand, it becomes unwieldy once a system grows past a certain point. Imagine trying to manage 10,000 users on 250 servers—the user and resource lists would soon overwhelm you! To get around this limitation, some NOS software, such as Microsoft NT 4, was configured so that small groups of servers could share one list of users (called a central accounts database) for security and authentication purposes, as shown in Figure 1.2. This central accounts database gave administrators a single point of management for a section of their network, known as a domain. Once again, however, this system becomes cumbersome after it reaches a certain size.

**Figure 1.2**
NT 4 security accounts database
The shift from server-based to domain-based networks was the first step in creating an environment where all users and resources are managed through a single database. In a domain, all user information is stored in a single place and managed with a single set of tools, and users can access the network via a single account (no more having to remember multiple account names and passwords). Network directories take this approach to the next phase: a single database to hold all user and resource information across your entire network.

**NOTE**  I’m using the phrase “user and resource” to refer to the records within a directory database because that is how traditional administrators see their world: users accessing resources. In a directory-based environment, however, users become nothing more than another resource. This subtle shift in philosophy is critical in understanding the strengths of a directory-based network. This distinction should become clear as you become more familiar with directory concepts.

Network directories are just databases that hold network information. They can contain many different types of information:

- User account information (logon name, password, restrictions)
- User personal information (phone number, address, employee ID number)
- Peripheral configuration information (printers, modem, fax)
- Application configuration (Desktop preferences, default directories)
- Security information
- Network infrastructure configuration (routers, proxies, Internet access settings)

If you can imagine it, a network directory can store it!

Once this information is stored in a centrally controlled, standards-based database, it can be used in many different ways. Most commonly, administrators will use such information to control access to the network and the network’s resources. The directory will become the central control point for many different network processes. Here are examples of some of these processes:

- When a user attempts to log on to the network, the client software will request authentication from the directory. The directory service will ascertain whether the account name is valid, check for a password, validate the password submitted, and check any restrictions on the account to determine if the logon request should be granted.

- Individual users can use directories to store personal preferences. Each time a user logs on to the network, his Desktop settings, default printer, home directory location—even his application icons—can be downloaded to whatever computer he happens to be at. Users will no longer have to re-create their environment each time they use a new computer. All of their settings will be centrally located to ensure a “universal environment” and, if you desire, centrally controlled to lock them down.

- As directories mature, you will also be able to use them to monitor and control traffic across network devices. When a user attempts to access a remote network, for instance, the directory could be used to determine whether the request is valid for that user. Imagine controlling Internet access with the same tool you use to control other security settings. Or perhaps the
directory could query various devices to determine the least congested network path to the destination. You might even be able to grant higher network priority to certain users, groups, applications, or services, allowing you to provide a guaranteed level of service.

**Traditional Networks vs. Network Directories**

Many network tasks can benefit from the capabilities of a network directory. Many of the hardest configuration issues of earlier networks will become a piece of cake when you use a network directory as the central controlling point for the network.

**Traditional Network Solutions for Common Administrative Tasks**

As food for thought, let’s consider a few common networking tasks and the nondirectory solutions to them. Each of these scenarios is a “real-world” implementation that I have been asked to complete on production networks. As you will see, the nondirectory-based solutions often border on the ridiculous. In some cases, the service provided could not justify the time spent to provide the requested solution. In other words, the constraints placed upon networks by traditional management techniques often limit the services that a network can realistically provide.

**Scenario 1: To Trust or Not to Trust**

Your company’s marketing department has a Color Wax Thermal Transfer Graphics printer, which is used to create camera-ready art for the company that prints your sales brochures. Because of the cost of consumables, which is somewhere in the neighborhood of $3.00 per page, you have been very careful about who is allowed to print to this device. Luckily, the marketing department is its own domain, so security has been fairly easy to maintain. Over in the engineering department, Susan has decided that she needs to print drawings of prototypes on this printer. Your job is to arrange the appropriate permissions.

In a multidomain environment, there are two basic ways to handle this situation:

- **You could** create a trust between the marketing domain and the engineering domain, create a global group in the engineering domain, place Susan’s account in the group, and then place that global group in the appropriate local group in the marketing domain. While this solution is great for Susan, it does mean that you now have to keep track of another trust relationship, not to mention the associated local and global groups.

- **You could** create a local account for Susan in the marketing domain and teach Susan to “Connect As” to use the printer. Now, of course, you’ve lost one of the biggest benefits of the domain concept—one user, one login.

**Scenario 2: Where’s Joe?**

An executive calls to inform you that a user named Joe in the sales department has been overheard discussing confidential information, including future product designs and marketing strategies. This executive would like a detailed explanation about where Joe has permissions and how they are acquired. She would also like you to ensure that Joe only has rights to resources appropriate for salespeople.