MCSA/MCSE: Windows® Server 2003 Network Simulator™

James Chellis
Matthew Sheltz

San Francisco • London

SYBEX®

Publisher: Neil Edde
Acquisitions and Developmental Editor: Jeff Kellum
Production Editor: Elizabeth Campbell
Technical Editor: Craig Vazquez
Copyeditor: Suzanne Goraj
Compositor: Judy Fung
Proofreader: Nancy Riddiough
Book Designer: Judy Fung

Library of Congress Card Number: 2003115546

ISBN: 0-7821-5024-1

Software License Agreement: Terms and Conditions

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

Software Support

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

Warranty

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

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

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

Disclaimer

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

Shareware Distribution

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

Copy Protection

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

Contents

Getting Started

The Sybex *MCSA/MCSE: Windows Server 2003 Network Simulator* gives you the most realistic and sophisticated Windows Server 2003 simulation tool on the market today. With this simulator, you can complete many tasks that normally would require a complex and costly installation. Programmed by Exam Solutions, the same company that created Microsoft's own exam simulations, this simulator was designed to integrate closely with the best-selling Microsoft certification Study Guide series published by Sybex.

Learning with the MCSA/MCSE: Windows Server 2003 Network Simulator

This Network Simulator is an instructional tool that simulates many components of a Windows Server 2003 network. You can use it to learn how to administer Windows Server 2003 without the need for an expensive computer lab.

Nothing beats hands-on experience. You learn by doing. With the Network Simulator, you can learn by interacting with a virtual network in a safe environment. Unlike practicing on "live" equipment, you do not have to worry about bringing down a network and affecting others. This is your private network: You can work with it without any concerns or pre-configuration issues, and you can start over as many times as you want.

You will notice that throughout this guide, a number of the labs have real-world requirements, depicted by the icon here. Real-world requirements represent prerequisites that you would need to have in place if you were to perform this lab in a live environment. In the Network Simulator you can assume that the real-world requirements have already been met.

People learn best when they can practice with realistic situations that model an actual working environment. Because these simulations are highly functional, you will find that the skills you acquire working with this Virtual Lab carry over into your live working environment.

Most of the labs cover material that is explained in detail in *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide* (Sybex, 2003) by Lisa Donald, Suzan Sage London, and James Chellis; *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide* (Sybex, 2003) by James Chellis, Paul Robichaux, and Matt Sheltz; *MCSE: Windows Server 2003 Network Infrastructure Planning and Maintenance Study Guide* (Sybex, 2003) by Suzan Sage London and James Chellis; and *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide* (Sybex, 2003) by Anil Desai and James Chellis. You should have a copy of the Study Guides close at hand while performing these labs.

Installing the MCSA/MCSE: Windows Server 2003 Network Simulator

The *MCSA/MCSE: Windows Server 2003 Network Simulator*'s installer will launch automatically if auto-run is enabled on your computer. If auto-run has been disabled, you will need to run `setup.exe`, which is located in the root folder of the *MCSA/MCSE: Windows Server 2003 Network Simulator* CD-ROM.

Once the installer launches, click Next at the welcome screen of the InstallShield wizard. Enter your personal information and choose who may use the application. Click the Next button to move to the next screen of the InstallShield wizard. Click the Change button on the Destination Folder screen to change the folder in which the installed files will be stored, or just click Next to accept the default and move on to the next screen. Verify that all the information is correct and click the Install button to complete the installation.

Launch the *MCSA/MCSE: Windows Server 2003 Network Simulator* by selecting Start ➢ All Programs ➢ Sybex ➢ Windows Server 2003 Network Simulator.

Please note that even after the software has been installed, the CD must be present in the drive in order for the software to run. If you encounter problems with the CD, please read the `readme.txt` file on the root of the CD for support information.

The program uses the Shockwave plug-in. If your system currently does not have Shockwave, it will auto-install when you install the *MCSA/MCSE: Windows Server 2003 Network Simulator*.

Getting Started on the Labs

The Network Simulator offers a wide range of exercises that are organized in the navigation screen. The navigation screen gives you immediate access to all of the individual labs.

The navigation screen presents four main Subjects, based on four core MCSA/MCSE exam requirements:

- *Managing and Maintaining a Microsoft Windows Server 2003 Environment*
- *Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure*
- *Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure*
- *Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure*

The labs in each main section build upon your experience in previous sections. You should complete the labs in order so that you don't miss anything you might be required to know later on.

To view the Topics available for each exam Subject, click the plus sign (+) next to the core exam in which you are interested. The Topics will then appear below that Subject. Each Topic corresponds with a chapter in the related study guide.

To view the individual labs available for each Topic, expand the Topic. The available labs will appear in the Current Subject pane to the right of the Subjects and Topics list.

The *MCSA/MCSE: Windows Server 2003 Network Simulator* offers two types of lab experiences:

- Open lab simulations
- Guided lab simulations

Open Labs

In the lab booklet, Open lab simulations are indicated by the icon appearing above.

In the navigation screen, open labs are indicated by a blue OPEN LAB label.

Open lab simulations re-create functionality from a wide variety of Windows Server 2003 utilities, without the need to install the operating system and establish a network environment. You can navigate through each open lab simulation in a variety of ways, because much of the functionality of the Windows Server 2003 environment has been simulated.

Clicking the Start Lab button while on an Open lab will open the Virtual Windows Server 2003 Desktop in a new window. The Virtual Windows Server 2003 Desktop is a simulated version of the actual Windows Server 2003 desktop. From there, you can perform most normal Windows Server 2003 tasks. Follow the steps of the lab text to complete the currently selected lab. In some cases, the final step of the lab text will indicate that you should leave the simulator window open. In these cases, simply continue on to the next lab in the list without closing any of the simulator windows. You will continue the next lab from the same point that you left the previous lab.

IMPORTANT! Many of the Open lab simulators allow you to save your configuration. For instance, if you have created several users, groups, and computers in the Active Directory Users and Computers tool, you can save the settings and return to them later. To save your settings, Click the Simulation pull-down menu and select Save This Configuration. Save the configuration anywhere on your hard drive. Be sure to use the .sim file extension. To load a configuration, simply choose the Load A Configuration option on the Simulation menu.

When you close an Open simulation window, you might see a warning dialog asking if you are sure you wish to close the simulation. You can click Yes to close the simulation, or No to leave it open and save your data for the next lab. When you close a simulation, all of the data that you entered is lost unless you save your configuration, as described above. Please note that sometimes the data you enter in a simulation is required to complete labs or exercises that follow. In those cases, the lab booklet instructs you to leave the simulation window open between labs.

Guided Labs

In the lab booklet, Guided simulations are indicated by the icon shown above.

In the navigation screen, guided labs are indicated by a red GUIDED LAB label.

Guided simulations guide you through each step of a particular administrative task. Each step of the task is displayed successively in the Guide window. With Guided simulations, you can't get lost. There is only one way to go: the right way! If you get stuck, you can click the Next button in the Guide window, and the Guided simulation will advance to the next step of the task.

Clicking the Start Lab button while on a Guided lab will open that guided lab in a new window. Simply follow the steps in the Guide window, then click Exit when you are done.

Features of the Navigation Screen

The navigation screen provides the following functions:

Lab Selector The left side of the screen displays an expandable list of the Subjects, Topics, and labs in the Windows Server 2003 Network Simulator. Expand a Subject to view the Topics contained within that Subject. Expand a Topic to view the labs contained within that Topic. Click a lab name to view the details and step-by-step instructions for that lab in the right side of the screen.

Start Lab Button Click the Start Lab button to begin the selected lab simulation. If the selected lab is an Open lab, then the Windows Server 2003 Virtual Desktop will appear. Use the steps in this lab manual to proceed. If the lab is a Guided lab, then the Guided lab will appear. Follow the steps in the guide, which closely match the steps listed here in this lab manual.

Checkmarks and the Remove Checkmarks Button When you visit a lab, a checkmark is placed next to that lab, indicating that you have visited that item. To reset the checkmarks and begin with a clean slate, click the Remove Checkmarks button.

Help Button Click the Help button to display the Help file for the *MCSA/MCSE: Windows Server 2003 Network Simulator*.

Exit Simulator Button Click the Exit Simulator button to exit the *MCSA/MCSE: Windows Server 2003 Network Simulator*.

Summary

In this introduction, you learned the basics of *MCSA/MCSE: Windows Server 2003 Network Simulator*. The lab is quite easy to operate, and yet the lab exercises offer variety and depth to help you learn to work with the product.

The Network Simulator is a great product, allowing individuals to complete exercises on a stand-alone computer that would normally require an expensive computer network and server operating software. Diligent use of the simulator will enhance your knowledge of Windows Server 2003 and take you one step closer toward your certification goals.

For upgrade information for this Virtual Lab, go to `www.comcourse.com/sim`.

Good luck with your studies!

Module

1

Managing and Maintaining a Microsoft Windows Server 2003 Environment

The Managing and Maintaining a Microsoft Windows Server 2003 Environment exam requires that you know how to perform many hands-on tasks using Windows Server 2003. While most study guides provide you with the steps you need to know in order to perform many of these tasks, most students studying for the exam do not have access to a fully configured Windows Server 2003 network, and they cannot perform the exercises.

The Managing and Maintaining a Microsoft Windows Server 2003 Environment module allows you to perform hands-on tasks in a simulated Windows environment. You can perform complicated exercises without the expense of a fully equipped network. If you get stuck, the simulator will show you how to perform the operation, just as if a live instructor were at your side pointing out what to do!

Most of the labs cover material that is explained in detail in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*, by Lisa Donald, with Suzan Sage London and James Chellis (Sybex, 2003). We recommend that you have a copy of the Study Guide close at hand while performing these labs.

Installing, Licensing, and Updating Windows Server 2003

In this section, you will join a Windows XP client to a Windows Server 2003 domain and configure licensing settings and Windows Update settings on a Windows Server 2003 computer.

This section corresponds to Chapter 1, "Installing, Licensing, and Updating Windows Server 2003," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 1.1: Joining an Existing Windows XP Professional Computer to a Windows 2003 Domain
- Exercise 1.2: Activating Windows Server 2003
- Exercise 1.3: Configuring the License Logging Service
- Exercise 1.4: Managing Per Server Licensing in a Single Server Environment
- Exercise 1.5: Using Windows Update
- Exercise 1.6: Configuring Automatic Updates

Exercise 1.1: Joining an Existing Windows XP Professional Computer to a Windows 2003 Domain

This exercise will show you how to join an existing computer to a domain.

1. From Windows XP Professional, select Start, right-click My Computer, and select Properties.
2. From the System Properties dialog box, select the Computer Name tab, then click the Network ID button.
3. The Network Identification Wizard will start. Click the Next button.
4. In the Connecting To The Network dialog box, verify that the This Computer Is Part Of A Business Network, And I Use It To Connect To Other Computers At Work option is selected and click the Next button.
5. The next question will ask what kind of network you use. Verify that the My Company Uses A Network With A Domain option is selected and click the Next button.
6. The Network Information dialog box will appear. Click the Next button.
7. The User Account And Domain Information dialog box will appear. For User Name, specify Administrator, and for Password and Domain, specify the options that are valid on your network. Since this is a simulated environment, you can use any password or domain name. Then click the Next button. Click Yes to continue.
8. The User Account dialog box will appear. Click the Do Not Add A User At This Time option and click the Next button.
9. The Completing The Network Identification Wizard dialog box will appear. Click the Finish button.
10. The Computer Name Changes dialog box will appear, notifying you that you need to restart the computer for the changes to take effect.

Exercise 1.2: Activating Windows Server 2003

In this exercise, you will activate Windows Server 2003.

If this were not a simulated environment you would need an Internet connection to complete the following exercise.

1. Select Start ➢ All Programs ➢ Activate Windows.
2. The Let's Activate Windows dialog box will appear. Select Yes, Let's Activate Windows Over The Internet Now and click the Next button.

3. The Register With Microsoft? dialog box will appear. Click the No, I Don't Want To Register Now; Let's Just Activate Windows option and click the Next button.
4. You will see a Thank You! dialog box indicating that you have successfully activated your copy of Windows. Click OK.
5. Leave the window open for the next lab.

Exercise 1.3: Configuring the License Logging Service

In this exercise, you will configure the License Logging service.

1. Select Start ➢ Administrative Tools ➢ Services.
2. Scroll down until you see the License Logging service, and double-click License Logging.
3. Click the Log On tab, and under Log On As, click Local System Account.
4. Click the General tab. Under Startup Type, select Automatic.
5. Under Service Status, click the Start button. The service will start and the Service Status will display Started. Click the OK button.
6. Close the Service window.
7. Leave the window open for the next lab.

Exercise 1.4: Managing Per Server Licensing in a Single Server Environment

In this exercise, you will administer Per Server licensing in a single server environment using the Licensing option in Control Panel.

1. Select Start ➢ Control Panel ➢ Licensing.
2. From the Choose Licensing Mode dialog box, click the Add Licenses button. (If you receive an error at this point, it's because the License Logging Service is not started.)
3. The New Client Access License dialog box will appear. In the Quantity field, click the up arrow once so that the quantity is 1 and click the OK button.
4. The Per Server Licensing Agreement dialog box will appear. Click the I Agree That: dialog box and click the OK button.
5. In the Choose Licensing Mode dialog box, you will see that your Per Server concurrent connections are listed as 6. Click OK.
6. Leave the window open for the next lab.

Exercise 1.5: Using Windows Update

In this exercise, you will use Windows Update.

1. Select Start ➢ Help And Support.
2. The Help And Support Center dialog box will appear.
3. Under Support Tasks, click the Windows Update option.
4. The Welcome To Windows Update screen will appear. Click Scan For Updates.
5. Windows Update will look for all available updates based on your computer's configuration.
6. A list of all updates for your computer will be listed. Click each option for Critical Updates And Service Packs, Windows Server 2003 Family, and Driver Updates and check the updates you want to install.
7. Click Review And Install Updates. In the Total Selected Updates section, click the Install Now button.
8. If you choose to restart the computer, the lab will return to the lab selection screen.

Exercise 1.6: Configuring Automatic Updates

In this exercise, you will configure Automatic Updates.

1. Select Start ➢ Control Panel ➢ System and click the Automatic Updates tab.
2. Verify that the Keep My Computer Up To Date option is checked.
3. Under Settings, select the Automatically Download The Updates, And Install Them On The Schedule That I Specify option. Select Every Sunday at 2:00 a.m. and click the OK button.
4. Leave the window open for the next lab.

Configuring Windows Server 2003 Hardware

In this section, you will configure your server's hardware.

This section corresponds to Chapter 2, "Configuring Windows Server 2003 Hardware," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 2.1: Using Device Manager
- Exercise 2.2: Managing Driver Signing
- Exercise 2.3: Updating a Device Driver
- Exercise 2.4: Using the System Information Utility

Exercise 2.1: Using Device Manager

In this exercise, you will use Device Manager to view your server's configuration and to print a report of your configuration.

1. Select Start ➢ Administrative Tools ➢ Computer Management. Expand System Tools, then Device Manager.
2. You will see a list of the devices that are installed on your computer. Expand Display Adapters, then double-click your display adapter.
3. Under the General tab, confirm that the Device Status is "This device is working properly."
4. Click the Driver tab, and note the digital signer for your driver.
5. Click the Resources tab and note the resources that are being used by your display adapter. Click OK to close the dialog box.
6. From the Computer Management Window, select View ➢ Resources By Connection. Expand the local machine, then expand Memory and you will see several memory ranges that have been used. Expand the memory range for PCI Bus and you should see the memory that is being used by your display adapter.
7. From the Computer Management Window, select View ➢ Devices By Type.
8. From the Computer Management Window, select Action ➢ Print. If you have a printer configured for your server, select All Devices And System Summary and click the Print button.
9. Close the Computer Management window.
10. Leave the window open for the next lab.

Exercise 2.2: Managing Driver Signing

In this exercise, you will check the setting for driver signing and run the File Signature Verification utility.

1. Select Start ➢ Control Panel ➢ System, click the Hardware tab, and under the Device Manager section, click the Driver Signing button.

2. In the Driver Signing Options dialog box, verify that the Warn radio button is selected and the Make This Action The System Default checkbox is checked.
3. Click the OK button to close the dialog box. Click the OK button within the System Properties dialog box.
4. Select Start ➢ Run. In the Run dialog box, type **`sigverif`** and click the OK button.
5. In the File Signature Verification window, click the Start button.
6. When the results of the signature verification appear, note whether the utility detected any files that were not digitally signed. From the Signature Verification dialog box, click the OK button.
7. From the File Signature Verification window, click the Advanced button, then the Logging tab.
8. From the Logging tab, click the View Log button. View the log file, and when done, close the log file. From the Advanced File Signature Verification Settings dialog box, click the OK button, then the Close button in the File Signature Verification window.
9. Leave the window open for the next lab.

Exercise 2.3: Updating a Device Driver

In this exercise, you will update a driver using Device Manager.

1. Select Start ➢ Administrative Tools ➢ Computer Management. Expand System Tools, then Device Manager.
2. The right side of the window lists all of the devices that are installed on your computer. Expand the Display Adapters item, then double-click the display device.
3. The display device's Properties dialog box appears. Click the Driver tab.
4. The Driver tab appears. Click the Update Driver button.
5. The Hardware Update Wizard starts. Select the Install From A List Or Specific Location (Advanced) radio button. Click the Next button.
6. The Hardware Update Wizard will continue and you will be asked to choose your search and installation options. Leave the options at the default setting and click Next. Specify which new driver you want to install and click the Next button
7. The files will be installed for your driver. Then you will see the Completing The Upgrade Device Driver Wizard dialog box. Click the Finish button to close this dialog box.
8. You may see a dialog box indicating that you must restart your computer before the change can be successfully implemented. Click Yes.
9. Leave the desktop window open for the next lab.

Exercise 2.4: Using the System Information Utility

In this exercise, you will use the System Information utility.

1. Select Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ System Information.
2. Review the System Summary for your server.
3. Expand System Summary, then Hardware Resources. Expand Conflict /Sharing to see the resources that are shared and to verify that no conflicts exist.
4. Select File ➢ Save to create a System Information file. Give the filename today's date, ***mmddyy***, and click the Save button. By default, an extension of `.nfo` will be applied.
5. Expand Software Environment. Click Signed Drivers to see a detailed listing of driver configurations for the drivers installed on your server.
6. Close the System Information utility.
7. Leave the window open for the next lab.

Managing Users, Groups, and Computers

In this section, you will create and edit users, groups, and computers in the domain with the Active Directory Users And Computers tool. You will also learn how to configure security settings for the security principals in the domain.

This section corresponds to Chapter 3, "Managing Users, Groups, and Computers," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 3.1: Setting Password Security Settings and User Rights Assignments
- Exercise 3.2: Creating Active Directory Users
- Exercise 3.3: Renaming a User
- Exercise 3.4: Changing a User's Password
- Exercise 3.5: Assigning a Home Folder to a User
- Exercise 3.6: Using User Account Templates
- Exercise 3.7: Creating and Managing an Active Directory Group

Exercise 3.1: Setting Password Security Settings and User Rights Assignments

In this exercise, you will set password security settings and user rights settings.

1. Select Start ➢ Administrative Tools ➢ Domain Security Policy.
2. Under Security Settings select Account Policies, Password Policy.
3. Double-click Minimum Password Length, and in the Minimum Password Length Properties dialog box, set the Password Must Be At Least field to 0. Click the Apply button, then the OK button.
4. Double-click Password Must Meet Complexity Requirements, and in the Password Must Meet Complexity Requirements Properties dialog box, click the Disabled radio button. Click the Apply button, then the OK button.
5. From the Default Domain Security Settings dialog box, select File ➢ Exit.
6. Select Start ➢ Administrative Tools ➢ Domain Controller Security Policy.
7. Under Security Settings, expand Local Policies, User Right Assignment.
8. Double-click Allow Log On Locally.
9. The Allow Log On Locally Properties dialog box will appear. Click the Define These Policy Settings Checkbox. Click the Add User Or Group button. The Add User Or Group dialog box will appear. In the User And Group Names field, type in Everyone and click the OK button. In the Allow Log On Locally Properties dialog box, click the Apply button, then the OK button.
10. From the Default Domain Controller Security Settings dialog box, select File ➢ Exit.
11. Leave the window open for the next lab.

Exercise 3.2: Creating Active Directory Users

In this exercise, you will create new domain user accounts.

1. Select Start ➢ Administrative Tools ➢ Active Directory Users And Computers.
2. In the Active Directory Users And Computers window, right-click Users, select New, and then select User.
3. In the first New Object–User dialog box, enter the following information:
   - First Name: **Ginnie**
   - Initial: **B.**
   - Last Name: **Donald**
   - User Logon Name: **Ginnie**

4. Click the Next button.
5. In the next New Object–User dialog box, type and confirm the password **girLYc@t**. Check the Password Never Expires checkbox and click OK on the warning message. Then click the Next button. Click finish when done.
6. Create six more users. For each user, uncheck the User Must Change Password At Next Logon checkbox. Fill out the fields as follows:
   - First Name: **Robert**; Last Name: **Jones**; User Logon Name: **Robert**; Password: **b4tm4n**
   - First Name: **Terry**; Last Name: **Belle**; User Logon Name: **Terry**; Password: **b4tg1rl**
   - First Name: **Ron**; Last Name: **Klein**; User Logon Name: **Ron**; Password: **sup3rm4n**
   - First Name: **Wendy**; Last Name: **Smith**; User Logon Name: **Wendy**; Password: **sup3rg1rl**
   - First Name: **Emily**; Last Name: **Buras**; User Logon Name: **Emily**; Password: **p34ch**
   - First Name: **Michael**; Last Name: **Phillips**; User Logon Name: **Michael**; Password: **4ppl3**
7. Leave the window open for the next lab.

Exercise 3.3: Renaming a User

In this exercise, you will rename a user account.

You need to complete all of the previous exercises in this section for this exercise to work correctly.

1. If it's not already open, select Start ➢ Administrative Tools ➢ Active Directory Users And Computers.
2. In the Active Directory Users And Computers window, click Users.
3. Right-click user Terry and select Rename.
4. Type in the username **Taralyn** and press Enter.
5. The Rename User dialog box will appear. Notice that the First Name retained the original property of Terry. Click OK.
6. Leave the window open for the next lab.

Exercise 3.4: Changing a User's Password

In this exercise, you will change a user's password.

You will have to have completed all of the previous exercises in this section for this exercise to work correctly.

1. If it's not already open, select Start ➢ Administrative Tools ➢ Active Directory Users And Computers.
2. In the Active Directory Users And Computers window, expand Users.
3. Right-click user Ron and select Reset Password.
4. The Reset Password dialog box will appear. Type **g0lf** in the New Password and Confirm Password fields. Check the box User Must Change Password At Next Logon to force Ron to change his password the next time he logs on. Click the OK button.
5. You will see an Active Directory Users And Computers dialog box appear confirming The Password For Ron Has Been Changed. Click the OK button.
6. Leave the window open for the next lab.

Exercise 3.5: Assigning a Home Folder to a User

In this exercise, you will assign a home folder to a user.

You will have to have completed all of the previous exercises in this section for this exercise to work correctly.

1. If it's not already open, select Start ➢ Administrative Tools ➢ Active Directory Users And Computers.
2. In the Active Directory Users And Computers window, expand the `Users` folder and double-click user Wendy. The user's Properties dialog box appears.
3. Select the Profile tab and click the Local Path radio button to select it.
4. Specify the home folder path by typing **C:\Users\Wendy** in the text box for the Local Path option. Then click the OK button.
5. Leave the window open for the next lab.

Exercise 3.6: Using User Account Templates

In this exercise, you will create a user account template and then create new users based on the template account.

1. If it's not already open, select Start ➢ Administrative Tools ➢ Active Directory Users And Computers.
2. In the Active Directory Users And Computers window, right-click Users, select New, and then select User.
3. In the first New Object–User dialog box, enter the following information:
   - First Name: **#Sales**
   - Last Name: **Template**
   - User Logon Name: **#Sales**
4. Click the Next button.
5. In the next New Object–User dialog box, do not specify any password. Check the Password Never Expires checkbox and click OK to close the warning. Click the Account Is Disabled checkbox. Then click the Next button. Click the Finish button.
6. Double-click #Sales to access the #Sales Template Properties dialog box.
7. Click the Address tab. For City, type in **Santa Cruz**. For State, type in **California**. For Zip/Postal Code, type in **95060**. For Country/Region, select United States from the pull-down list.
8. Click the Organization tab. For Department, type in **Sales**. For Company, type in **Wacky Widgets Corporation**. Click the OK button.
9. Right-click #Sales Template User and select Copy.
10. The Copy Object–User dialog box will appear. Enter the following information:
    - First Name: **Dietrich**
    - Last Name: **Moorehead**
    - User Logon Name: **Dietrich**
11. Click the Next button.
12. In the next New Object–User dialog box, do not specify any password. Uncheck the Account Is Disabled option. Then click the Next button. Click the Finish button.
13. Double-click user Dietrich and click the Address tab and the Organization tab to verify that the information was populated based on the settings configured for the #Sales account template. Click OK.
14. Leave the window open for the next lab.

Exercise 3.7: Creating and Managing an Active Directory Group

In this exercise, you will create and manage an Active Directory group.

You will have to have completed all of the previous exercises in this section for this exercise to work correctly.

1. If it's not already open, select Start ➢ Administrative Tools ➢ Active Directory Users And Computers.
2. In the Active Directory Users And Computers utility, right-click the `Users` folder, select New, and then select Group.
3. In the New Object–Group dialog box, enter **Test Group** as the group name. Choose the Global option for the group scope and the Security option for the group type. Click the OK button.
4. In the Active Directory Users And Computers utility, right-click Test Group and select Properties.
5. In the Test Group Properties dialog box, click the Members tab and then click the Add button. Enter user **Ginnie** and click the OK button. In the Test Group Properties dialog box, click the OK button.
6. Close the Active Directory Users And Computers utility.
7. Leave the window open for the next lab.

Managing Disks

In this section, you will manage the server's disk configuration.

This section corresponds to Chapter 4, "Managing Disks," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 4.1: Creating a Partition
- Exercise 4.2: Converting a Basic Disk to a Dynamic Disk
- Exercise 4.3: Editing a Drive Letter
- Exercise 4.4: Compressing Folders and Files

Exercise 4.1: Creating a Partition

In this exercise, we will create a partition.

1. Select Start ➢ Administrative Tools ➢ Computer Management. Expand the `Storage` folder and click the Disk Management utility.
2. Right-click an area of unallocated space and choose the New Partition option from the pop-up menu.
3. The Welcome To The New Partition Wizard dialog box appears. Click the Next button to continue.
4. The Select Partition Type dialog box appears. In this dialog box, select the type of partition you want to create: primary, extended, or logical drive (you will only see logical drive as an active choice if you have already created an extended partition). Click the Primary Partition radio button, then click the Next button.
5. The Specify Partition Size dialog box appears. Here, you can specify the maximum partition size, up to the amount of free disk space that is recognized. In this exercise, specify 5012 MB and click Next.
6. The Assign Drive Letter Or Path dialog box appears. Through this dialog box, you can specify a drive letter, mount the partition as an empty folder, or choose not to assign a drive letter or drive path. If you choose to mount the volume as an empty folder, you can have an unlimited number of volumes, negating the drive-letter limitation. In this exercise, accept the default drive letter, then click the Next button.
7. The Format Partition dialog box appears. This dialog box allows you to choose whether or not you will format the partition. If you choose to format the volume, you can format it as FAT32 or NTFS. You can also select the allocation unit size, enter a volume label (for informative purposes), specify a quick format, or choose to enable file and folder compression. Specifying a quick format is risky, because it will not scan the disk for bad sectors (which is done in a normal format operation). In this exercise, accept the default value to format as NTFS (leave the other settings as their defaults) and click the Next button.
8. The Completing The Create Partition Wizard dialog box appears. Verify your selections. If you need to change any of them, click the Back button to reach the appropriate dialog box. Otherwise, click the Finish button.
9. Leave the window open for the next lab.

Exercise 4.2: Converting a Basic Disk to a Dynamic Disk

In this exercise, you will upgrade a basic disk to a dynamic disk.

1. If it's not already open, select Start ➢ Administrative Tools ➢ Computer Management. Expand the `Storage` folder to see the Disk Management utility. Click on the Disk Management utility.
2. Right-click Disk 0 and select Convert to Dynamic Disk.
3. The Convert To Dynamic Disk dialog box appears. Verify that Disk 0 is selected and click the OK button.

4. The Disks To Convert dialog box appears. Click the Convert button.
5. A confirmation dialog box warns you that you will no longer be able to boot previous versions of Windows from this disk. Click the Yes button to continue.
6. The next confirmation dialog box warns you that any file systems mounted on the disk will be dismounted. Click the Yes button to continue.
7. An information dialog box tells you that a reboot is required to complete the upgrade. Click the No button for now. The disk will remain a basic disk until you reboot.
8. Leave the window open for the next lab.

Exercise 4.3: Editing a Drive Letter

In this exercise, you will edit the drive letter of the partition you created in Exercise 4.1.

1. If it's not already open, select Start ➢ Administrative Tools ➢ Computer Management. Expand Storage, then click Disk Management.
2. Right-click your CD drive and select Change Drive Letter And Paths.
3. In the Change Drive Letter And Paths dialog box, click the Change button.
4. In the Edit Drive Letter Or Path dialog box, select a new drive letter L: and click the OK button.
5. In the confirmation dialog box, click the Yes button to confirm that you want to change the drive letter.
6. Right-click the partition you created in Exercise 4.1 and select Change Drive Letter And Paths.
7. In the Change Drive Letter And Paths dialog box, click the Change button.
8. In the Edit Drive Letter Or Path dialog box, select a new drive letter D: and click the OK button.
9. In the confirmation dialog box, click the Yes button to confirm that you want to change the drive letter.
10. Right-click your CD drive and select Change Drive Letter And Paths.
11. In the Change Drive Letter And Paths dialog box, click the Change button.
12. In the Change Drive Letter Or Path dialog box, select a new drive letter E: and click the OK button.
13. In the confirmation dialog box, click the Yes button to confirm that you want to change the drive letter.
14. Close the Computer Management window.
15. Leave the desktop open for the next lab.

Exercise 4.4: Compressing Folders and Files

In the following exercise, you will compress folders and files.

This exercise assumes that you have completed Exercise 4.1.

1. Select Start ➢ Windows Explorer.
2. Expand My Computer ➢ EN_WS03 (E:) ➢ WIN2003 ➢ Support, and click the Tools folder. Notice the list of files in the folder. Select all of the files, then click the Edit menu and select Copy. Now, expand Local Disk (D:) and click the Temp folder. Click the Edit menu and select Paste.
3. Right-click the Temp folder and select Properties. In the General tab of the folder's Properties dialog box, note the value listed for Size On Disk. Then click the Advanced button.
4. In the Advanced Attributes dialog box, check the Compress Contents To Save Disk Space option. Then click the OK button. In the folder's Properties dialog box, click the Apply button.
5. In the Confirm Attribute Changes dialog box, select Apply Changes To This Folder, Subfolders And Files (if this dialog box does not appear, click the Apply button in the folder Properties dialog box to display it). Then click the OK button.
6. In the General tab of the folder's Properties dialog box, note the value that now appears for Size On Disk. This size should have decreased because you compressed the folder. Click OK.
7. Leave the window open for the next lab.

Accessing Files and Folders

In this section, you will control access to the local computer's files and folders with NTFS and Share permissions.

This section corresponds to Chapter 5, "Accessing Files and Folders," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 5.1 Creating a Directory and File Structure
- Exercise 5.2 Configuring NTFS Permissions

- Exercise 5.3 Using Take Ownership
- Exercise 5.4 Creating a Shared Folder
- Exercise 5.5 Applying Share Permissions

Exercise 5.1: Creating a Directory and File Structure

In this exercise, you will create a directory structure that will be used throughout the exercises in this section.

If this were not a simulated environment, this exercise would need to be completed from your member server or XP Professional computer.

1. If it's not already open, select Start ➢ Windows Explorer.
2. In Windows Explorer, expand My Computer, then Local Disk (D:). Double-click the `Data` folder to open the folder. Select File ➢ New ➢ Folder and name the new folder **WP Docs**.
3. Double-click the `Data` folder, select File ➢ New ➢ Folder, and name the new folder **SS Docs**.
4. Confirm that you are still in the `Data` folder. Select File ➢ New ➢ Text Document. Name the file **`Doc1.txt`**.
5. Double-click the `WP Docs` folder. Select File ➢ New ➢ Text Document. Name the file **`Doc2.txt`**.
6. Double-click the `SS Docs` folder. Select File ➢ New ➢ Text Document. Name the file **`Doc3.txt`**.
7. Close all of the windows and return to the lab menu.

Exercise 5.2: Configuring NTFS Permissions

In this exercise, you will configure NTFS permissions. You need to complete Exercise 5.1 first.

This exercise would need to be completed from your member server or XP Professional computer.

1. Using the Active Directory Users And Computers utility, create two users: **Marilyn** and **Dan**. (See Exercise 3.2 to see how to create a user.) Deselect the User Must Change Password At Next Logon option.

2. Using the Active Directory Users And Computers utility, create four global security groups: **Accounting**, **Execs**, **Sales**, and **Temps**. Add Marilyn to the Accounting and Execs groups, and add Dan to the Sales and Temps groups.
3. Select Start ➢ Windows Explorer. Expand the `D:\Data` folder you created in Exercise 5.1.
4. Right-click the `Data` folder, select Properties, and click the Security tab.
5. In the Security tab of the folder's Properties dialog box, highlight the Users group and click the Remove button. You see a dialog box telling you that you cannot remove Users because it is inheriting permissions from a higher level. Click the OK button.
6. Click the Advanced button. Deselect the Allow Inheritable Permissions From The Parent To Propagate To This Object And All Child Objects checkbox, and click Copy in the Security dialog box in case you need to restore the permissions later. Click OK to exit the Advanced Security Settings dialog box. Now remove the Users group from the Security tab of the folder's Properties dialog box.
7. Configure NTFS permissions for the Accounting group by clicking the Add button. In the Select Users Or Groups dialog box, enter **Accounting; Execs; Sales; Temps**, and click the OK button.
8. In the Security tab, highlight each group and check the Allow or Deny checkboxes to add permissions as follows:
   - For Accounting, allow Read & Execute (List Folder Contents and Read will automatically be allowed) and Write.
   - For Execs, allow Read.
   - For Sales, allow Modify (Read & Execute, List Folder Contents, Read, and Write will automatically be allowed).
   - For Temps, deny Write.
9. Click the OK button to close the folder Properties dialog box.
10. You will see a Security dialog box cautioning you about the deny entry. Click the Yes button to continue.

Exercise 5.3: Using Take Ownership

In this exercise, you will configure NTFS permissions as a regular user and block access to a folder for all other users. You will then use the Take Ownership option to access the file as a member of the Administrators group.

1. Using the Active Directory Users And Computers utility, create a user named **Aaron**. (See Exercise 3.2 on how to create a user.) Deselect the User Must Change Password At Next Logon option.
2. Log on as Aaron and select Start ➢ My Computer
3. Open the D: drive and select File ➢ New ➢ Folder and name the new folder **Aaron's Data**.

4. Create a text file called **Secret.txt** in `D:\Aaron's Data`.
5. Right-click `Aaron's Data`, select Properties, and click the Security tab.
6. In the Security tab of the folder's Properties dialog box, highlight the Users group and click the Remove button. You see a dialog box telling you that you cannot remove Users because this group is inheriting permissions from a higher level. Click the OK button.
7. Click the Advanced button. Deselect the Allow Inheritable Permissions From The Parent To Propagate To This Object And All Child Objects checkbox, and click Copy in the Security dialog box in case you need to restore the permissions later. Click OK to exit the Advanced Security Settings dialog box. Now remove the Users group and the Administrators group from the Security tab of the folder's Properties dialog box. Click OK.
8. Log off as Aaron and log on as Administrator.
9. Try to access `D:\Aaron's Data\Secret.txt`. When you click `D:\Aaron's Data`, you will get an Access Is Denied error message. Click the OK button.
10. Right-click the Aaron's Data folder, select Properties, and click the Security tab. You may see a message that you do not have permission to view or edit the current permission settings for the folder but you can take ownership or change auditing settings. Click the OK button.
11. Click the Advanced button and select the Owner tab. Click on the Administrator account and check the box Replace Owner On Subcontainers And Objects and click the OK button.
12. The Security dialog box will appear notifying you that you do not have permissions to read the contents of the directory and asking you if you want to replace the directory permissions so that you are granted Full Control permission. Click the Yes button to replace all permissions. You will now have Full Control permission to the `Aaron's Data` folder and the `Secret.txt` file.

Exercise 5.4: Creating a Shared Folder

In this exercise, you will create a shared folder.

1. Select Start ➢ Windows Explorer. Expand My Computer, and then expand Local Disk (D:).
2. Select File ➢ New ➢ Folder and name the new folder **Share Me**.
3. Right-click the Share Me folder, select Properties, and click the Sharing tab.
4. In the Sharing tab of the folder's Properties dialog box, click the Share This Folder radio button.
5. Type **Test Shared Folder** in the Share Name text box.
6. Type **This is a comment for a shared folder** in the Description text box.
7. Under User Limit, click the Allow This Number Of Users radio button and specify 5 users.
8. Click the OK button to close the dialog box.
9. Leave the window open for the next lab.

Exercise 5.5: Applying Share Permissions

In this exercise, you will apply share permissions to a folder.

This exercise assumes that you have completed the other exercises in this section.

1. If it's not already open, select Start ➢ Windows Explorer. Expand My Computer, then expand Local Disk (D:).
2. Right-click the `Share Me` folder, select Sharing And Security, and click the Permissions button.
3. In the Share Permissions dialog box, highlight the Everyone group and click the Remove button. Then click the Add button.
4. In the Select Users, Computers, Or Groups dialog box, enter **Dan; Marilyn** and then click the OK button.
5. Click user Marilyn and check the Allow box for the Full Control permission.
6. Click user Dan and check the Allow box for the Read permission.
7. Click the OK button to close the dialog box, and click OK again to close the folder's Properties dialog box.
8. Close Windows Explorer.
9. Leave the desktop window open for the next lab.

Managing Web Services

In this section, you will manage Web services using IIS 6.0, which is all-new in Windows Server 2003.

This section corresponds to Chapter 6, "Managing Web Services," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 6.1: Enabling Web Service Extensions
- Exercise 6.2: Creating a New Website
- Exercise 6.3: Managing Websites

Exercise 6.1: Enabling Web Service Extensions

In this exercise, you will enable Web Service Extensions.

1. Select Start ➢ Administrative Tools ➢ Internet Information Services (IIS) Manager.
2. Click the Web Service Extensions directory. From Web Service Extensions listed on the right-hand side of the dialog box, select Active Server Pages and click Allow.
3. Select ASP .NET v1.1.4322 and click Allow.
4. Select Internet Data Connector and click Allow.
5. Select Server Side Includes and click Allow.
6. Select WebDAV and click Allow.
7. Leave the window open for the next exercise.

Exercise 6.2: Creating a New Website

In this exercise, you will create a new website.

This exercise assumes that you have completed Exercise 6.1.

1. Right-click Web Sites and select New ➢ Web Site.
2. The Web Site Creation Wizard starts. Click the Next button.
3. The Web Site Description dialog box appears. Under Description, type **Practice Web Site** and click the Next button.
4. The IP Address And Port Settings dialog box appears. Click the arrow for Enter The IP Address To Use For This Web Site and select the IP address of your Windows Server 2003 server. Click the Next button.
5. The Web Site Home Directory dialog box appears. Type in **C:\Practice Web Site** in the path field. Then, click the Next button.
6. The Web Site Access Permissions dialog box appears. Accept the default settings and click the Next button.
7. The Web Site Creation Wizard will tell you that you have successfully completed the Web Site Creation Wizard. Click the Finish button.
8. Leave the window open for the next exercise.

Exercise 6.3: Managing Websites

In this exercise, you will manage the properties of the website you created in Exercise 6.2.

This exercise assumes that you have completed Exercise 6.2.

1. If it's not already expanded, expand the server name and expand Web Sites. Right-click Practice Web Site and select Properties.
2. On the Practice Web Site tab, in the Connection Timeout option, specify **1200** seconds.
3. Click the Performance tab. Select the Connections Limited To option and specify 500 connections.
4. Click the Home Directory tab. Under the Execute Permissions option, select Scripts And Executables.
5. Click the OK button to close the Default Web Site Properties dialog box.
6. Close IIS.
7. Leave the desktop window open for the next lab.

Managing Printing

In this section, you will manage printing and printer sharing in Windows Server 2003.

This section corresponds to Chapter 7, "Managing Printing," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 7.1: Creating Printers
- Exercise 7.2: Sharing an Existing Printer
- Exercise 7.3: Managing Advanced Printer Properties
- Exercise 7.4: Assigning Print Permissions
- Exercise 7.5: Managing Printers and Print Documents
- Exercise 7.6: Monitoring Print Queue Status

Exercise 7.1: Creating Printers

In this exercise, you will manually create two local printers—one to share and one that will not be shared. You will manually specify their print device configuration.

To add the first printer, follow these steps:

1. Select Start ➢ Printers And Faxes.
2. Double-click the Add Printer icon. The Add Printer Wizard will start. Click the Next button to continue.
3. In the Local Or Network Printer dialog box, select the Local Printer Attached To This Computer radio button. Make sure that the Automatically Detect And Install My Plug And Play Printer checkbox is not checked and click the Next button.
4. In the Select The Printer Port dialog box, select the Use The Following Port radio button, select LPT1 in the list box, and click the Next button.
5. In the Install Printer Software dialog box, choose HP in the Manufacturer list box and HP OfficeJet Pro 1170Cxi in the Printers list box. Then click the Next button.
6. In the Name Your Printer dialog box, leave the default name of HP OfficeJet Pro 1170Cxi and click the Next button.
7. In the Printer Sharing dialog box, select the Share Name radio button and type **HPOJPro** in the Share Name text box. Then click the Next button.
8. In the Location And Comment dialog box, type **Training Room** in the Location text box and **Color Printer** in the Comment text box. Click the Next button.
9. In the Print Test Page dialog box, select the No radio button to skip printing a test page and click the Next button.
10. In the Completing The Add Printer Wizard dialog box, click the Finish button.

To add the second printer, follow these steps:

11. In the Printers And Faxes Control Panel, double-click the Add Printer icon.
12. When the Add Printer Wizard starts, click the Next button to continue.
13. In the Local Or Network Printer dialog box, select the Local Printer Attached To This Computer radio button. Make sure that Automatically Detect And Install My Plug And Play Printer is not checked and click the Next button.
14. In the Select The Printer Port dialog box, select the Use The Following Port radio button, select LPT2 in the list box, and click the Next button.
15. In the Install Printer Software dialog box that appears, choose HP in the Manufacturer list box and HP LaserJet 4Si in the Printers list box. Then click the Next button.
16. In the Name Your Printer dialog box, leave the default name of HP LaserJet 4Si and click the Next button.

17. In the Printer Sharing dialog box, select the Do Not Share This Printer radio button and click the Next button.
18. In the Print Test Page dialog box, select No to skip printing a test page and click the Next button.
19. In the Completing The Add Printer Wizard dialog box, click the Finish button.
20. Leave the window open for the next lab.

Exercise 7.2: Sharing an Existing Printer

In this exercise, you will share an existing printer.

This exercise assumes that you have completed Exercise 7.1.

1. If it's not already open, select Start ➢ Printers And Faxes, right-click HP LaserJet 4Si, and choose Properties.
2. Click the Sharing tab.
3. Click the Share This Printer radio button. Accept the default value, HPLaserJ.
4. Click the Apply button, then click the OK button to close the dialog box.
5. Leave the window open for the next lab.

Exercise 7.3: Managing Advanced Printer Properties

In this exercise, you will configure some advanced printer properties.

This exercise assumes you have completed Exercise 7.2.

1. If it's not already open, select Start ➢ Printers And Faxes, right-click HP LaserJet 4Si, and select Properties.
2. Click the Advanced tab.
3. Click the Available From radio button and specify that the printer is available from 12:00 A.M. to 6:00 A.M.
4. Click the Start Printing After Last Page Is Spooled radio button.

5. Click the Separator Page button. In the Separator Page dialog box, click the Browse button and choose the `sysprint.sep` file. Click the Open button, then click the OK button in the Separator Page dialog box.
6. Click the OK button to close the printer Properties dialog box.
7. Leave the window open for the next labs in this section.

Exercise 7.4: Assigning Print Permissions

In this exercise, you will assign print permissions.

This exercise assumes that you have completed Exercise 7.3.

1. Don't close the window from the previous lab yet. From your Windows Server 2003 domain controller, using the Active Directory Users And Computers utility, create two users named **Kim** and **Jennifer**. (See Exercise 3.2 on how to create a user.) Deselect the User Must Change Password At Next Logon option.
2. Using the Active Directory Users And Computers utility, verify that you have a group named **Execs**. If you do not, then create a new group called Execs. (See Exercise 3.7 on how to create a group.) Place Kim in the Execs group.
3. Switch to the Printers and Faxes window, right-click HP LaserJet 4Si, and select Properties.
4. Click the Security tab and click the Add button.
5. In the Select Users, Computers, Or Groups dialog box, type in **Execs**. Click the OK button to continue.
6. In the Security tab, highlight the Execs group. By default, the Allow checkbox should be selected for the Print permission. Leave the default setting. Highlight the Everyone group and click the Remove button. Click OK to close the Printer Properties dialog box and save the changes. Leave the window open for the next lab.

Exercise 7.5: Managing Printers and Print Documents

In this exercise, you will manage printers and print documents.

This exercise assumes that you have completed the previous exercises in this section.

1. Select Start ➢ Printers And Faxes, right-click HP LaserJet 4Si, and select Pause Printing.
2. Select Start ➢ All Programs ➢ Accessories ➢ Notepad.
3. Create a new text file and then select File ➢ Save As. In the Save As dialog box, save the file in the default location, My Documents, as **`PrintMe.txt`**. Click the Save button.
4. While still in Notepad, select File ➢ Print. Select HP LaserJet 4Si and click the Print button. Repeat this step two more times so that you have sent a total of three print jobs. Close Notepad.
5. Select Start ➢ Printers And Faxes and double-click HP LaserJet 4Si. At the top of the window, you will see that the status of the printer is Paused.
6. Right-click one of the print jobs in the print queue and select Cancel. The print job will be deleted after you confirm the cancellation.
7. Right-click one of the print jobs in the print queue and select Properties. The print job Properties dialog box appears. Change Notify from Administrator to Kim. Set the Priority from 1 to 99. For Schedule, select Only From 12:00 A.M. to 4:00 A.M. Then click the OK button.
8. Close all of the dialog boxes.

Exercise 7.6: Monitoring Print Queue Status

In this exercise, you will use the System Monitor utility to monitor print queue status.

1. Select Start ➢ Administrative Tools ➢ Performance.
2. From System Monitor, click the Add button (button that looks like a plus sign).
3. The Add Counters dialog box will appear.
4. Select the Print Queue Performance Object from the pull-down menu.
5. Click the All Counters radio button and the Add button. Click the Close button.

Administering Terminal Services

In this section, you will administer terminal services on the server.

This section corresponds to Chapter 8, "Administering Terminal Services," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 8.1: Installing a Terminal Services Server
- Exercise 8.2: Configuring a Terminal Services Server

Exercise 8.1: Installing a Terminal Services Server

In the following exercise, you install Terminal Services.

1. Select Start ➢ Control Panel ➢ Add Or Remove Programs.
2. In the Add Or Remove Programs window, click Add/Remove Windows Components.
3. The Windows Components Wizard will automatically start. Check the Terminal Server checkbox and click the Next button.
4. The Terminal Server Setup page will appear. You'll be presented with information notifying you that certain applications may not work properly after installing Terminal Services in Terminal Server mode and that you will need to have Terminal Server Licensing configured within 120 days. Click the Next button.
5. The Terminal Server Setup page for security settings will appear. You can select Full Security or Relaxed Security. Select the Relaxed Security option and click the Next button to continue.
6. The appropriate files will be copied from the Windows Server 2003 distribution CD. The Completing The Windows Components Wizard page will appear. Click the Finish button.
7. The System Settings Change page will appear. This prompts you to reboot the computer. Click Yes.

Exercise 8.2: Configuring a Terminal Services Server

In this exercise, you will use the Terminal Services Configuration utility to configure the Terminal Services server you installed in Exercise 8.1.

1. Select Start ➢ Administrative Tools ➢ Terminal Services Configuration.
2. In the Terminal Services Configuration window, expand the `Connections` folder and then right-click the RDP-Tcp connection and select Properties.
3. In the General tab of the RDP-Tcp Properties dialog box, select High from the Encryption Level drop-down list.
4. Click the Sessions tab. Check the first Override User Settings checkbox and specify 15 minutes for the Idle Session Limit option.
5. Click the Remote Control tab. Click the Use Remote Control With The Following Settings radio button and select the Interact With The Session radio button.
6. Click the OK button to close the RDP-Tcp Properties dialog box.
7. Close all of the windows and return to the lab selection screen.

Optimizing Windows Server 2003

In this section, you will optimize the server by examining counters in System Monitor, configuring multiple processors, and using Performance Logs and Alerts and the Task Manager.

This section corresponds to Chapter 9, "Optimizing Windows Server 2003," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 9.1: Monitoring System Memory
- Exercise 9.2: Monitoring the System Processor
- Exercise 9.3: Monitoring the Disk Subsystem
- Exercise 9.4: Monitoring the Network Subsystem
- Exercise 9.5: Creating a Baseline Report
- Exercise 9.6: Managing Computer Processes

Exercise 9.1: Monitoring System Memory

In this exercise, you will monitor your computer's memory subsystem.

1. Select Start ➢ Administrative Tools ➢ Performance. System Monitor will open by default.
2. In the System Monitor window, click the Add button on the toolbar, which appears as a plus sign (+).
3. In the Add Counters dialog box, select the following performance objects and counters:
   - Select Memory from the Performance Object drop-down list, select Available MBytes in the counter list box, and click the Add button.
   - Select Paging File from the Performance Object drop-down list, select %Usage in the counter list box, and click the Add button.
4. Click the Close button. You should see a graph showing how your computer's memory is being used.
5. Note the Paging > %Usage counter. If this counter is below 99 percent, you are not using excessive paging.
6. Note the Memory > Available MBytes counter. If this counter is above 4MB, you should have sufficient RAM.
7. Close the window and return to the lab selection screen.

Exercise 9.2: Monitoring the System Processor

In this exercise, you will monitor your computer's processor.

1. In the System Monitor window, click the Add button on the toolbar.
2. In the Add Counters dialog box, select the following performance objects and counter:
   - If it's not already selected, select Processor from the Performance Object drop-down list, select Interrupts/Sec in the counter list box, and click the Add button.
3. Click the Close button. You should see these counters added to your graph.
4. Note the Processor > %Processor Time counter (which was added by default). If this counter's average is below 85 percent, you do not have a processor bottleneck.
5. Note the Processor > Interrupts/Sec counter. If this counter is below 1000 on a Pentium computer, you do not have any processes or hardware that are generating excessive interrupts.
6. Close the window and return to the lab selection screen.

Exercise 9.3: Monitoring the Disk Subsystem

In this exercise, you will monitor your disk subsystem.

1. In the System Monitor window, click the Add button on the toolbar.
2. In the Add Counters dialog box, select the following performance objects and counters:
   - Select PhysicalDisk from the Performance Object drop-down list, select %Disk Time from the counter list box, and click the Add button.
   - Select PhysicalDisk from the Performance Object drop-down list, select Current Disk Queue Length from the counter list box, and click the Add button.
   - Select LogicalDisk from the Performance Object drop-down list, select %Idle Time from the counter list box, and click the Add button.
3. Click the Close button. You will see these counters added to your graph.
4. Close the window and return to the lab selection screen.

Exercise 9.4: Monitoring the Network Subsystem

In this exercise, you will monitor your network subsystem.

1. In the System Monitor window, click the Add button on the toolbar.

2. In the Add Counters dialog box, select the following performance objects and counters:
   - Select Network Interface from the Performance Object drop-down list, select Bytes Total/Sec in the counter list box, and click the Add button.
   - Select TCPv4 from the Performance Object drop-down list, select Segments/Sec from the counter list box, and click the Add button.
3. Click the Close button. You should see these counters added to your graph.
4. Note the Network Interface > Bytes Total/Sec and TCPv4 > Segments/Sec counters. These numbers are cumulative. Use them in your baselines to determine network activity.
5. Close the window and return to the lab selection screen.

Exercise 9.5: Creating a Baseline Report

In this exercise, you will create a baseline report for your computer.

1. Expand Performance Logs And Alerts.
2. Right-click Counter Logs and select New Log Settings.
3. In the New Log Settings dialog box, type **Counter*mmddyy*** (replace *mmddyy* with the current month, date, and year) as the log name. The log file will be stored in the C:\PerfLogs folder by default. Click the OK button.
4. In the General tab of the counter log's Properties dialog box, click the Add button and add the following counters:
   - Memory > Available Mbytes
   - Memory > Pages/Sec
   - Paging File > %Usage
   - Processor > %Processor Time
   - Processor > Interrupts/Sec
   - PhysicalDisk > %Disk Time
   - PhysicalDisk > Current Disk Queue Length
   - Network Interface > Bytes Total/Sec
   - TCPv4 > Segments/Sec
5. Set the interval for sampling data to 5 seconds.
6. Click the Log Files tab. Uncheck the End File Names With checkbox. This will prevent the filename from being appended with *mmddhh* (month/day/hour). Click the OK button to close the Properties dialog box and start the log file.

7. To view your log file, open System Monitor. Click the Properties button on the toolbar. Click the Log Files radio button shown to the left, then click Add.

8. In the open file dialog box, select C:\PerfLogs\Countermmddyy and click the Open button.
9. Add the counters from the log file you created to see the data that was collected in your log.
10. Close the window and return to the lab selection screen.

Exercise 9.6: Managing Computer Processes

In this exercise, you will manage your computer's processes.

1. Right-click an empty space on your Taskbar and select Task Manager from the pop-up menu.
2. In the Applications tab, click the New Task button.
3. In the Create A New Task dialog box, type **Calc** and click the OK button.
4. Click the Processes tab. Right-click `calc.exe` and select Set Priority, then Low. In the Task Manager Warning dialog box, click the Yes button to continue.
5. Right-click `calc.exe` and select End Process. In the Task Manager Warning dialog box, click the Yes button.
6. Close all of the open windows and return to the lab selection screen.

Performing System Recovery Functions

In this section, you will use the Backup utility to back up and restore the system. In addition, you will examine system events in the Event Viewer and use Remote Desktop, which is primarily used as a remote diagnosis tool.

This section corresponds to Chapter 10, "Performing System Recovery Functions," in the *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 10.1: Using the Event Viewer Utility
- Exercise 10.2: Using Startup and Recovery Options
- Exercise 10.3: Using the Backup Wizard
- Exercise 10.4: Backing Up System State Data
- Exercise 10.5: Using the Restore Wizard
- Exercise 10.6: Using Remote Desktop Connection

Exercise 10.1: Using the Event Viewer Utility

In this exercise, you will view events in Event Viewer and set log properties.

1. Select Start ➢ Administrative Tools ➢ Event Viewer.
2. Click System in the left pane of the Event Viewer window to display the System log events.
3. Double-click the first event in the right pane of the Event Viewer window to see its Event Properties dialog box. Click the OK button to close the dialog box.
4. Right-click System in the left pane of the Event Viewer window and select Properties.
5. Click the Filter tab. Clear all the check marks under Event Types except those in the Warning and Error checkboxes, then click the OK button. You should see only Warning and Error events listed in the System log.
6. To remove the filter, return to the Filter tab of the log's Properties dialog box, click the Restore Defaults button at the bottom of the dialog box, and click the OK button. You will see all of the event types listed again.
7. Right-click System and select Clear All Events.
8. You see a dialog box asking if you want to save the System log before clearing it. Click the Yes button. Specify the path and filename for the log file, then click the Save button. All the events should be cleared from the System log.
9. Close the window and return to the lab selection screen.

Exercise 10.2: Using Startup and Recovery Options

In this exercise, you will access the Startup and Recovery options and make changes to the settings.

1. Select Start, right-click My Computer, and choose Properties. Click the Advanced tab and then click the Startup And Recovery Settings button.
2. Change the Time To Display List Of Operating Systems option from 30 seconds to 10 seconds.
3. In the Write Debugging Information section, choose (None) from the drop-down list.
4. Click the OK button to close the Startup And Recovery dialog box, and click OK to close the System Properties dialog box.
5. Close the window and return to the lab selection screen.

Exercise 10.3: Using the Backup Wizard

In this exercise, you will use the Backup Wizard.

If this were not a simulated environment, you would need a blank, formatted, high-density floppy disk for this exercise.

1. Create a folder on your D: drive called **DATA**. Create some small text files in this folder. The size of all of the files combined should not exceed 1MB. (See Exercise 5.1 for more information on creating files and folders.)
2. Select Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Backup.
3. The Welcome To The Backup Utility Advanced Mode dialog box appears. The Welcome To The Backup Or Restore Wizard page appears. Click the Next button.
4. The Backup Or Restore page appears. Ensure that the Back Up Files And Settings option is selected and click the Next button.
5. The What To Back Up page appears. Select Let Me Choose What To Back Up and click the Next button.
6. In the Items To Back Up dialog box, select My Computer, expand D:, and check the DATA folder. Click the Next button.
7. In the Backup Type, Destination, And Name page, select Let Me Choose A Location Not Listed Here from the Choose A Place To Save Your Backup pull-down menu and click the Browse button. In the Open dialog box, select E:. Enter any descriptive filename. Then click the Open button.
8. The Completing The Backup Or Restore Wizard page appears. If all of the information is correct, click the Finish button.
9. When the Backup Wizard completes, click the Report button in the Backup Progress dialog box. This will show the backup log in a Notepad window. Close this window when you are finished viewing the report.
10. Close all of the Backup Wizard dialog boxes.
11. Close the window and return to the lab selection screen.

Exercise 10.4: Backing Up System State Data

In this exercise, you will back up your System State data.

You would need a backup device attached to your computer to complete this exercise. The information will not fit on a single floppy disk.

1. Select Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Backup.
2. The Welcome To The Backup Utility Advanced Mode dialog box will appear; click Advanced mode for Backup Wizard. The Welcome To The Backup Wizard dialog box will appear. Click the Next button to continue.
3. On the What To Back Up page, select the Only Back Up the System State Data option and click the Next button.
4. In the Backup Type, Destination, And Name dialog box, select the location of your backup media (for example, `D:\Backup`) and click the Next button.
5. The Completing The Backup Wizard dialog box will appear. If all of the information is correct, click the Finish button.
6. When the backup is complete, click the Report button in the Backup Progress dialog box.
7. The backup log appears in a Notepad window. Close this window when you are finished viewing the report.
8. Close all of the Backup dialog boxes.
9. Close the window and return to the lab selection screen.

Exercise 10.5: Using the Restore Wizard

In this exercise, you will use the Restore Wizard.

You will need to have completed Exercise 10.4 to do this exercise.

1. Select Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Backup.
2. The Welcome To The Backup Utility Advanced Mode dialog box appears. The Welcome To The Backup Or Restore Wizard page appears. Click the Next button.
3. The Backup Or Restore page appears. Select the Restore Files And Settings option and click the Next button.
4. The What To Restore page appears. Select the session you created in Exercise 10.4, and specify the files you want to restore. Click the Next button.
5. The Completing The Backup Or Restore Wizard page appears. If all of the information is correct, click the Finish button.

6. During the restore process, the Wizard displays the Restore Progress dialog box. Once the restore process is complete, you can click the Report button to verify that all files were successfully restored.
7. Close the window and return to the lab selection screen.

Exercise 10.6: Using Remote Desktop Connection

In this exercise, you will remotely access your Windows Server 2003 domain controller from your Windows XP Professional computer.

1. From your Windows Server 2003 domain controller, select Start ➢ Control Panel ➢ System and click the Remote tab.
2. Within the Remote tab of System Properties, check Allow Users To Connect Remotely To This Computer.
3. From your Windows XP Professional computer, log on to the domain as Administrator.
4. Select Start ➢ All Programs ➢ Accessories ➢ Communications ➢ Remote Desktop Connection and click the Options button.
5. In the General tab, type in the name of your Windows Server 2003 domain controller in the Computer field. Use the Administrator username and configure your password and domain in the Password and Domain fields.
6. Click the Experience tab. Select Desktop Background, Themes, and Bitmap Caching from the Allow The Following list.
7. Click the Connect button at the bottom of the Remote Desktop Connection dialog box.
8. Close the window and return to the lab selection screen.

Module

2

Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance

The Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure exam requires that you know how to perform many hands-on tasks using Windows Server 2003. While most study guides provide you with the steps you need to know in order to perform many of these tasks, most students studying for the exam do not have access to a fully configured Windows Server 2003 network, and they cannot perform the exercises.

The Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance module allows you to perform hands-on tasks in a simulated Windows environment. You can perform complicated exercises without the expense of a fully equipped network. If you get stuck, the simulator will show you how to perform the operation, just as if a live instructor were at your side pointing out what to do!

Most of the labs cover material that is explained in detail in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*, by James Chellis, Paul Robichaux, and Matt Sheltz. We recommend that you have a copy of the Study Guide close at hand while performing these labs.

Since Chapter 1 of the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide* is mostly theory, there are no labs associated with it.

Installing and Configuring TCP/IP

In this section, we will examine some of the more advanced TCP/IP monitoring techniques that are available in Windows Server 2003. Specifically, we will use Network Monitor to view detailed information about TCP/IP traffic on the machine, and we will monitor the network subsystem in System Monitor.

This section corresponds to Chapter 2, "Installing and Configuring TCP/IP," in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 2.1: Installing the Network Monitor Driver and Application
- Exercise 2.2: Capturing Data with Network Monitor
- Exercise 2.3: Creating a Display Filter
- Exercise 2.4: Monitoring the Network Subsystem

Exercise 2.1: Installing the Network Monitor Driver and Application

To install the network monitor driver, follow these steps:

1. Open the Network Connections folder by clicking Start ➢ Connect To ➢ Show All Connections.
2. Right-click Local Area Connection and select Properties.
3. When the Properties dialog box appears, click the Install button. The Select Network Component Type dialog box appears. Click Protocol in the Component list and click the Add button.
4. The Select Network Protocol dialog box appears. Select Network Monitor Driver and click the OK button.
5. Once the driver is installed, the Properties dialog box reappears. Click OK on the Local Area Connection Properties dialog box. Click the Close button.

To install the network monitor application, follow these steps:

6. Select Start ➢ Control Panel ➢ Add Or Remove Programs.
7. When the Add Or Remove Programs dialog box appears, click the Add/Remove Windows Components button, which opens the Windows Components Wizard.
8. Select the Management And Monitoring Tools item and then click the Details button.
9. Check the box next to the Network Monitor Tools item and then click OK, which returns you to the Windows Components Wizard.
10. Click Next in the Windows Components Wizard.
11. After the necessary files are copied, click Finish to close the wizard.
12. Click the Close button to close the Add Or Remove Programs dialog box.

Exercise 2.2: Capturing Data with Network Monitor

In this lab, you will capture some data with the network monitor that you installed in the previous lab.

1. Install Network Monitor as described in Exercise 2.1. Open the Network Monitor application by selecting Start ➢ Administrative Tools ➢ Network Monitor. You will be prompted to select an interface to monitor. Select the Local Area Connection to continue with this exercise.

You will be asked to select an interface to monitor only after the first time you install Network Monitor.

2. Use the Capture ➢ Buffer Settings command to increase the capture buffer size to 2MB. This gives you room for 4096 frames of data. Click OK.
3. Start a capture with the Capture ➢ Start command. The simulator will automatically generate some network traffic for the network monitor to capture.
4. Let the capture run until the buffer is full; you can tell by watching the "# Frames in Buffer" line in the Captured Statistics section of the Total Stats pane. Then click the Stop button to stop the capture.
5. Save the capture buffer to disk with the File ➢ Save As command. You'll need it for the next exercise.
6. Leave the window open for the next lab.

Exercise 2.3: Creating a Display Filter

In this lab, you will filter the data that you captured in the previous lab.

1. In the Network Monitor, Select Capture ➢ Display Captured Data to open the Frame Viewer window. The capture information should be intact from the previous exercise.
2. When the Frame Viewer window appears, use the Display ➢ Filter command to open the Display Filter dialog box.
3. Select the Protocol == Any line and click the Edit Expression button. You'll see the Protocol tab of the Expression dialog box.
4. Click the Disable All button to remove all the protocols. The filter screens out any protocol that's disabled.
5. Select HTTP in the Disabled Protocols list and click the Enable button. Now HTTP should be the only enabled protocol. Click the OK button.
6. Click the OK button in the Display Filter dialog when you're done. The Frame Viewer window reappears, but notice that the frame numbers (in the leftmost column) are no longer consecutive—the filter is screening out any traffic that doesn't match its criteria.
7. Double-click a frame to see its contents. Because you're looking at unencrypted HTTP packets, you can clearly see the requests and responses. Close all of the open windows, including the desktop, and proceed to the next lab.

Exercise 2.4: Monitoring the Network Subsystem

In this lab, you will monitor the network subsystem with the System Monitor.

1. Open the System Monitor by selecting Start ➢ Administrative Tools ➢ Performance.
2. In the System Monitor window, click the Add button on the toolbar.

3. In the Add Counters dialog box, select the following performance objects and counters:
   - Select Network Interface from the Performance Object drop-down list, select Bytes Total/Sec from the counter list box, and click the Add button.
   - Select TCPv4 from the Performance Object drop-down list, select Segments/Sec from the counter list box, and click the Add button.
4. Click the Close button. You should see these counters added to your chart.
5. To generate some activity, copy some files between your domain controller and the member server.
6. Note the Network Interface > Bytes Total/Sec and TCPv4 > Segments/Sec counters. These numbers are cumulative. Use them in your baselines to determine network activity.

Administering Security Policy

In this section, you will administer a domain controller's security policy using the Group Policy options included in Windows Server 2003. In addition, you will use the Security Configuration And Analysis tool to compare the machine's security settings to those in a template, and you will update the computer's security using Windows Update.

This section corresponds to Chapter 3, "Administering Security Policy," in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 3.1: Creating a Management Console for Security Settings
- Exercise 3.2: Setting Password Policies
- Exercise 3.3: Setting Account Lockout Policies
- Exercise 3.4: Setting Audit Policies
- Exercise 3.5: Setting Local User Rights
- Exercise 3.6: Defining Security Options
- Exercise 3.7: Using the Security Configuration And Analysis Tool
- Exercise 3.8: Using Windows Update
- Exercise 3.9: Configuring Automatic Updates

Exercise 3.1: Creating a Management Console for Security Settings

In this lab, you will create and save an MMC console session that includes the GPO editor.

1. Select Start ➢ Run, type **MMC** in the Run dialog box, and click the OK button to open the MMC.
2. From the main menu, select File ➢ Add/Remove Snap-In.
3. In the Add/Remove Snap-In dialog box, click the Add button.
4. Select the Group Policy Object Editor option and click the Add button.
5. The Group Policy Object specifies Local Computer by default. Click the Finish button.
6. Select the Event Viewer option and click the Add button.
7. The Select Computer dialog box appears with Local Computer selected by default. Click the Finish button. Then click the Close button.
8. In the Add/Remove Snap-In dialog box, click the OK button.
9. Select File ➢ Save As. Save the console as **Security** in the C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools folder and click the Save button.

You can now access this console by selecting Start ➢ Administrative Tools ➢ Security. For now, close all of the open windows and return to the lab selection screen.

Exercise 3.2: Setting Password Policies

In this lab, you will configure password policies in the GPO editor.

1. In the Local Computer Policy snap-in, expand the folders as follows: Computer Configuration, Windows Settings, Security Settings, Account Policies, Password Policy.
2. Open the Enforce Password History policy. In the Effective Policy Setting field, specify five passwords remembered. Click the OK button.
3. Open the Maximum Password Age policy. In the Local Policy Setting field, specify that the password expires in 60 days. Click the OK button.
4. Select Start ➢ Command Prompt. At the command prompt, type **`gpupdate`** and press Enter.
5. At the command prompt, type **`exit`** and press Enter.
6. Exit the lab when prompted.

Exercise 3.3: Setting Account Lockout Policies

In this lab, you will configure account lockout policies in the GPO editor.

1. In the Local Computer Policy snap-in, expand the folders as follows: Computer Configuration, Windows Settings, Security Settings, Account Policies, Account Lockout Policy.

2. Open the Account Lockout Threshold policy. In the Local Policy Setting field, specify that the account will lock after three invalid logon attempts. Click the OK button.
3. The Suggested Value Changes dialog box appears. Accept the default values for Account Lockout Duration and Reset Account Lockout Counter by clicking the OK button.
4. Exit the lab when prompted.

Exercise 3.4: Setting Audit Policies

In this lab, you will set audit policies in the GPO editor.

1. Select Start ➢ Administrative Tools ➢ Security and expand the Local Computer Policy snap-in.
2. Expand the folders as follows: Computer Configuration, Windows Settings, Security Settings, Local Policies, Audit Policy.
3. Open the Audit Account Logon Events policy. In the Local Policy Setting field, under Audit These Attempts, check the boxes for Success and Failure. Click the OK button.
4. Open the Audit Account Management policy. In the Local Policy Setting field, under Audit These Attempts, check the boxes for Success and Failure. Click the OK button.
5. The simulator will automatically generate three failed logon attempts. Open the MMC and expand the Event Viewer snap-in.
6. From Event Viewer, open the security log. You should see the audited events listed in this log.
7. Exit the lab when prompted.

Exercise 3.5: Setting Local User Rights

In this lab, you will set local user rights in the GPO editor.

1. Select Start ➢ Administrative Tools ➢ Security and expand the Local Computer Policy snap-in.
2. Expand folders as follows: Computer Configuration, Windows Settings, Security Settings, Local Policies, User Rights Assignment.
3. Open the Log On As A Service user right. The Local Security Policy Setting dialog box appears.
4. Click the Add User Or Group button. The Groups dialog box appears.
5. Enter any valid username. Click the OK button. Then click the OK button again on the Log On As A Service Properties dialog box.
6. Close all of the open windows and return to the lab selection screen.

Exercise 3.6: Defining Security Options

In this lab, you will configure security options in the GPO editor.

1. In the Local Computer Policy snap-in, expand folders as follows: Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options.
2. Open the policy Interactive Logon: Message Text For Users Attempting To Log On. In the Local Policy Setting field, type **Welcome to all authorized users**. Click the OK button.
3. Open the policy Interactive Logon: Prompt User To Change Password Before Expiration. In the Local Policy Setting field, specify 3 days. Click the OK button.
4. Select Start ➢ Command Prompt. At the command prompt, type **`gpupdate`** and press Enter.
5. At the command prompt, type **`exit`** and press Enter.
6. Exit the lab when prompted.

Exercise 3.7: Using the Security Configuration And Analysis Tool

To add the Security Configuration And Analysis snap-in, follow these steps:

1. Select Start ➢ Administrative Tools ➢ Security.
2. Select File ➢ Add/Remove Snap-In.
3. In the Add/Remove Snap-In dialog box, click the Add button. Highlight the Security Configuration And Analysis snap-in and click the Add button. Then click the Close button.
4. In the Add/Remove Snap-In dialog box, click the OK button.

To specify the security database, follow these steps:

5. Right-click Security Configuration And Analysis and select Open Database.
6. In the Open Database dialog box, type **`sampledb`** in the File Name text box. Then click the Open button.
7. In the Import Template dialog box, select the template `securews` and click the Open button.

To create the security template, follow these steps:

8. In the MMC, select File ➢ Add/Remove Snap-In.
9. In the Add/Remove Snap-In dialog box, click the Add button. Highlight the Security Templates snap-in and click the Add button. Then click the Close button.
10. In the Add/Remove Snap-In dialog box, click the OK button.
11. Expand the Security Templates snap-in and then expand the C:\Windows\Security\Templates folder.

12. Double-click the `securews` file.
13. Select Account Policies and then double-click Password Policy.
14. Edit the password policies as follows:
    - Set the Enforce Password History option to 10 passwords remembered.
    - Enable the Passwords Must Meet Complexity Requirements option.
    - Set the Maximum Password Age option to 30 days.
15. Highlight the `securews` filename, right-click, and select the Save As option.
16. In the Save As dialog box, place the file in the default folder and name the file **servertest**. Click the Save button.

To import the security template, follow these steps:

17. Highlight the Security Configuration And Analysis snap-in, right-click, and select the Import Template option.
18. In the Import Template dialog box, highlight the `servertest` filename and click the Open button.

To perform and review the security analysis, follow these steps:

19. Highlight the Security Configuration And Analysis snap-in, right-click, and select the Analyze Computer Now option.
20. In the Perform Analysis dialog box, accept the default error log file path and click the OK button.
21. When you return to the main MMC window, double-click the Security Configuration And Analysis snap-in.
22. Double-click Account Policies and then double-click Password Policy. You will see the results of the analysis for each policy, indicated by an *x* or a check mark next to the policy. Close the window and return to the desktop. Leave the desktop open for the next lab.

Exercise 3.8: Using Windows Update

In this lab, you will use Windows Update to find and install service packs and hot fixes on your computer.

1. Select Start ➢ Help And Support.
2. The Help And Support Center dialog box appears.
3. Under Support Tasks, click the Windows Update option.
4. The Welcome To Windows Update screen appears. Click Scan For Updates.
5. Windows Update will look for all available updates based on your computer's configuration.

6. All updates for your computer will be listed. Click on each option for Critical Updates And Service Packs, Windows Server 2003 Family, and Driver Updates and check the updates you want to install.
7. Click Review And Install Updates. In the Total Selected Updates section, click the Install Now button.

Exercise 3.9: Configuring Automatic Updates

In this lab, you will configure automatic updates.

1. Select Start ➢ Control Panel ➢ System and click the Automatic Updates tab.
2. Verify that the Keep My Computer Up To Date option is checked.
3. Under Settings, select the Automatically Download The Updates, And Install Them On The Schedule That I Specify option. Select Every Sunday At 2:00 a.m. and click the OK button.

Managing IP Security

In this section, you will manage the IP Security (also known as IPSec) extensions to secure data transmission on the network.

This section corresponds to Chapter 4, "Managing IP Security," in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 4.1: Enabling IPSec on the Local Computer
- Exercise 4.2: Enabling IPSec for an Entire Domain
- Exercise 4.3: Customizing and Configuring the Local Computer IPSec Policy and Rules for Transport Mode
- Exercise 4.4: Configuring a Policy for IPSec Tunnel Mode
- Exercise 4.5: Adding the IP Security Monitor to the MMC
- Exercise 4.6: Configuring IPSec Logon Activity Monitoring

Exercise 4.1: Enabling IPSec on the Local Computer

In this lab, you will enable IPSec on the local computer by assigning a policy.

1. Click Start ➢ Run, type **MMC**, and click OK. An empty MMC console window appears.
2. Select File ➢ Add/Remove Snap-In. When the Add/Remove Snap-In dialog box appears, click the Add button.
3. In the Add Standalone Snap-In dialog box, select IP Security Policy Management and click the Add button.
4. The Select Computer Or Domain dialog box appears. Select the Local Computer (default setting) radio button and then click the Finish button.
5. Click the Close button in the Add Standalone Snap-In dialog box.
6. Click the OK button in the Add/Remove Snap-In dialog box.
7. Select the IP Security Policies On Local Computer node in the MMC.
8. Right-click the Server (Request Security) policy and choose Assign.
9. Verify that the entry in the Policy Assigned column for the selected policy has changed to Yes. Close the MMC window and return to the desktop. Leave the desktop open for the next lab.

Exercise 4.2: Enabling IPSec for an Entire Domain

In this lab, you will enable ipsec for an entire domain, rather than just for the local computer.

1. Click Start ➢ Run, type **MMC**, and click OK. An empty MMC console window appears.
2. Select File ➢ Add/Remove Snap-In. When the Add/Remove Snap-In dialog box appears, click the Add button.
3. In the Add Standalone Snap-In dialog box, select Group Policy Object Editor and click the Add button.
4. The Select Group Policy Object dialog box appears. Click the Browse button to bring up the Browse For A Group Policy Object dialog box.
5. Select Default Domain Policy and click the OK button.
6. Click the Finish button in the Select Group Policy Object dialog box.
7. Click the Close button in the Add Standalone Snap-In dialog box and then click the OK button in the Add/Remove Snap-In dialog box.
8. Expand Default Domain Policy ➢ Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ IP Security Policies on Default Domain Name.
9. The right side of the MMC window lists the available policies, including the three predefined policies.
10. Right-click the Server (Request Security) policy and select the Assign command. Notice that the Policy Assigned column for that policy now reads Yes. Leave the window open for the next lab.

Exercise 4.3: Customizing and Configuring the Local Computer IPSec Policy and Rules for Transport Mode

In this lab, you will customize one of the IPSec policies on the server.

1. Make sure that the MMC window is still open from the previous lab.
2. Select the File ➢ Add/Remove Snap-In command. When the Add/Remove Snap-In dialog box appears, click the Add button.
3. In the Add Standalone Snap-In dialog box, scroll through the snap-in list until you see the one marked IP Security Policy Management. Select it and click the Add button.
4. The Select Computer dialog box appears. Select the Local Computer radio button and then click the Finish button.
5. Click the Close button in the Add Standalone Snap-In dialog box, and then click the OK button in the Add/Remove Snap-In dialog box.
6. Select the IP Security Policies On Local Computer node in the MMC. In the right-hand pane of the MMC, right-click the Server (Request Security) policy and choose Properties. The Server (Request Security) Properties dialog box appears.
7. The All IP Traffic rule is selected by default. Click the Edit button. The Edit Rule Properties dialog box appears.
8. Switch to the Filter Action tab. Select the Request Security (Optional) filter action and then click the Edit button. The filter action's Properties dialog box appears.
9. Click the Add button. When the New Security Method dialog box appears, click the Custom radio button and then click the Settings button.
10. In the Custom Security Method Settings dialog box, check the Data And Address Integrity Without Encryption (AH) checkbox, and in the drop-down list, select SHA1. Check the Data Integrity and Encryption (ESP) checkbox. Using the drop-down lists under (ESP), set Integrity to SHA1 and Encryption to 3DES.
11. First check the Generate A New Key Every checkbox and set the key generation interval to 24,000 Kbytes. (Kbytes must be in the range 20,480–2,147,483,647Kb.) Then click the next Generate A New Key Every checkbox and specify a key generation interval of 1800 seconds.
12. Click the OK button in the Custom Security Method Settings dialog box and then click OK in the New Security Method dialog box.
13. When the Request Security (Optional) Properties dialog box appears, use the Move Up button to move the custom filter you just defined to the top of the list.
14. Click the OK button in the Request Security (Optional) Properties dialog box.
15. Click the Close button in the Edit Rule Properties dialog box and then click the OK button in the Server (Request Security) Properties dialog box. Leave the window open for the next lab.

Exercise 4.4: Configuring a Policy for IPSec Tunnel Mode

In this lab, you will configure a policy for IPSec tunnel mode.

If this were not a simulated environment, this lab would require you to use two separate machines to which you have administrator access. Let's call them machine A and machine B. Before you start, you would need their IP addresses, and you would need to have their local IPSec policies open in an MMC console.

1. In the MMC console that should still be open from the previous lab, right-click the IP Security Policies On Local Computer node, then choose the Create IP Security Policy command. The IP Security Policy Wizard appears. Click Next.
2. Name your policy **Tunnel To B** and then click the Next button.
3. On the Requests For Secure Communication page, turn off the Activate Default Response Rule checkbox and click the Next button.
4. When the summary page for the wizard appears, make sure the Edit Properties checkbox is on and then click Finish. The Tunnel To B Properties dialog box appears. Click the Add button on the Rules tab. The Welcome To The Create IP Security Rule Wizard begins. Click Next.
5. In the Tunnel Endpoint page of the wizard, select The Tunnel Endpoint Is Specified By The Following IP Address and enter the IP address of machine B. Click Next.
6. In the Network Type page, select Local Area Network (LAN). Click Next.
7. Select the All IP Traffic radio button. Click Next.
8. Select the Request Security (Optional) radio button on the Filter Action page. Click Next.
9. In the Authentication Method page, select Active Directory Default (Kerberos V5 protocol). Click Next.
10. Clear the Edit Properties checkbox, click Finish, then click OK. Leave the window open for the next lab.

Exercise 4.5: Adding the IP Security Monitor to the MMC

In this lab, you will add the IP Security Monitor snap-in to the MMC.

1. Make sure that the MMC is still open from the previous lab.
2. Select Add/Remove Snap-In on the File menu and click the Add button.

3. Select IP Security Monitor in the list of snap-ins and click the Add button. Click Close and then click OK. You should return to the MMC, and the snap-in should appear in the left pane.
4. To save the MMC, select File ➢ Save and specify a name and a location in which to save the console. Leave the window open for the next lab.

Exercise 4.6: Configuring IPSec Logon Activity Monitoring

In this lab, you will configure IPSec logon activity monitoring so that IPSec logon activity appears in the event log.

1. The MMC should still be open from the previous labs. First, locate the GPO that you created in Exercise 4.2.
2. Find and select the Audit Policy folder by following this path: Local Computer Policy, Computer Configuration, Windows Settings, Security Settings, Local Policies, Audit Policy.
3. Double-click the Audit Logon Events entry. When the Local Security Policy Setting dialog box appears, check the Success and Failure checkboxes and then click the OK button.
4. Double-click the Audit Object Access entry. When the Local Security Policy Setting dialog box appears, check the Success and Failure checkboxes and then click the OK button. Close the window and return to the virtual desktop.

Managing the Dynamic Host Configuration Protocol (DHCP)

In this section, you will manage DHCP settings using the DHCP utility.

This section corresponds to Chapter 5, "Managing the Dynamic Host Configuration Protocol (DHCP)," in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 5.1: Installing the DHCP Service
- Exercise 5.2: Authorizing a DHCP Server
- Exercise 5.3: Creating a New Scope
- Exercise 5.4: Configuring User Class Options
- Exercise 5.5: Creating a New Multicast Scope
- Exercise 5.6: Enabling DHCP-DNS Integration
- Exercise 5.7: Inspecting Leases

Exercise 5.1: Installing the DHCP Service

In this lab, you will install DHCP with the Add or Remove Programs utility.

1. Select Start ➢ Control Panel ➢ Add or Remove Programs.
2. Click the Add/Remove Windows Components icon. The Windows Components Wizard opens and lists all of the available components.
3. Select the Networking Services item from the component list and click the Details button.
4. When the Subcomponents Of Network Services list appears, make sure Dynamic Host Configuration Protocol (DHCP) is selected and click the OK button.
5. Click the Next button to continue the Windows Components Wizard.
6. If prompted, enter the path to the Windows Server 2003 distribution files.
7. Click Finish to close the Windows Components Wizard. Close the Add or Remove Programs window.

Exercise 5.2: Authorizing a DHCP Server

In this lab, you will authorize a DHCP server in Active Directory.

1. Select Start ➢ Administrative Tools ➢ DHCP to open the DHCP snap-in.
2. Right-click the server you want to authorize and choose the Authorize command.
3. Wait a short time (30–45 seconds) to allow the authorization to take place.
4. Right-click the server again. Verify that the Unauthorize command appears in the pop-up menu; this indicates that the server is now authorized.
5. Leave the window open for the next lab.

Exercise 5.3: Creating a New Scope

In this lab, you will create a new scope in the DHCP utility.

1. In the DHCP window, right-click the server on which you want to create the new scope and choose New Scope. The New Scope Wizard appears.
2. Click the Next button on the Welcome page.
3. Enter a name and a description for your new scope and click the Next button.
4. In the IP Address Range page, enter **190.168.0.2** as the start IP address for the scope and **192.168.0.250** as the end IP address. Leave the subnet mask controls alone (though when creating a scope on a production network you might need to change them). Click the Next button.

5. In the Add Exclusions page, click Next without adding any excluded addresses.
6. In the Lease Duration page, set the lease duration to 3 days and click the Next button.
7. In the Configure DHCP Options page, click the Next button to indicate that you want to configure default options for this scope.
8. Enter a router IP address (in this case, **192.168.0.1**) in the IP Address field and then click the Add button. Once the address is added, click the Next button.
9. In the Domain Name And DNS Servers page, enter the IP address of a DNS server on your network in the IP address field (in this case, **192.168.0.251**), and click the Add button. Click the Next button.
10. On the WINS Servers page, click the Next button to leave the WINS options unset and display the Activate Scope page.
11. Select the No, I Will Activate This Scope Later radio button. Click the Next button. When the Wizard Summary page appears, click the Finish button to create the scope.
12. Leave the window open for the next lab.

Exercise 5.4: Configuring User Class Options

Now, you will create a user class and configure options for it.

1. In the DHCP window, right-click the DHCP server and select Define User Classes.
2. Click the Add button in the DHCP User Classes dialog box.
3. In the New Class dialog box, enter a descriptive name for the class in the Display Name field. Enter a class ID in the ID field.

Typically, you will enter the class ID in the ASCII portion of the ID field. You should make sure that the computers you want to use in the class have been configured with the `ipconfig /setclassid` command as described earlier in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*.

4. When you are done, click the OK button.
5. The new class appears in the DHCP User Classes dialog box. Click the Close button to return to the DHCP administrative tool.
6. Right-click either the Server Options or a Scope Options node (depending on whether you want to set the class options at the server or scope level) and select Configure Options.
7. Click the Advanced tab. Select the class you defined in step 3 from the User Class pull-down menu.

8. Configure the options that you want to set for the class. Click OK when you are done. Notice that the options you configured (and the class that they are associated with) appear in the right pane of the DHCP window.
9. Leave the window open for the next lab.

Exercise 5.5: Creating a New Multicast Scope

In this lab, you will create a new multicast scope in the DHCP utility.

1. In the DHCP window, right-click your DHCP server and choose New Multicast Scope. The New Multicast Scope Wizard appears. Click the Next button on the Welcome page.
2. In the Multicast Scope Name page, name your multicast scope (and add a description if you like). Click the Next button.
3. The IP Address Range page appears. Enter a start IP address of **224.0.0.0** and an end IP address of **224.255.0.0**. Adjust the TTL to 1 to make sure that no multicast packets escape your local network segment. Click the Next button when you're done.
4. The Add Exclusions page appears; click its Next button.
5. The Lease Duration page appears. Normally you leave multicast scope assignments in place somewhat longer than you would with a regular unicast scope, hence the default lease length of 30 days. Click the Next button.
6. The wizard asks you if you want to activate the scope now. Click the No radio button and then the Next button.
7. The Wizard Summary page appears; click the Finish button to create your scope.
8. Verify that your new multicast scope appears in the DHCP snap-in.
9. Leave the window open for the next lab.

Exercise 5.6: Enabling DHCP-DNS Integration

In this lab, you will configure dynamic updates so that DHCP and DNS are integrated.

1. In the DHCP window, right-click the DHCP server you configured in Exercise 5.1 and select Properties.
2. The Server Properties dialog box appears. Click the DNS tab.
3. Verify that the Enable DNS Dynamic Updates According To The Settings Below checkbox is checked and verify that the Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients radio button is selected. If it is not, then check it.
4. Verify that the Discard A And PTR Records When Lease Is Deleted checkbox is checked. If it is not, then check it.

5. Click the OK button to apply your changes and close the Properties dialog box.
6. Leave the window open for the next lab.

Exercise 5.7: Inspecting Leases

In this lab, you will see where DHCP leases would normally be located.

1. In the DHCP window, expand the target server's node in the MMC until you see the Address Leases node.
2. Right-click the Address Leases node and click Export List on the pop-up menu.
3. When the Save As dialog box appears, select a location for the list file. Type a meaningful name in the Filename field and click the Save button.

Installing and Managing Domain Name Service (DNS)

In this section, you will manage DNS settings using the DNS utility.

This section corresponds to Chapter 6, "Installing and Managing Domain Name Service (DNS)," in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 6.1: Installing and Configuring the DNS Service
- Exercise 6.2: Configuring Zones and Configuring Zones for Dynamic Updates
- Exercise 6.3: Creating a Delegated DNS Zone
- Exercise 6.4: Manually Creating DNS RRs
- Exercise 6.5: Installing and Running Replication Monitor
- Exercise 6.6: Working with Replication Monitor

Exercise 6.1: Installing and Configuring the DNS Service

In this lab, you will install the DNS service using the Configure Your Server wizard. Then, you will configure the DNS zones.

1. Open the Configure Your Server Wizard by selecting Start ➢ Administrative Tools ➢ Configure Your Server.
2. Click Next to dismiss the Welcome screen and click Next again to dismiss the Preliminary Steps screen.
3. Click the DNS Server item in the Server Role list and click Next to continue.
4. Click Next on the Summary page to complete the DNS installation.

If this were not a simulated environment, you would need to insert the Windows Server 2003 CD into the CD-ROM drive.

5. The Configure A DNS Sever Wizard automatically appears. Click Next to dismiss the Welcome screen.
6. Select the Create Forward And Reverse Lookup Zones radio button and click Next to continue. If you want to create a caching-only server, you can select the Configure Root Hints Only option.
7. If it's not already selected, select Yes, Create A Forward Lookup Zone Now and click Next to continue.
8. If not already selected, select the Primary Zone option and the Store The Zone In Active Directory option. Click Next when you are ready.
9. Enter sybex.com in the Zone Name field and click Next to continue.
10. Select the Allow Only Secure Dynamic Updates radio button and click Next.
11. If not already selected, select No, Don't Create A Reverse Lookup Zone Now and click Next to continue.
12. If not already selected, select the No, It Should Not Forward Queries radio button and click Next to continue.
13. Click Finish to end the wizard. The Configure Your Server wizard reappears and informs you that the DNS service was successfully installed. Click the Finish button.

Exercise 6.2: Configuring Zones and Configuring Zones for Dynamic Updates

In this lab, you will configure the zones you created in the previous lab.

1. Open the DNS management snap-in by selecting Start ➢ Administrative Tools ➢ DNS.
2. Locate the Forward Lookup Zones folder.
3. Right-click sybex.com and choose the Properties command.
4. Switch to the WINS tab and click the Use WINS Forward Lookup checkbox.

5. Enter the IP address of a valid WINS server on your network, click Add, and then click OK. For purposes of this simulation, you can enter any IP address here.
6. Click the General tab.
7. Change the value of the Dynamic Updates control to Secure Only. Click OK to close the Properties dialog box. Notice that there's now a new WINS Lookup RR in your zone.
8. Leave the window open for the next lab.

Exercise 6.3: Creating a Delegated DNS Zone

In this lab, you will create a delegated DNS zone for another server.

1. In the DNS window, expand the DNS server and locate the sybex.com zone.
2. Right-click the zone and choose the New Delegation command.
3. The New Delegation Wizard appears. Click Next to dismiss the initial wizard page.
4. Enter **`ns1`** in the Delegated Domain field of the Delegated Domain Name page. Click Next to complete this step.

This is the name of the domain for which you want to delegate authority to another DNS server. It should be a subdomain of the primary domain (for example, to delegate authority for huntsville.chellis.net, you'd enter **`huntsville`** in the Delegated Domain field).

5. When the Name Servers page appears, use the Add button to add the name and IP address(es) of the servers that will be hosting the newly delegated zone. For the purpose of this exercise, enter the zone name you used in Exercise 6.1. Click the Resolve button to automatically resolve this domain name's IP address into the IP address field. Click Add to add the resolved address to the list. Click OK when you are done. Click Next to continue with the wizard.
6. Click the Finish button. The New Delegation wizard disappears and you'll notice the new zone you just created appear beneath the zone you selected in step 1. The newly delegated zone's folder icon is drawn in gray to indicate that control of the zone is delegated.
7. Leave the window open for the next lab.

Exercise 6.4: Manually Creating DNS RRs

In this lab, you will manually configure DNS resource records.

1. In the DNS window, expand your DNS server, right-click sybex.com, and use the New Mail Exchanger (MX) command.

2. Enter **mailtest** in the Host Or Child Domain field, and enter **mailtest.*yourDomain.com*** (where ***yourDomain*** is the domain name you used in Exercise 6.1) in the Fully Qualified Domain Name (FQDN) Of Mail Server field and then click OK. Notice that the new record is already visible.
3. Right-click the sybex.com zone and choose Other New Records. When the Resource Record Type dialog box appears, find Alias (CNAME) in the list and select it.
4. Click the Create Record button. The New Resource Record dialog box appears.
5. Type **mail** into the Alias Name field.
6. Type **mailtest.*yourDomain.com*** into the Fully Qualified Domain Name (FQDN) For Target Host field.
7. Click the OK button and then close the Resource Record Type dialog box.

Exercise 6.5: Installing and Running Replication Monitor

In this lab, you will install and run the Replication Monitor, which can be used to monitor DNS zone replication in an Active Directory environment.

1. In Windows Explorer, navigate to the \SUPPORT\TOOLS\ folder on the Windows Server 2003 CD.
2. Double-click the SUPTOOLS file that appears in the folder.
3. The Support Tools Installation Wizard guides you through the installation process. To ensure smooth operation of the support tools, be sure to install them to the default directory.
4. After the installation is complete, you can run the Replication Monitor by selecting Start ➢ Run and entering **REPLMON** in the Run dialog box.

Exercise 6.6: Working with Replication Monitor

In this lab, you will use the replication monitor to view and synch replication on the server.

1. Open Replication Monitor by selecting Start ➢ Run and entering **REPLMON** in the Run dialog box.
2. To add a server to the Replication Monitor window, right-click Monitored Servers and select Add Monitored Server from the pop-up menu.
3. The Add Monitored Server Wizard appears. Select Add The Server Explicitly By Name. Click Next when you are done.
4. Enter the name of the server to monitor (the server from Exercise 6.1) and click Finish.
5. To search for replication errors, click the Action menu and select Domain ➢ Search Domain Controllers For Replication Errors.

6. The Search Domain Controllers For Replication Failures window appears. Click the Run Search button and enter the name of the local domain. After a few moments, Replication Monitor should list any failures in the Search Domain Controllers For Replication Failures window. Click Close.
7. You can manually synchronize either the entire Active Directory or just individual pieces. In order to synchronize the domain DNS zones only, right click the DC=DomainDNSZones,DC=*domain*,DC=*suffix* item under the monitored server and select Synchronize This Directory Partition With All Servers from the pop-up menu.
8. Depending on how your domain is configured, you can choose the Disable Transitive Replication, Push Mode, or Cross Site Boundaries checkboxes. In this case, leave them blank and click OK.
9. You will be prompted to confirm the replication. Click Yes.
10. Click OK at the success notification. Close all of the open windows and return to the lab selection screen.

Managing Remote Access Services

In this section, you will manage remote access services, such as dial-up and VPN.

This section corresponds to Chapter 7, "Managing Remote Access Services," in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 7.1: Installing the Routing and Remote Access Services
- Exercise 7.2: Controlling Multilink for Incoming Calls
- Exercise 7.3: Configuring Incoming Connections
- Exercise 7.4: Installing the Routing and Remote Access Services as a VPN Server
- Exercise 7.5: Changing Remote Access Logging Settings
- Exercise 7.6: Installing and Configuring the DHCP Relay Agent on an RRAS Server
- Exercise 7.7: Configuring the DHCP Relay Agent on a Network Interface

Exercise 7.1: Installing the Routing and Remote Access Services

In this lab, you will enable routing and remote access on the server.

1. Open the RRAS MMC console by selecting Start ➢ Administrative Tools ➢ Routing And Remote Access.
2. Select the server in the left pane of the MMC. Right-click the server and choose Configure And Enable Routing And Remote Access. The RRAS Setup Wizard appears. Click the Next button.
3. On the Common Configuration page of the wizard, select the Remote Access (Dial-Up Or VPN) radio button and then click the Next button
4. The Remote Access page appears, allowing you to select a VPN server and/or a dial-up server. Check both checkboxes.
5. Choose any interface for the VPN. Click Next.
6. The IP Address Assignment page appears. To use DHCP (either a DHCP server on your network or the built-in address allocator), leave the Automatically radio button selected. Click the Next button.
7. The Managing Multiple Remote Access Servers page appears. You use this page to configure your RRAS server to work with other RADIUS-capable servers on your network. In this case, you don't want to use RADIUS, so leave the No, Use Routing And Remote Access To Authenticate Connection Requests button selected and then click the Next button.
8. The summary page appears. Click the Finish button to start the RRAS service and prepare your server to be configured.
9. Leave the window open for the next lab.

Exercise 7.2: Controlling Multilink for Incoming Calls

In this lab, you will disable and then re-enable multilink.

1. In the RRAS window, right-click the server in the left pane of the MMC and choose Properties. The server Properties dialog box appears.
2. Click the PPP tab.
3. Turn multilink capability off by making sure the Multilink Connections checkbox is unchecked. To turn it back on, simply check the checkbox.
4. If you decide to turn multilink capability on, you should also enable the use of BAP/BACP to make it easier for your server to adjust to the load placed on it. To do so, make sure the Dynamic Bandwidth Control Using BAP Or BACP checkbox is marked.
5. Click the OK button.
6. Close the RRAS window and return to the lab selection screen.

Exercise 7.3: Configuring Incoming Connections

In this lab, you will ensure that incoming connections are enabled.

1. In the RRAS window, right-click the server in the left pane of the MMC and choose Properties. The server Properties dialog box appears.
2. Click the IP tab. Verify that both the Enable IP Routing and the Allow IP-Based Remote Access And Demand-Dial Connections checkboxes are marked.
3. Click the OK button. After a brief pause, the Properties dialog box disappears and your changes become effective.

Exercise 7.4: Installing the Routing and Remote Access Services as a VPN Server

In this lab, you will enable RRAS as a VPN server.

1. Open the RRAS window. In the RRAS window, select the server in the left pane of the MMC. Right-click the server and choose Configure And Enable Routing And Remote Access. The RRAS Setup Wizard appears. Click the Next button.
2. In the Configuration page of the wizard, select the Remote Access (Dial-Up Or VPN) radio button, and then click the Next button.
3. On the Remote Access page, check the VPN checkbox. Click the Next button.
4. On the VPN Connections page, leave the default setting and click the Next button.
5. The IP Address Assignment page appears. If you want to use DHCP (either a DHCP server on your network or the built-in address allocator), leave the Automatically radio button selected. If you want to pick out an address range, select the From A Specified Range Of Addresses button. Click the Next button.

If you choose to use static addressing, at this point the wizard will give you the opportunity to define one or more address ranges to be assigned to remote clients.

6. On the Managing Multiple Remote Access Servers page, leave the No, Use Routing And Remote Access To Authenticate Connection Requests button selected and click the Next button.
7. On the summary page, click the Finish button to start the RRAS service and prepare your server to be configured.
8. Leave the window open for the next lab.

Exercise 7.5: Changing Remote Access Logging Settings

In this lab, you will change RRAS logging settings.

1. In the RRAS window, expand the server and select the Remote Access Logging node. The right-hand MMC pane lists the log files on that server.
2. Locate the log file named Local File and then open its Properties dialog box by right-clicking it and choosing Properties.
3. The Local File Properties dialog box appears. On the Settings tab, make sure the Accounting Requests and Authentication Requests checkboxes are marked.
4. Switch to the Log File tab. Select an appropriate time period for log rollover by choosing one of the radio buttons in the Create A New Log File control group.
5. Click the OK button.
6. Leave the window open for the next lab.

Exercise 7.6: Installing and Configuring the DHCP Relay Agent on an RRAS Server

In this lab, you will install and configure the DHCP relay agent, which is necessary if your DHCP server is not located on the local network.

1. In the RRAS window, expand the server, IP Routing, then General.
2. Right-click the General node and choose New Routing Protocol. The New Routing Protocol dialog box appears.
3. Select DHCP Relay Agent from the list of routing protocols and then click the OK button.
4. The IP Routing node will now have a child node named DHCP Relay Agent. Select it and choose Properties to open its Properties dialog box.
5. In the DHCP Relay Agent Properties dialog box, add the IP addresses of the DHCP servers you want DHCP requests forwarded to and then click the OK button. For purposes of this simulation, any IP address will do.
6. Leave the window open for the next lab.

Exercise 7.7: Configuring the DHCP Relay Agent on a Network Interface

In this lab, you will configure the DHCP relay that you created in the previous lab.

1. In the RRAS window, verify that the DHCP relay agent is installed. If it is not, refer to Exercise 7.6.
2. Right-click the DHCP Relay Agent item and choose New Interface.

3. The New Interface For DHCP Relay Agent dialog box appears, listing each of the interfaces to which you could attach the relay agent. Select Local Area Connection and click the OK button.
4. The interface-specific Properties dialog box appears. If you have a DHCP server on your local network, increase the boot threshold to 5 seconds; if you don't, decrease it to 0.
5. Click the OK button. Note that the list of DHCP relay agent interfaces has been updated to reflect the new interface. Leave the RRAS window open for the next exercise.

Managing User Access to Remote Access Services

In this section, you will configure the permissions, policies, and profiles that control user access to remote access services.

This section corresponds to Chapter 8, "Managing User Access to Remote Access Services," in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*.

You will perform the following tasks:

- Exercise 8.1: Creating a Remote Access Policy
- Exercise 8.2: Configuring a User Profile for Dial-In Access
- Exercise 8.3: Configuring Encryption
- Exercise 8.4: Creating a VPN Remote Access Policy
- Exercise 8.5: Configuring Authentication Protocols

Exercise 8.1: Creating a Remote Access Policy

In this lab, you will create a remote access policy for restricting access to the RRAS server.

1. Switch to the RRAS snap-in that should still be open from the previous lab.
2. Expand the server you want to configure in the left pane of the MMC.
3. Select the Remote Access Policies folder.
4. Select Action ➢ New Remote Access Policy. The New Remote Access Policy Wizard starts. Click Next to dismiss the Welcome page and continue with the wizard.
5. On the Policy Configuration Method page, select the Set Up A Custom Policy radio button, type **Working Hours Restrictions** in the Policy Name field, and then click the Next button.

6. On the Policy Conditions page, click the Add button. The Select Attributes dialog box appears.
7. Select the Day-and-Time-Restrictions attribute and then click the OK button.
8. The Time Of Day Constraints dialog box appears. Use the calendar controls to allow remote access Monday through Saturday from 7 A.M. to 7 P.M. and then click the OK button.
9. The Conditions page reappears, this time with the new condition listed. Click the Next button.
10. The Permissions page appears. Select the Grant Remote Access Permission radio button and click Next to continue.
11. The Profile page appears. Click the Next button (you'll edit the profile in the next exercise).
12. Click the Finish button on the confirmation screen to close the wizard and save your changes. Leave the window open since you will need it again later in this section.

Exercise 8.2: Configuring a User Profile for Dial-In Access

In this lab, you will configure a user profile for dial-in access.

1. Open the Active Directory Users And Computers snap-in by selecting Start ➢ Administrative Tools ➢ Active Directory Users And Computers.
2. Expand the tree to the Users folder. Right-click the Administrator account in the right-hand pane and choose Properties. The Administrator Properties dialog box appears.
3. Switch to the Dial-In tab. On machines that participate in Active Directory, the Control Access Through Remote Access Policy radio button in the Permissions group should be set.
4. Click the Deny Access radio button to prevent the use of this account over a dial-in connection.
5. Click the OK button. Close the Active Directory Users and Computers window.

Exercise 8.3: Configuring Encryption

In this lab, you will configure encryption settings on the RRAS server.

1. Open the RRAS snap-in by selecting Start ➢ Administrative Tools ➢ Routing And Remote Access.
2. Expand the server in the left pane of the MMC.
3. Select the Remote Access Policies folder. The right pane of the MMC displays the policies defined for this server. Select the Working Hours Restrictions policy (which you created in Exercise 8.1).
4. Select Action ➢ Properties. The policy Properties dialog box appears.

5. Click the Edit Profile button. The Edit Dial-In Profile dialog box appears. Select the Encryption tab.
6. Uncheck the No Encryption checkbox. Make sure that the Basic, Strong, and Strongest checkboxes are all marked.
7. Click the OK button. When the policy Properties dialog box reappears, click the OK button.
8. Leave the window open for the next lab.

Exercise 8.4: Creating a VPN Remote Access Policy

In this lab, you will create a policy for controlling access to the VPN.

1. In the RRAS window, expand the server node until you see the Remote Access Policies node.
2. Right-click the Remote Access Policies folder and choose New Remote Access Policy. This starts the New Remote Access Policy Wizard. Click Next on the Welcome screen.
3. Name the policy **VPN Access** and then click the Next button.
4. When the Policy Conditions page of the wizard appears, click the Add button to add this condition: NAS-Port-Type Attribute Set To "Virtual (VPN)." Click OK. Click the Next button. Click Next on the Policy Conditions page.
5. In the Permissions page of the wizard, make sure the Grant Remote Access Permission radio button is selected (unless you're trying to *prevent* VPN users from connecting). Click the Next button.
6. The Profile page appears next. If you want to create a specific profile (perhaps to restrict which authentication types VPN clients may use), use the Edit Profile button to specify the new profile. At a minimum, you should clear the No Encryption option on the Encryption tab of the remote access profile. When you're done editing the profile, click OK, click the Next button, then click the Finish button to create and activate the policy.
7. Leave the window open for the next lab.

Exercise 8.5: Configuring Authentication Protocols

In this lab, you will configure authentication protocols in RRAS.

1. In the RRAS window, select the server and then select Action ➢ Properties to open the server Properties dialog box.
2. Switch to the Security tab. Make sure that Windows Authentication is selected in the Authentication Provider drop-down list.
3. Click the Authentication Methods button. The Authentication Methods dialog box appears.

4. Select the Extensible Authentication Protocol (EAP) checkbox.
5. Select the two MS-CHAP checkboxes.
6. Select the CHAP checkbox.
7. Verify that the SPAP and PAP checkboxes are cleared.
8. Verify that the Allow Remote Systems To Connect Without Authentication checkbox is cleared.
9. Click the OK button; when the server Properties dialog box reappears, click its OK button.
10. You will be asked if you want to view the help files associated with configuring authentication protocols. Click No to finish the exercise.

Managing IP Routing

In this section, you will configure the Windows Server 2003 computer as a router.

This section corresponds to Chapter 9, "Managing IP Routing," in the *MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide*.

You will perform the following tasks:

- Exercise 9.1: Installing the Routing and Remote Access Services for IP Routing
- Exercise 9.2: Creating a Demand-Dial Interface
- Exercise 9.3: Installing the RIP and OSPF Protocols
- Exercise 9.4: Adding and Removing Static Routes
- Exercise 9.5: Configure PPTP Packet Filters
- Exercise 9.6: Monitoring Routing Status

Exercise 9.1: Installing the Routing and Remote Access Services for IP Routing

In this lab, you will configure and enable RRAS for IP routing, rather than for remote access like you did in the previous section.

1. In this lab, you will want to start over in the RRAS window without saving the changes from the previous section. If the RRAS window is still open, close it now. Then, open the RRAS MMC console by selecting Start ➢ Administrative Tools ➢ Routing And Remote Access.

2. Select the server in the left pane of the MMC. Right-click the server and choose Configure And Enable Routing And Remote Access. The Routing And Remote Access Server Setup Wizard appears. Click the Next button.
3. In the Configuration dialog box, ensure that the Secure Connection Between Two Private Networks radio button is selected and then click the Next button.
4. The Demand-Dial Connections page appears. Select Yes to use demand-dial connections. Click Next to continue.
5. On the IP Address Assignment page, you can choose how RRAS assigns IP addresses to incoming demand-dial calls. If you want to use DHCP (either a DHCP server on your network or the built-in address allocator), leave the Automatically radio button selected. If you want to pick out an address range, select the From A Specified Range Of Addresses button. Click the Next button.
6. If you chose to manually pass out IP addresses, the next page that appears is the Address Range Assignment page. You use this page to specify which IP address ranges you want handed out to incoming calls (whether demand-dial or from remote access users). Use the New, Edit, and Delete buttons to specify the address ranges you want to use and then click the Next button.
7. Click the Finish button on the Summary page to close the wizard. If you chose to create a demand-dial interface, the Demand-Dial Interface Wizard appears automatically. Leave the computer in its current state because the next exercise in this chapter will walk you through the Demand-Dial Interface Wizard.

Exercise 9.2: Creating a Demand-Dial Interface

In this lab, you will create a demand-dial interface.

1. In the Demand Dial Interface Wizard, click the Next button on the Welcome page. Specify a name for the interface on the Interface Name page.
2. The Connection Type dialog page will appear. Select the Connect Using A Modem, ISDN Adapter, Or Other Physical Device radio button on the Connection Type page if you have one of these devices installed. Select the Connect Using Virtual Private Networking (VPN) radio button if you want to connect to the remote router via a VPN interface. Alternately, you can choose to connect through a Point to Point over Ethernet (PPPoE) connection. For the rest of this exercise we will assume that you chose the first option. Click Next.
3. Select your device from the list of devices that appears on the Select A Device page. Click Next.
4. On the Protocols And Security page, make sure the Route IP Packets On This Interface checkbox is the only one selected. Click Next.

5. If you have not defined any static routes yet, you will be asked to do so before you can activate the demand-dial connection. On the Static Routes For Remote Networks page, click the Add button and enter the IP address, subnet mask, and metric of the remote router. Click OK when you're done. You will notice the new static route in the list. Click Next.
6. In the Dial Out Credentials page, fill in the username, domain (if any), and password needed to connect to the remote network. Click Next.
7. When the wizard summary page appears, click the Finish button to create the interface. You will return to the RRAS window. Leave the window open for the next lab.

Exercise 9.3: Installing the RIP and OSPF Protocols

In this lab, you will install the RIP and OSPF protocols in RRAS.

1. Select the server in the left pane of the MMC. Expand it until you see the General node beneath IP Routing.
2. Right-click the General node and select New Routing Protocol. The New Routing Protocol dialog box appears.
3. Select RIP Version 2 For Internet Protocol and click the OK button.
4. The RRAS console refreshes its display, revealing a new node labeled RIP under the IP Routing node.
5. Right-click the General node and select New Routing Protocol. This time, select Open Shortest Path First (OSPF) and click the OK button.
6. Leave the window open for the next lab.

Exercise 9.4: Adding and Removing Static Routes

In this lab, you will add and remove static routes from the routing table.

1. In the RRAS window, select the server in the left pane of the MMC. Expand it until you see the Static Routes node beneath IP Routing.
2. Right-click the Static Routes node and select New Static Route. The Static Route dialog box appears.
3. Select the interface you want to use from the Interface drop-down list; you can use the internal interface or any other interface you've already defined.
4. Enter **216.92.80.0** as the destination address and a net mask of **255.255.255.0**.
5. For the gateway address, enter the IP address of your RRAS server.

6. Click the OK button. The RRAS console reappears.
7. Right-click the Static Routes item and choose Show IP Routing Table. The IP Routing Table window appears. Verify that your newly added static route is present in the table.
8. Select the Static Routes item. Note that the right pane of the MMC changes to list all static routes that you've defined. Compare the list with the contents of the IP Routing Table window.
9. Right-click the static route you added and use the Delete command to remove it.
10. Leave the window open for the next lab.

Exercise 9.5: Configure PPTP Packet Filters

In this lab, you will configure PPTP packet filters for tunneling.

1. In the RRAS window, expand the server and IP Routing nodes to expose the General node of the server you're working on. Select the General node.
2. Right-click the interface that you used in the previous lab and choose Properties.
3. In the General tab of the interface Properties dialog box, click the Inbound Filters button. The Inbound Filters dialog box appears.
4. Click the New button and the Add IP Filter dialog box appears.
5. Fill out the Add IP Filter dialog box as follows:
   - Check the Destination Network checkbox.
   - Fill in the destination IP address field with the IP address of the remote VPN interface. For this lab, you can use any IP address.
   - Supply a destination subnet mask of **255.255.255.255**.
   - Select a protocol type of TCP and then specify a source port of 0 and a destination port of 1723.

   Click the OK button.
6. The Inbound Filters dialog box reappears, listing the new filter you created in step 5. Repeat step 5, but this time specify Other in the Protocol field and fill in a protocol ID of 47. When you're done, click the OK button and you'll go back to the Inbound Filters dialog box.
7. In the Inbound Filters dialog box, click the Drop All Packets Except Those That Meet The Criteria Below radio button and click the OK button.
8. Repeat steps 3–7, but this time create output filters. Make sure to specify the IP address of the VPN adapter as the source, not the destination!
9. Close the interface Properties dialog box.
10. Leave the window open for the next lab.

Exercise 9.6: Monitoring Routing Status

In this lab, you will monitor the IP routing interfaces in RRAS.

1. In the RRAS window, select the server in the left pane of the MMC. Expand it until you see the Network Interfaces node.
2. Select the Network Interfaces node. Note that the right pane of the MMC now lists all known interfaces along with their status and connection state.
3. Select the General node beneath IP Routing. Note that the right pane of the MMC updates to show the IP routing interfaces, their IP addresses, their administrative and operational states, and whether or not IP filtering is enabled on each interface.
4. Right-click the General node and choose Show TCP/IP Information. Check the number of IP routes shown.
5. Right-click the Static Routes node and choose Show IP Routing Table. Note that the number of routes listed corresponds to the route count in the TCP/IP Information window and that some of the routes listed are automatically generated.

Module

3

Windows Server 2003 Network Infrastructure Planning and Maintenance

The Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure exam requires that you know how to perform many hands-on tasks using Windows Server 2003. While most study guides provide you with the steps you need to know in order to perform many of these tasks, most students studying for the exam do not have access to a fully configured Windows Server 2003 network, and they cannot perform the exercises.

The Windows Server 2003 Network Infrastructure Planning and Maintenance module allows you to perform hands-on tasks in a simulated Windows environment. You can perform complicated exercises without the expense of a fully equipped network. If you get stuck, the simulator will show you how to perform the operation, just as if a live instructor were at your side pointing out what to do!

Most of the labs cover material that is explained in detail in the *MCSE: Windows Server 2003 Network Infrastructure Planning and Maintenance Study Guide,* by Suzan Sage London with James Chellis. We recommend that you have a copy of the Study Guide close at hand while performing these labs.

Planning a Network Connectivity Strategy

In this section, you will configure NAT on an RRAS server.

This section corresponds to Chapter 3, "Planning a Network Connectivity Strategy," in the *MCSE: Windows Server 2003 Network Infrastructure Planning and Maintenance Study Guide*. Due to Microsoft's overlapping exam objectives, many of the labs in this section were removed because they are exactly the same as labs from the previous module in the section titled "Managing IP Routing." Please review that section before proceeding.

You will perform the following lab:

- Exercise 3.1: Installing NAT on an RRAS Server

Exercise 3.1: Installing NAT on an RRAS Server

In this exercise, you will install NAT with the RRAS console.

1. Open the Routing And Remote Access snap-in by clicking Start ➢ Administrative Tools ➢ Routing And Remote Access.
2. If the configuration from Exercise 9.1 in the previous module is saved in the simulator, you can skip this step and continue directly to step 9. Otherwise, continue with step 3.

3. Select the server in the left pane of the MMC. Right-click the server and choose Configure And Enable Routing And Remote Access. The Routing And Remote Access Server Setup Wizard appears. Click the Next button.
4. In the Configuration dialog box, ensure that the Secure Connection Between Two Private Networks radio button is selected and then click the Next button.
5. The Demand-Dial Connections page appears. Select Yes to use demand-dial connections. Click Next to continue.
6. On the IP Address Assignment page, you can choose how RRAS assigns IP addresses to incoming demand-dial calls. If you want to use DHCP (either a DHCP server on your network or the built-in address allocator), leave the Automatically radio button selected. If you want to pick out an address range, select the From A Specified Range Of Addresses button. Click the Next button.
7. If you chose to manually pass out IP addresses, the next page that appears is the Address Range Assignment page. You use this page to specify which IP address ranges you want handed out to incoming calls (whether demand-dial or from remote access users). Use the New, Edit, and Delete buttons to specify the address ranges you want to use and then click the Next button.
8. Click the Finish button on the Summary page to close the wizard. If you chose to create a demand-dial interface, the Demand-Dial Interface Wizard appears automatically. Leave the computer in its current state because the next exercise in this chapter will walk you through the Demand-Dial Interface Wizard.
9. After the installation is complete, right-click the General node under IP Routing and select New Routing Protocol. In the New Routing Protocol dialog box, select the NAT/Basic Firewall option and click OK. If this choice does not appear, it was already installed via the RRAS Wizard.
10. Notice that a new node called "NAT/Basic Firewall" now appears under IP Routing.
11. Leave the Routing and Remote Access tool open for Exercise 6.1. Switch to the virtual desktop for the next lab.

Planning a WINS Strategy

In this section, you will configure WINS on a Windows Server 2003 computer.

This section corresponds to Chapter 5, "Planning a WINS Strategy," in the *MCSE: Windows Server 2003 Network Infrastructure Planning and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 5.1: Installing the WINS Service
- Exercise 5.2: Configuring WINS Replication
- Exercise 5.3: Manually Compacting the WINS Database with the Jetpack Utility
- Exercise 5.4: Using the `Nbtstat` Command

Exercise 5.1: Installing the WINS Service

In this exercise, you will install the WINS service on the server.

1. Open the Add Or Remove Programs in Control Panel by selecting Start ➢ Control Panel ➢ Add Or Remove Programs.
2. When the Add Or Remove Programs window appears, click the Add/Remove Windows Components icon. This starts the Windows Components Wizard.
3. In the Components list, scroll down until the Networking Services item is visible. Click it once, and click the Details button.
4. The Networking Services window appears. Scroll down the Networking Services list until you see Windows Internet Name Service (WINS), and then select its checkbox. Click the OK button.
5. The Windows Components Window reappears. Click the Next button.
6. If this were not a simulated environment, you would need to insert the Windows Server 2003 CD. In this lab, you can skip this step. Click Finish to close the wizard. Close the Add or Remove Programs window. You can leave the virtual desktop open for the next lab.

Exercise 5.2: Configuring WINS Replication

In this exercise, you will configure WINS replication.

1. Open the WINS snap-in by selecting Start ➢ Administrative Tools ➢ WINS.
2. Choose the WINS server you want to manage, and then expand it so you can see its Replication Partners node.
3. Right-click on Replication Partners and select New Replication Partner.
4. Enter the IP address of the WINS partner to add a replication partner.
5. Right-click the Replication Partners node, and choose Properties. The Replication Partners Properties dialog box appears.
6. On the General tab, make sure the Replicate Only With Partners checkbox is marked.

7. Switch to the Push Replication tab, and then check both Start Push Replication checkboxes.
8. Switch to the Pull Replication tab and verify that the Start Pull Replication At Service Startup checkbox is checked.
9. Click the OK button in the Properties dialog box. Close the WINS utility. Return to the lab selection screen.

Exercise 5.3: Manually Compacting the WINS Database with the Jetpack Utility

In this exercise, you will compact the WINS database using the jetpack utility.

1. Log on to the console of your WINS server.
2. Open the WINS snap-in by selecting Start ➢ Administrative Tools ➢ WINS.
3. Right-click the appropriate WINS server, and then choose All Tasks ➢ Stop.
4. Open a command prompt by selecting Start ➢ Run. Type **cmd**.
5. Change to the WINS database directory (by default, it's `Windows\system32\wins`).
6. Type **dir *.mdb** and note the size of the `wins.mdb` file.
7. Type **jetpack wins.mdb temp.mdb**.
8. Type **dir *.mdb** and note the size of the `wins.mdb` file. Determine whether or not the size has changed.
9. Switch back to the WINS snap-in console, right-click the server, and choose All Tasks ➢ Start command.

Exercise 5.4: Using the *Nbtstat* Command

In this exercise, you will use the `nbtstat` command to resolve a NetBIOS name.

1. Open the command prompt by selecting Start ➢ Run. Type **cmd**.
2. At the command prompt, type **`nbtstat /?`**. You should see the list of valid switches, as shown in Table 5.2.
3. Enter **`nbtstat -a`** ***`name`***, where ***`name`*** is the NetBIOS name of your computer. You should see output displaying the NetBIOS name table and MAC address of the local computer.
4. Try entering **`nbtstat -c`**. If there have been any recent successful attempts to resolve a NetBIOS name, the output of this command should include a list of names. If there haven't been any recent successful attempts, the command will return the message "No names in cache."

5. If step 4 returns at least one name, you can use `nbtstat` to clear the name cache. Change the IP address of one of the machines that was listed in the output of step 4, and then try pinging the NetBIOS name of that machine. You should receive a timeout message because the cache is pointing to an IP address that is no longer valid for that machine. Now enter **`nbtstat -R`** to purge the cache, and try pinging the NetBIOS name of that machine again. You should get a response this time.

Planning Secure Network Access

In this section, you will configure IPSec on a Windows Server 2003 computer.

This section corresponds to Chapter 6, "Planning Secure Network Access," in the *MCSE: Windows Server 2003 Network Infrastructure Planning and Maintenance Study Guide*. Due to Microsoft's overlapping exam objectives, many of the labs in this section were removed because they are exactly the same as labs from the previous module in the section titled "Managing IP Security." Please review that section before proceeding.

You will perform the following labs:

- Exercise 6.1: Configuring Security Options in the RRAS Server's Properties
- Exercise 6.2: Managing Remote Access Policies and Profiles

Exercise 6.1: Configuring Security Options in the RRAS Server's Properties

In this exercise, you will configure the properties for an RRAS server.

1. The RRAS window should still be open from Exercise 3.1. Switch to it now. If it is not open, then follow the steps in Exercise 3.1 to configure RRAS on the server.
2. In the Routing And Remote Access window, right-click your server and select Properties.
3. Click the Security tab and click the Authentication Methods button.
4. In the Authentication Methods dialog box, note the defaults. Click the OK button.
5. Click the OK button again to return to the main console window. Click No to close the warning dialog box. Leave the window open for the next lab.

Exercise 6.2: Managing Remote Access Policies and Profiles

In this exercise, you will edit the existing remote access policy and profile.

Due to Microsoft's overlapping exam objectives, some of the topics in this lab are repeated from Module 2. We recommend that you review this lab in order to reinforce your understanding of the topics covered.

1. In the Routing And Remote Access console, expand your computer, then expand Remote Access Policies. Right-click Connections To Microsoft Routing And Remote Access server and select Properties. This accesses the Properties dialog box for the policy, and the Settings tab is displayed.
2. In the Settings tab of the remote access policy Properties dialog box, click the Add button.
3. In the Select Attribute dialog box, select the Windows Groups attribute and click the Add button.
4. In the Groups dialog box, click the Add button.
5. In the Select Groups dialog box, add the Domain Users group and click the OK button.
6. In the Groups dialog box, click the OK button.
7. In the If A Connection Request Matches The Specified Conditions section of the Settings tab, click the Grant Remote Access Permission radio button. Then click the Edit Profile button.
8. In the Dial-In Constraints tab of the Edit Dial-In Profile dialog box, check the Minutes Server Can Remain Idle Before It Is Disconnected (Idle-Timeout) option and set it for 10 minutes. Check the Minutes Client Can Be Connected (Session-Timeout) option and set it to 60 minutes.
9. Click the IP tab. Configure IP address assignment by choosing Server Must Supply An IP Address.
10. Click the Multilink tab. Select the Allow Multilink Connections radio button and set the Maximum Number Of Ports Allowed: to 2 ports. Leave the Bandwidth Allocation Protocol (BAP) settings at the default values.
11. Click the Authentication tab. Deselect the default protocols and select Microsoft Encrypted Authentication version 2 (MS-CHAP v2).
12. Click the Encryption tab and note the default settings.
13. Click the Advanced tab and note the default settings.
14. Click the OK button to close the Edit Dial-In Profile dialog box.
15. In the Settings tab of the remote access policy's properties, click the OK button. Close the Routing and Remote Access tool.

Planning Server-Level Security

In this section, you will configure security options on a Windows Server 2003 computer.

This section corresponds to Chapter 7, "Planning Server-Level Security," in the *MCSE: Windows Server 2003 Network Infrastructure Planning and Maintenance Study Guide*. Due to Microsoft's overlapping exam objectives, many of the labs in this section were removed because they are exactly the same as labs from the previous module in the section titled "Administering Security Policy." Please review that section before proceeding.

You will perform the following labs:

- Exercise 7.1: Using the Configure Your Server Wizard
- Exercise 7.2: Using the Manage Your Server Tool
- Exercise 7.3: Creating a Custom MMC Console to Manage Security Policy for a New GPO
- Exercise 7.4: Setting Local User Rights

Exercise 7.1: Using the Configure Your Server Wizard

This exercise walks you through using the Configure Your Server Wizard to add or remove a server role, depending on whether or not the role has already been configured.

1. Launch the Configure Your Server Wizard by going to Start ➢ Administrative Tools ➢ Configure Your Server Wizard. Choose Next to continue.
2. The Preliminary Steps page displays the preliminary steps, prompting you to make sure all cabling and hardware is in place, peripherals are connected, and Internet connectivity is established if the computer will be used for Internet connectivity. You are also reminded to have your Windows Server 2003 CD on hand. Choose Next to continue.
3. After the wizard detects the network settings, the Server Role page is displayed.
4. Highlight the Streaming Media Server role to remove it, then click Next. The Role Removal Confirmation page is displayed. Note that you need to enable a checkbox to confirm removal of a role. Enable the checkbox, and choose Next to continue.
5. When the wizard finishes, choose Finish to close the wizard. Leave the virtual desktop open for the next lab.

Exercise 7.2: Using the Manage Your Server Tool

In this exercise, you will learn how to use the Manage Your Server tool.

1. Launch this tool on a domain controller by going to Start ➢ Administrative Tools ➢ Manage Your Server.

2. The main page of the Manage Your Server tool shows the roles that are configured for this server. Click Add Or Remove A Role at the top of the screen to launch the Configure Your Server Wizard. Choose Cancel to return to the main page of the Manage Your Server tool.
3. Scroll down to the Domain Controller (Active Directory) role, which has options to manage users and computers in Active Directory, manage domains and trusts, and manage sites and services. Click Manage Users And Computers In Active Directory, which launches the Active Directory Users And Computers console. Close the console to return to the main page of the Manage Your Server tool.
4. In the section for the Domain Controller (Active Directory) role, click Review The Next Steps For This Role, which opens Help and displays a checklist for completing additional tasks. Close Help to return to the main page of the Manage Your Server tool.
5. Click Computer And Domain Name Information in the upper-right corner of the page, which opens the System Properties page with the Computer Name tab active. Click Cancel to return to the main page of the Manage Your Server tool.
6. Exit the Manage Your Server tool. Leave the virtual desktop open for the next lab.

Exercise 7.3: Creating a Custom MMC Console to Manage Security Policy for a New GPO

In this exercise, you'll create a management console for a new GPO named *Security Policy GPO*, and customize it by adding Event Viewer. This exercise is performed from a domain controller. The Security Policy GPO will be used for the remaining exercises in the module.

For the remaining exercises in this module, you will be logged on as the Administrator.

1. Select Start ➢ Run, type ***MMC*** in the Run dialog box, and choose OK to open the MMC.
2. From the main menu, select File ➢ Add/Remove Snap-In.
3. In the Add/Remove Snap-In dialog box, choose Add. The Add Standalone Snap-In is displayed.
4. Highlight the Group Policy Object Editor snap-in and choose Add. The Group Policy Wizard is displayed.
5. The Group Policy Object specifies Local Computer by default. Choose Browse to browse for a Group Policy Object.
6. The Browse For A Group Policy Object dialog box is displayed. The Domains/OU tab is the default, showing the current domain. Notice that you can choose the Default Domain Policy here, and that you have a Create New Group Policy Object button to the right of the drop-down list of domains (it's the middle icon). In the Domains/OUs tab, click the Create New Group Policy Object button. Name the GPO **Security Policy GPO**. Choose OK, then choose Finish to return to the Add Standalone Snap-in window.

7. Highlight the Event Viewer snap-in and choose Add.
8. The Select Computer dialog box appears with Local Computer selected by default. Choose the Another Computer radio button, and type Sybex.com.
9. Click Finish, then Close.
10. In the Add/Remove Snap-In dialog box, notice that the new GPO is now listed, along with Event Viewer.
11. Choose OK to return to the main console window.
12. Select File ➢ Save As. Save the console as **Security Policy GPO**.
13. You can now access this console by selecting Start ➢ Administrative Tools ➢ Security Policy GPO. For now, close the MMC.

Exercise 7.4: Setting Local User Rights

In this exercise, you will apply a local User Rights Assignment policy.

1. Select Start ➢ Administrative Tools ➢ Security Policy GPO, and expand the Security Policy GPO object.
2. Expand folders as follows: Computer Configuration, Windows Settings, Security Settings, Local Policies, User Rights Assignment.
3. Double-click the Log On As A Service user right to open its Properties page.
4. Click Define These Policy Settings. Click the Add User Or Group button. The Select Users Or Groups dialog box appears.
5. Enter user **Matt**. Then click the OK button. Close the MMC window.

Planning Certificate Services

In this section, you will plan certificate services on a Windows Server 2003 computer.

This section corresponds to Chapter 8, "Planning Certificate Services," in the *MCSE: Windows Server 2003 Network Infrastructure Planning and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 8.1: Assigning Permissions to Templates
- Exercise 8.2: Enabling Automatic Enrollment
- Exercise 8.3: Creating a New CTL

- Exercise 8.4: Revoking a Certificate
- Exercise 8.5: Issuing Certificates
- Exercise 8.6: Using the Certificate Import Wizard

Exercise 8.1: Assigning Permissions to Templates

The Active Directory Sites and Services snap-in is where you adjust permissions for enterprise-wide services, including the use of certificate templates and other PKI components. You will adjust template permissions in Exercise 8.1.

You will perform this exercise on an enterprise CA.

1. Open the Active Directory Sites And Services snap-in.
2. Highlight the main node for the domain, then right-click the node and choose View ➢ Show Services Node.
3. Expand Services ➢ Public Key Services, and choose Certificate Templates node. This fills the right half of the MMC window with a list of installed templates.
4. Right-click the template whose permissions you want to set, then choose Properties. When the Properties dialog box appears, switch to the Security tab.
5. Adjust the permissions to suit your needs. To keep users from using the template to request new certificates, make sure that you deny the appropriate groups the Enroll permission. Close the Active Directory Sites and Services tool.

Exercise 8.2: Enabling Automatic Enrollment

This exercise shows you how to enable automatic enrollment for the CA.

You will use an enterprise CA to complete this exercise.

1. Open the Security Policy GPO in the Administrative Tools folder.
2. Open the GPO's Computer Configuration node, then open Windows Settings ➢ Security Settings, and expand the Public Key Policies node. This exposes four subfolders beneath the Public Key Policies node.

3. Right-click the Automatic Certificate Request Settings folder under the Public Key Policies node, and select New ➢ Automatic Certificate Request. This starts the Automatic Certificate Request Wizard.
4. Click Next to get past the wizard's introductory page. When the Certificate Template page appears, it lists all the types of certificates that can be automatically issued to computers. Normally, you'll use the basic Computer type, but separate types exist for domain controllers and devices that participate in IPSec. Select the template type you want to use, then click the Next button. Click Finish to close the Wizard.
5. Once you've completed these steps, the new request appears as an item in the Automatic Certificate Request Settings folder; you can edit or remove it later by selecting it and using the commands in the Action menu.
6. Leave the window open for the next lab.

Exercise 8.3: Creating a New CTL

This exercise shows you how to create a new CTL.

You must perform the steps of this exercise on a domain controller.

1. In the GPO snap-in, right-click the Enterprise Trust folder. Then select the New ➢ Certificate Trust List command to start the Certificate Trust List Wizard. Click the Next button, and you'll see the Certificate Trust List Purpose page.
2. Enter a descriptive prefix for the CTL in the provided field. Leave the other options at the default and click Next.
3. The Certificates In The CTL page appears. Click the Next button to continue.
4. The Signature Certificate page appears. Examine the default settings and click Next to continue.
5. On the Secure Timestamp page, check the Add A Timestamp To The Data checkbox, then enter a URL in the Timestamp Service URL field. For purposes of this lab, you can enter any URL. Click Next to continue.
6. Enter any name in the Friendly Name field, and any description in the description field. Then click Next to continue.
7. Once you've completed the wizard, you get the usual summary page. Clicking the Finish button will create the CTL and store it in Active Directory. Close the MMC window. Close the desktop and return to the lab list.

Exercise 8.4: Revoking a Certificate

In this exercise you will revoke a certificate.

1. Open the Certification Authority administrative tool by selecting Start ➢ Administrative Tools ➢ Certification Authority. Expand the CA folder.
2. Open the Issued Certificates folder, and then select the certificate you want to revoke.
3. Right-click the certificate, and choose All Tasks ➢ Revoke Certificate.
4. Select a reason code for the revocation, and then click the OK button.

Exercise 8.5: Issuing Certificates

You will see how to issue a certificate with the web enrollment component in this exercise. Your server is preconfigured to use IIS, which is required in order to continue.

1. Open a Web browser and load the CA enrollment page (`http://localhost/certsrv/`).
2. When the Microsoft Certificate Services page appears, click Request A Certificate.
3. In the Request A Certificate page, click User Certificate.
4. The User Certificate–Identifying Information page will appear. Click Submit and a summary page will appear telling you that the CA has all the information it needs.
5. If you have automatic certificate approval turned on, which it is by default, you'll see a page titled Certificate Issued with a link reading Install This Certificate. Click it and your new certificate will be downloaded and installed.

Exercise 8.6: Using the Certificate Import Wizard

This exercise shows you how to use the Certificate Import Wizard to import the certificate that you exported in the previous exercise.

1. Start the Certificate Import Wizard by right-clicking the Personal certificate storage folder and selecting All Tasks ➢ Import.
2. Skip the introductory page by clicking its Next button.
3. On the File To Import page, provide the full path and filename of the certificate file that you exported in the previous exercise, and then click the Next button. Alternatively, you can browse to the file by selecting the Browse button. You can import certificates in three formats:
   - PKCS#12 (`.PFX` or `.P12`) files are used to store certificates with their associated private keys. Outlook, Outlook Express, and Netscape's tools all produce PKCS#12 files when you export a certificate, as do many third-party PKI components.

- PKCS#7 (`.P7B`, `.P7C`, or `.CRT`) files are used to store certificates without keys. A PKCS#7 file can contain an entire certificate chain (including CA certificates) or just a certificate—the application that creates the file gets to decide what goes in it. Almost every PKI component that runs on Windows can produce PKCS#7 files.
- Microsoft's own SST format, which is sparsely used.

4. The Certificate Store page allows you to choose the store in which you want to put the certificate. Choose the Automatically Select The Certificate Store Based On The Type Of Certificate radio button and click Next.
5. The Completing the Certificate Import Wizard page is displayed. Click Finish to actually import the certificate. You'll get a dialog box indicating whether the import attempt succeeded or not.

Planning Network Monitoring, Remote Administration, and Recovery

In this section, you will plan network monitoring, remote administration, and system recovery on a Windows Server 2003 computer.

This section corresponds to Chapter 10, "Planning Network Monitoring, Remote Administration, and Recovery," in the *MCSE: Windows Server 2003 Network Infrastructure Planning and Maintenance Study Guide*. Due to Microsoft's overlapping exam objectives, many of the labs in this section were removed because they are exactly the same as labs from Module 1 in the sections titled "Optimizing Windows Server 2003" and "Performing System Recovery Functions," and Module 2 in the section titled "Installing and Configuring TCP/IP." Please review those sections before proceeding.

You will perform the following lab:

- Exercise 10.1: Monitoring Network Services

Exercise 10.1: Monitoring Network Services

In this exercise, you will monitor network infrastructure services on your network. To monitor Network Server Activity on a file and print server, follow these steps:

1. Open System Monitor by launching Start ➢ Administrative Tools ➢ Performance.
2. Click the Add button on the toolbar.

3. In the Add Counters dialog box, specify a file and print server other than the local computer and select the following performance objects and counters:
   a. Select Server from the performance object drop-down list, select Bytes Total/Sec in the counter list box, and click the Add button.
   b. Select Server from the performance object drop-down list, select Server Sessions from the counter list box, and click the Add button.
   c. Select Server from the performance object drop-down list, select Sessions Errored Out from the counter list box, and click the Add button.
   d. Select Print Queue from the performance object drop-down list, select Jobs from the counter list box, and click the Add button.
   e. Select Print Queue from the performance object drop-down list, select Bytes Printed/Sec from the counter list box, and click the Add button.
   f. Select Print Queue from the performance object drop-down list, select Out Of Paper Errors from the counter list box, and click the Add button.
4. Click the Close button. You will see these counters added to your chart.
5. Change to the Histogram view by clicking the Histogram button on the toolbar. The Histogram button looks like a small bar graph.
6. From a client computer, generate activity to be measured by copying several files from the file server. Remove the paper from the printer and send three one-page print jobs to the printer.
7. Note the change in counters for the Server and Print Queue performance objects. These numbers are cumulative for the session. You can use them in your baselines to estimate the load on a file and print server.
8. Go to Start ➢ Control Panel ➢ Printers and Faxes, and open the print queue for the printer to which you sent the jobs. Clear the print queue by choosing Printer ➢ Cancel All Documents, and choose Yes when prompted.

To monitor the Network Server Activity on a Web server, follow these steps:

9. Launch System Monitor on a computer that is configured as a Web server.
10. Remove the default counters by highlighting each counter and clicking the Delete button on the toolbar. The Delete button looks like a black X.
11. Click the Add button on the toolbar.
12. In the Add Counters dialog box, specify a Web server other than the local computer and select the following performance objects and counters:
    a. Select Web Service from the performance object drop-down list, select Bytes Total/Sec in the counter list box, choose the appropriate instance, and click the Add button.
    b. Select Web Service from the performance object drop-down list, select Get Requests/Sec from the counter list box, choose the appropriate instance, and click the Add button.

   c. Select Web Service from the performance object drop-down list, select Total Not Found Errors from the counter list box, choose the appropriate instance, and click the Add button.
   d. Select Web Service from the performance object drop-down list, select Service Uptime from the counter list box, choose the appropriate instance, and click the Add button.
   e. Select Web Service Cache from the performance object drop-down list, select File Cache Hits % from the counter list box, choose the appropriate instance, and click the Add button.
13. Click the Close button. You will see these counters added to your chart.
14. Change to the Histogram view by clicking the Histogram button on the toolbar. The Histogram button looks like a small bar graph.
15. From a client computer, generate activity to be measured by accessing every page in the Web site through Internet Explorer.
16. Note the change in counters for the Web Service and Web Service Cache performance objects. These numbers are cumulative. You can use them in your baselines to estimate load on a Web server.

Module

4

Windows Server 2003 Active Directory Planning, Implementation, and Maintenance

The Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure exam requires that you know how to perform many hands-on tasks using Windows Server 2003. While most study guides provide you with the steps you need to know in order to perform many of these tasks, most students studying for the exam do not have access to a fully configured Windows Server 2003 network, and they cannot perform the exercises.

The Windows Server 2003 Active Directory Planning, Implementation, and Maintenance module allows you to perform hands-on tasks in a simulated Windows environment. You can perform complicated exercises without the expense of a fully equipped network. If you get stuck, the simulator will show you how to perform the operation, just as if a live instructor were at your side pointing out what to do!

Most of the labs cover material that is explained in detail in the *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide* by Anil Desai and James Chellis. We recommend that you have a copy of the Study Guide close at hand while performing these labs.

Planning and Installing the Active Directory

In this section, you will prepare for and install Active Directory on a Windows Server 2003 machine. This process automatically makes the machine a domain controller and sets up the machine for the rest of the exercises in this module.

This section corresponds to Chapter 2, "Planning and Installing the Active Directory," in the *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 2.1: Promoting a Domain Controller
- Exercise 2.2: Viewing the Active Directory Event Log
- Exercise 2.3: Configuring DNS Integration with Active Directory

Exercise 2.1: Promoting a Domain Controller

In this exercise, you will promote an existing Windows Server 2003 computer to a domain controller.

If this were not a simulated environment, you would need to have already installed and configured a Windows Server 2003 computer and a DNS server that supports SRV records. If you do not have a DNS server available, the Active Directory Installation Wizard automatically configures one for you.

1. Open the Manage Your Server utility, which is located in the Administrative Tools program group.
2. Click Add Or Remove A Role and click Next to begin the process. For the server role, select Domain Controller (Active Directory) and then click Next. Finally, click Next once more to start the Active Directory Installation Wizard.

Alternatively, you can start the Active Directory Installation Wizard by clicking Start ➢ Run and typing **dcpromo**.

3. Click Next on the Welcome To The Active Directory Installation Wizard page to begin the domain controller promotion process. The Operating System Compatibility page of the wizard provides you with an important note about operating system compatibility. Click Next to continue.
4. On the Domain Controller Type page, specify the type of domain controller this server will be. To choose the domain controller type, select Domain Controller For A New Domain and click Next.
5. On the Create New Domain page, choose whether the new domain tree is part of an existing forest or a new one that you create. Since this is the first tree in the forest, select Domain In A New Forest and click Next.
6. On the New Domain page, type **`test.mycompany.com`** as the full name of the DNS domain. Once you've selected a name, click Next.

If you are not working in a test environment, be sure that you have chosen a root domain name that is consistent for your organization, and doesn't overlap with others. For example, you might choose `ActiveDirectory.test`, since it is unlikely to conflict with other existing domains and DNS namespaces.

7. On the NetBIOS Domain Name page, type in the NetBIOS name for this machine and click Next.
8. In the Database And Log Folders page, you can specify the file system locations for the Active Directory database and log file. Leave the settings at the default and click Next.
9. On the Shared System Volume page, you can select a shared system volume location. Leave the default settings and click Next.

10. On the Permissions page, choose Permissions Compatible Only With Windows 2000 Or Windows Server 2003 Operating Systems and click Next.
11. On the Directory Services Restore Mode Administrator Password page, provide a Directory Services Restore Mode Administrator password. Once you've selected and confirmed the password, click Next.
12. Based on the installation options you've selected, the Active Directory Installation Wizard presents a summary of your choices. Verify the options, then click Next to begin the Active Directory installation process. When the necessary operations are complete, the wizard prompts you to click Finish. For purposes of this simulation, click Don't Restart Now.

Exercise 2.2: Viewing the Active Directory Event Log

This exercise walks you through the process of viewing Active Directory-related events in the Event Viewer. Entries seen with the Event Viewer include errors, warnings, and informational messages. You should complete the previous exercise before attempting this lab.

1. Open the Event Viewer snap-in from the Administrative Tools program group.
2. In the left pane, select Directory Service.
3. Double-click an event in the list to see the details for that item. Click OK when you are done viewing an event.
4. Filter an event list by right-clicking the Directory Service item in the left pane, selecting Properties, and then selecting the Filter tab. Deselect the Warning checkbox and click OK. Notice how any warnings in the display are no longer visible. Note that filtering does not remove entries from the event logs—it only restricts their display.
5. To verify the Active Directory installation, look for events related to the proper startup of Active Directory, such as Event ID 1000 (Active Directory Startup Complete) and 1394 (Attempts To Update The Active Directory Database Are Succeeding). Also, be sure to examine any Error or Warning messages because these could indicate problems with DNS or other necessary services.
6. When you're done viewing information in the Event Viewer, close the application.

Exercise 2.3: Configuring DNS Integration with Active Directory

This exercise shows the steps that you can take to ensure that DNS Active Directory integration features are enabled.

1. Open the DNS snap-in from the Administrative Tools program group.
2. Right-click the icon for the local DNS Server, and select Properties. Click the Security tab. Notice that you can now specify which users and groups have access to modify the configuration of the DNS server. Make any necessary changes, and click OK.

3. If they aren't already expanded, expand the local server branch and the Forward Lookup Zones folder.
4. Right-click the domain you want to work on and select Properties.
5. On the General tab, verify that the type is Active Directory-Integrated and that the Data Is Stored In Active Directory message is displayed. If this option is not currently selected, you can change it by clicking the Change button next to Type.
6. Verify that the Dynamic Updates option is set to Secure Only Updates.
7. Finally, notice that you can define the security permissions at the zone level by clicking the Security tab. Make any necessary changes, and click OK. Close the DNS tool.

Installing and Managing Trees and Forests

In this section, you will see how to create new domain trees and forests, assign single master operations, manage trust relationships, add a UPN suffix, and manage global catalog servers. All of these exercises require multiple domains, which are managed in trees and forests.

This section corresponds to Chapter 3, "Installing and Managing Trees and Forests," in the *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide*.

You will perform these labs:

- Exercise 3.1: Creating a New Subdomain
- Exercise 3.2: Assigning Single Master Operations
- Exercise 3.3: Managing Trust Relationships
- Exercise 3.4: Adding and Removing a UPN Suffix
- Exercise 3.5: Managing Global Catalog Servers

Exercise 3.1: Creating a New Subdomain

In this exercise, you will create a new child domain using the Active Directory Installation Wizard.

This exercise assumes that you have already created the parent domain, and that you are using a server in the domain that is not already a domain controller.

1. Log on to the computer as a member of the Administrators group and open the Active Directory Installation Wizard by clicking Start ➢ Run and typing **dcpromo**. Click Next to begin the wizard.
2. You will see a message that states that Windows 95 and Windows NT 4.0 computers running Service Pack 3 or earlier will be unable to communicate with Windows Server 2003 computers. Read the information and click Next to continue.
3. On the Domain Controller Type page, select Domain Controller For A New Domain. Click Next.
4. On the Create New Domain page, choose Child Domain In An Existing Domain Tree. Click Next.
5. On the Network Credentials page, enter the username and password for the domain administrator of the domain you wish to join. You will also need to specify the full name of the domain. For purposes of this simulation, you can enter any information here. After you have entered the appropriate information, click Next.
6. On the Child Domain Installation page, enter the name of the child domain. Click Next to continue.
7. On the NetBIOS Domain Name page, you'll be prompted for the NetBIOS name for this domain controller. Choose a name that is up to 15 characters in length and includes only alphanumeric characters. Click Next to continue.
8. On the Database And Log Folders page, you'll need to specify the database and log locations. Leave the default settings and click Next.
9. On the Shared System Volume page, accept the default settings and click Next.
10. The Active Directory Installation Wizard prompts you about whether or not the DNS service on the local machine should be configured automatically. Accept the setting to allow the wizard to automatically configure DNS. Click Next to continue.
11. On the Permissions page, choose Permissions Compatible Only With Windows 2000 Or Windows Server 2003 Operating Systems. Click Next.
12. On the Directory Services Restore Mode Administrator Password page, enter a password, confirm it, and click Next.
13. On the Summary page, you will be given a brief listing of all the choices you made in the previous steps. Click Next to continue.
14. The Active Directory Installation Wizard will automatically begin performing the steps required to create a new domain in your environment. Note that you can click Cancel if you want to abort this process. When the process has completed, you will be prompted to reboot the system. After the system has been rebooted, the local server will be the first domain controller in a new domain. This domain will also be a subdomain of an existing one.

Exercise 3.2: Assigning Single Master Operations

This exercise shows you how single master operations roles can be assigned to servers within the Active Directory environment.

1. Open the Active Directory Domains And Trusts administrative tool by clicking Start ➢ Administrative Tools ➢ Active Directory Domains And Trusts.
2. Right-click Active Directory Domains And Trusts and choose Operations Master.
3. This brings up the Change Operations Master dialog box. Click Close to continue without making any changes.

Note that you can change the operations master by clicking the Change button. If you want to move this assignment to another computer, you first need to connect to that computer and then make the change.

4. Close the Active Directory Domains And Trusts administrative tool.
5. Select Start ➢ Administrative Tools ➢ Active Directory Users And Computers.
6. Right-click the name of the domain and select Operations Masters. This brings up the RID tab of the Operations Master dialog box.

Notice that you can change the computer that is assigned to the role. In order to change the role, you first need to connect to the appropriate domain controller. Notice that the PDC and Infrastructure roles have similar tabs.

7. Click OK to continue without making any changes. Leave the window open for the next lab.

Exercise 3.3: Managing Trust Relationships

In this exercise, you will see how to manage trusts and assign trust relationships between domains.

1. If it is not already open, open the Active Directory Domains And Trusts administrative tool by clicking Start ➢ Administrative Tools ➢ Active Directory Domains And Trusts.
2. Right-click the name of the domain and select Properties.
3. Select the Trusts tab. You will see a list of the trusts that are currently configured. To modify the trust properties for an existing trust, highlight the trust and click Properties.
4. This screen displays information about the trust's direction, transitivity, and type, along with the names of the domains involved in the relationship. Click Cancel to exit without making any changes.

5. To create a new trust relationship, click the New Trust button on the Trusts tab. The New Trust Wizard appears. Click Next to proceed with the wizard.
6. On the Trust Name page, you are prompted for the name of the domain with which the trust should be created. For purposes of this lab, you can enter any domain name and click Next.
7. On the Trust Type page, you would normally choose the Trust With A Windows Domain option if you know that the other domain uses a Windows domain controller. In order to continue with this lab (without requiring access to another domain), it is important to choose the Realm Trust option. This selection allows you to walk through the process of creating a trust relationship without needing an untrusted domain in the Active Directory environment. Select the Realm Trust option. Click Next when you are done.
8. On the Transitivity Of Trust page, choose the Nontransitive option and click Next to continue.
9. On the Direction Of Trust page, choose One-Way: Incoming and click Next.
10. On the Trust Password page, specify a password that should be used to administer the trust. Click Next to continue.

Note that if there is an existing trust relationship between the domains, the passwords must match.

11. Now you see a summary page that recaps the selections you have made. Since this is a simulation, you don't actually want to establish this trust. Click Cancel on the Trust Selections Complete page to cancel the wizard without saving the changes.
12. Exit the Trust properties for the domain by clicking Cancel.
13. Leave the window open for the next lab.

Exercise 3.4: Adding and Removing a UPN Suffix

In this exercise, you will add additional suffixes to a forest.

1. In the Active Directory Domains And Trusts tool, right-click Active Directory Domains And Trusts in the left side of the window and select Properties.
2. On the UPN Suffixes tab of the Active Directory Domains And Trusts Properties dialog box, enter any alternate UPN suffix in the Alternate UPN Suffixes field. Click the Add button to add the suffix to the list.
3. To remove a UPN suffix, select its name in the list and click the Remove button. Close the Active Directory Domains and Trusts tool.

Exercise 3.5: Managing Global Catalog Servers

This exercise walks you through the steps you need to take to configure a domain controller as a Global Catalog server.

1. Open the Active Directory Sites And Services administrative tool by clicking Start ➢ Administrative Tools ➢ Active Directory Sites And Services.
2. Find the name of the local domain controller within the list of objects (typically under Default First Site Name ➢ Servers) and expand this object. Right-click NTDS Settings and select Properties.
3. In the NTDS Settings Properties dialog box, type **Primary GC Server for Domain** in the Description field. Select the Global Catalog checkbox, then click OK to continue.

If the box is checked, then this domain controller contains a subset of information from all other domains within the Active Directory environment.

4. Leave the window open for the next lab.

Configuring Sites and Managing Replication

In this section, you will configure sites, which are used to determine the flow of replication traffic.

This section corresponds to Chapter 4, "Configuring Sites and Managing Replication," in the *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 4.1: Creating Sites
- Exercise 4.2: Creating Subnets
- Exercise 4.3: Configuring Sites
- Exercise 4.4: Creating Site Links and Site Link Bridges
- Exercise 4.5: Creating Connection Objects
- Exercise 4.6: Moving Server Objects between Sites

Exercise 4.1: Creating Sites

In this exercise, you will create new sites that represent the physical locations of the company.

1. Open the Active Directory Sites And Services administrative tool by clicking Start ➢ Administrative Tools ➢ Active Directory Sites And Services.
2. Expand the Sites folder.
3. Right-click the Default-First-Site-Name item and choose Rename. Rename the site to **CorporateHQ**.
4. Create a new site by right-clicking the Sites object and selecting New Site.
5. On the New Object–Site dialog box, type **Austin** for the site name. Click the DEFAULTIPSITELINK item, then click OK to create the site. Note that you cannot include spaces or other special characters in the name of a site.
6. You will see a dialog box stating the actions that you should take to finish the configuration of this site. Click OK to continue.
7. Create another new site and name it **NewYork**. Again, choose the DEFAULTIPSITELINK item.
8. Leave the window open for the next lab.

Exercise 4.2: Creating Subnets

In this exercise, you will create subnets that are associated with your sites. You should have completed the previous lab before attempting this exercise.

1. In the Active Directory Sites And Services tool, expand the Sites folder. Right-click the Subnets folder and select New Subnet.
2. In the New Object–Subnet dialog box, you are prompted for TCP/IP information for the new subnet. For the address, type **100.1.1.0**, and for the mask, type **255.255.255.0**. You will see that the Name value has been automatically calculated as 100.1.1.0/24. Click the Austin site, then click OK to create the subnet.
3. In the Active Directory Sites And Services tool, right-click the newly created 100.1.1.0/24 subnet object and select Properties.
4. On the subnet Properties dialog box, type **Austin 100Mbit LAN** for the description. Click OK to continue.
5. Create a new subnet using the following information:

   Address: **160.25.0.0**

   Mask: **255.255.0.0**

   Site: **NewYork**

   Description: **NewYork 100Mbit LAN**

6. Create another subnet using the following information:

   Address: **176.33.0.0**

   Mask: **255.255.0.0**

   Site: **CorporateHQ**

   Description: **Corporate 100Mbit switched LAN**

7. Leave the window open for the next lab.

Exercise 4.3: Configuring Sites

In this exercise, you will configure the sites that you created earlier. You should have completed the previous lab before attempting this exercise.

1. In the Active Directory Sites And Services tool, expand the Sites folder, then click and expand the Austin site.
2. Right-click the Servers container in the Austin site and select New ➢ Server. Type **AustinDC1** for the name of the server, then click OK.
3. Create a new Server object within the CorporateHQ site and name it **CorpDC1**. Note that this object also includes the name of the local domain controller.
4. Create two new Server objects within the NewYork site and name them **NewYorkDC1** and **NewYorkDC2**.
5. Right-click the NewYorkDC1 Server object and select Properties. In the NewYorkDC1 Properties box, select the IP in the Transports Available For Inter-site Data Transfer box and click Add to make this server a preferred IP bridgehead server. Click OK to accept the settings.
6. Set the Licensing server for the CorporateHQ site by clicking the Austin container and look in the right pane. Right-click the Licensing Site Settings object, and select Properties. To change the computer that will act as the Licensing server for the site, click Change in the Licensing Site Setting Properties dialog box. Enter the name of the local domain controller and click OK. Click OK to save the settings.
7. Leave the window open for the next lab.

Exercise 4.4: Creating Site Links and Site Link Bridges

In this exercise, you will create site links and site link bridges for the sites you created earlier. You should have completed the previous lab before attempting this exercise.

1. In the Active Directory Sites And Services tool, expand Sites, Inter-site Transports, IP object. Right-click the DEFAULTIPSITELINK item in the right pane and select Rename. Rename the object to **CorporateWAN**.

2. Right-click the CorporateWAN link and select Properties. In the CorporateWAN Properties dialog box, type **T1 Connecting Corporate and NewYork Offices** for the description. Remove the Austin site from the link by highlighting Austin and clicking Remove. For the Cost value, type **50**, and specify that replication should occur every 60 minutes. To create the site link, click OK.
3. Right-click the IP folder and select New Site Link. On the New Object–Site Link dialog box, name the link **CorporateDialup**. Add the Austin and CorporateHQ sites to the site link and click OK.
4. Right-click the CorporateDialup link and select Properties. In the CorporateDialup Properties dialog box, type **ISDN Dialup between Corporate and Austin office** for the description. Set the Cost value to 100, and specify that replication should occur every 120 minutes. To specify that replication should occur only during certain times of the day, click the Change Schedule button.
5. On the Schedule For CorporateDialup dialog box, highlight the area between 8:00 A.M. and 6:00 P.M. for the days Monday through Friday, and click the Replication Not Available option. This will ensure that replication traffic is minimized during normal work hours. Click OK to accept the new schedule, then OK again to create the site link.
6. Right-click the IP object, and select New Site Link Bridge. In the New Object–Site Link Bridge dialog box, name the site link bridge **CorporateBridge**. Note that the CorporateDialup and CorporateWAN site links are already added to the site link bridge. Since there must be at least two site links in each bridge, you will not be able to remove these links. Click OK to create the site link bridge.
7. Leave the window open for the next lab.

Exercise 4.5: Creating Connection Objects

In this exercise, you will create connection objects. You should have completed the previous lab before attempting this exercise.

1. In the Active Directory Sites And Services tool, find the site that contains the local domain controller and expand this object.
2. Expand the name of the local domain controller. Right-click NTDS Settings and select New Active Directory Connection.
3. The Find Domain Controllers box appears, showing a list of the servers that are available. Highlight the name of the server to which you want to connect and click OK.
4. For the name of the connection object, type **Connection**. Click OK.
5. In the right pane of the Active Directory Sites And Services tool, right-click the Connection item and select Properties.
6. When the Connection Properties dialog box appears, type **After-hours synchronization** in the Description field. For the Transport, choose IP from the drop-down list.

7. When you are finished, click OK to save the properties of the Connection object.
8. Leave the window open for the next lab.

Exercise 4.6: Moving Server Objects between Sites

In this exercise, you will move a server from one site to another. You should have completed the previous lab before attempting this exercise.

1. In the Active Directory Sites And Services tool, right-click the server named NewYorkDC1 and select Move.
2. In the Move dialog box, select the Austin site, then click OK. This moves the server to the Austin site.
3. To move the server back, right-click NewYorkDC1 (now located in the Austin site) and click Move. Select New York for the destination site.
4. When finished, close the Active Directory Sites And Services administrative tool.

Administering the Active Directory

In this section, you will create and manage OUs and other Active Directory objects. In addition, you will publish shared folders and printers to the Active Directory, find objects in the Active Directory, and delegate control of objects to other users.

This section corresponds to Chapter 5, "Administering the Active Directory," in the *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 5.1: Creating an OU Structure
- Exercise 5.2: Modifying an OU Structure
- Exercise 5.3: Creating Active Directory Objects
- Exercise 5.4: Managing Object Properties
- Exercise 5.5: Moving Active Directory Objects
- Exercise 5.6: Resetting an Existing Computer Account
- Exercise 5.7: Finding Objects in Active Directory
- Exercise 5.8: Creating and Publishing a Printer
- Exercise 5.9: Creating and Publishing a Shared Folder

Exercise 5.1: Creating an OU Structure

In this exercise, you will create an OU structure that you will use for the rest of the labs in this chapter.

1. Open the Active Directory Users And Computers administrative tool by clicking Start ➢ Administrative Tools ➢ Active Directory Users And Computers.
2. Right-click the name of the local domain, and choose New ➢ Organizational Unit. Notice that this box shows you the current context within which the OU will be created. In this case, you're creating a top-level OU, so the full path is simply the name of the domain.
3. Type **North America** for the name of the first OU. Click OK to create this object.
4. Create the following top-level OUs by right-clicking the name of the domain and choosing New ➢ Organizational Unit:

   Africa

   Asia

   Europe

   South America

Note that the order in which you create the OUs is not important. In this exercise, you are simply using a method that emphasizes the hierarchical relationship.

5. Create the following second-level OUs within the North America OU by right-clicking the North America OU and selecting New ➢ Organizational Unit:

   Austin

   Boston

   Canada

   Chicago

   Corporate

   Los Angeles

   Mexico

   New York

   San Francisco

6. Create the following OUs under the Asia OU:
   - **China**
   - **India**
   - **Malaysia**
   - **Vietnam**
7. Create the following OUs under the Europe OU:
   - **France**
   - **Germany**
   - **Spain**
   - **UK**
8. Create the following OUs under the South America OU:
   - **Argentina**
   - **Brazil**
   - **Chile**
   - **Peru**
9. Create the following third-level OUs under the India OU by right-clicking India within the Asia OU, and selecting New ➢ Organizational Unit:
   - **Bombay**
   - **New Delhi**
10. Within the North America ➢ Corporate OU, create the following OUs:
    - **Engineering**
    - **HR**
    - **Marketing**
    - **Research**
    - **Sales**
11. Leave the window open for the next lab.

Exercise 5.2: Modifying an OU Structure

In this exercise, you will modify the OU structure that you created in the previous lab. You should have completed the previous lab before attempting this exercise.

1. In the Active Directory Users And Computers tool, right-click the Engineering OU (located within North America ➢ Corporate) and click Delete. When you are prompted for confirmation, click Yes.

Note that if this OU contained objects, they all have been automatically deleted as well.

2. Right-click the Research OU and select Rename. Type **RD** to change the name of the OU and press Enter.
3. Right-click the Sales OU and select Move. In the Move dialog box, expand the North America branch and click the New York OU. Click OK to move the OU.
4. You will use an alternate method to move the Marketing OU. Select the Marketing OU, select Action ➢ Cut (or Ctrl+X), select the Chicago OU, and select Action ➢ Paste (or Ctrl+V). Either method moves the Marketing OU into the Chicago OU.
5. Leave the window open for the next lab.

Exercise 5.3: Creating Active Directory Objects

In this exercise, you will create various active directory objects such as users and groups. You should have completed the previous lab before attempting this exercise.

1. In the Active Directory Users And Computers tool, expand the current domain to list the objects currently contained within it. For this exercise, you will use the second- and third-level OUs contained within the North America top-level OU.
2. Right-click the Corporate OU, and select New ➢ User. Fill in the following information:

   First Name: **Monica**

   Initial: **D**

   Last Name: **President**

   Full Name: (leave as default)

   User Logon Name: **mdpresident** (leave default domain)

   Click Next to continue.
3. Enter a password for this user, then confirm it. Note that you can also make changes to password settings here. Click Next.
4. You will see a summary of the user information. Click Finish to create the new user.

5. Create another user in the RD container with the following information:

   First Name: **John**

   Initials: **Q**

   Last Name: **Admin**

   Full Name: (leave as default)

   User Logon Name: **jqadmin** (leave default domain)

   Click Next to continue.

6. Assign a password. Click Next, then click Finish to create the user.

7. Right-click the RD OU, and select New ➢ Contact. Use the following information to fill in the properties of the Contact object:

   First Name: **Jane**

   Initials: **R**

   Last Name: **Admin**

   Display Name: **jradmin**

   Click OK to create the new Contact object.

8. Right-click the RD OU, and select New ➢ Shared Folder. Enter **Software** for the name and **`\\server1\applications`** for the network path. Note that although this resource does not exist, the object can still be created. Click OK to create the Shared Folder object.

9. Right-click the HR OU, and select New ➢ Group. Type **All Users** for the group name (leave the Group Name (Pre-Windows 2000) field with the same value). For the group scope, select Global, and for the group type, select Security. To create the group, click OK.

10. Right-click the Sales OU and select New ➢ Computer. Type **Workstation1** for the name of the computer. Notice that the pre-Windows 2000 name is automatically populated and that, by default, the members of the Domain Admins group are the only ones that can add this computer to the domain. Place a check mark in the Assign This Computer Account As A Pre-Windows 2000 Computer box, then click Next. This is not a managed computer, so just click Next again to continue. Finally, click Finish to create the Computer object.

11. Leave the window open for the next lab.

Exercise 5.4: Managing Object Properties

In this exercise, you will manage object properties for some of the objects you created earlier. You must have completed the previous lab before you attempt this exercise.

1. In the Active Directory Users And Computers tool, expand the name of the domain and select the RD container. Right-click the John Q. Admin user account and select Properties.

2. On the various tabs of the John Q. Admin Properties dialog box, make some configuration changes based on your personal preferences. Click OK to continue.

3. Select the HR OU. Right-click the All Users group and click Properties. In the All Users Properties dialog box, you will be able to modify the membership of the group. Click the Members tab, then click Add. Add the Monica D. President and John Q. Admin user accounts to the group. Click OK to save the settings and OK to accept the group modifications.
4. Select the Sales OU. Right-click the Workstation1 Computer object and choose Properties. Examine the various options and make changes based on your personal preference. After you have examined the available options, click OK to continue.
5. Select the Corporate OU. Right-click the Monica D. President user account, and choose Reset Password. Enter a new password and then confirm it. Note that you can also force the user to change this password upon the next logon. Click OK.
6. Leave the window open for the next lab.

Exercise 5.5: Moving Active Directory Objects

In this exercise, you will move a computer account from one OU to another.

1. In the Active Directory Users And Computers tool, expand the name of the domain.
2. Select the Sales OU, right-click Workstation1, and select Move. A dialog box appears. Select the RD OU, and click OK to move the Computer object to that container.
3. Click the RD OU and verify that Workstation1 was moved.
4. Leave the window open for the next lab.

Exercise 5.6: Resetting an Existing Computer Account

In this exercise, you will reset a computer account and disconnect it from the domain.

1. In the Active Directory Users And Computers tool, expand the name of the domain.
2. Click the RD OU, then right-click the Workstation1 computer account.
3. Select Reset Account from the context menu. Click Yes to confirm your selection. Click OK at the success prompt.
4. When you reset the account, you break the connection between the computer and the domain, so after performing this exercise, you would need to reconnect the computer if you want it to continue working on the network.
5. Leave the window open for the next lab.

Exercise 5.7: Finding Objects in Active Directory

In this exercise, you will search for objects in the Active Directory.

1. In the Active Directory Users And Computers tool, right-click the name of the domain and select Find.
2. In the Find dialog box, select Users, Contacts, And Groups from the Find drop-down list. For the In setting, choose Entire Directory. This searches the entire Active Directory environment for the criteria you enter. Note that if this is a production domain and if there are many objects, this may be a time-consuming and network-intensive operation.
3. In the Name field, type **admin** and click Find Now to obtain the results of the search.
4. To filter the result set even further, click the View menu and select Filter. The filter is displayed in the row just above the Search Results windows. In the Name field, type **John** and press Enter. Notice that this filters the list to only the John Q. Admin User object.
5. To view more information about the User object, you can right-click it and select Properties.
6. To quickly view (and filter) more information about multiple objects, select the View menu and select Choose Columns. By selecting fields and clicking Add, you can view more information about the retrieved objects. Click OK to add the information.
7. When you have finished searching, close the Find dialog box. Leave the Active Directory Users and Computers Tool open for now. If you wish to close the tool, please make sure you save your settings, as explained in the help documentation.

Exercise 5.8: Creating and Publishing a Printer

In this exercise, you will create and publish a printer in the Active Directory.

1. Click Start ➢ Control Panel ➢ Printers And Faxes ➢ Add Printer. This starts the Add Printer Wizard. Click Next to begin.
2. In the Network Or Local Printer page, select Local Printer. Uncheck the Automatically Detect And Install My Plug And Play Printer box. Click Next.
3. In the Select The Printer Port page, select Use The Following Port. From the list beside that option, select LPT1: Printer Port. Click Next.
4. On the Install Printer Software page, select Generic for the manufacturer, and for the printer, highlight Generic/Text Only. Click Next.
5. On the Name Your Printer page, type **Text Printer**. Click Next.
6. On the Printer Sharing page, select Share Name and accept the default share name of Generic/Text Only. Click Next.
7. On the Location and Comment page, type **Building 203** and add the following comment: **This is a text-only printer.** Click Next.

8. On the Print Test Page page, click No, then click Next.
9. On the Completing The Add Printer Wizard page, you see a confirmation of the printer options you selected. Click Finish to create the printer.
10. Next, you need to verify that the printer will be listed in the Active Directory. Click Start ➢ Control Panel ➢ Printers And Faxes, then right-click the Text Printer icon and select Properties.
11. Next, select the Sharing tab, and ensure that the List In The Directory box is checked. Note that you can also add additional printer drivers for other operating systems using this tab. Click OK to accept the settings. Close the Printers and Faxes window.

Exercise 5.9: Creating and Publishing a Shared Folder

In this exercise, you will create and publish a shared folder in the Active Directory.

1. Open Windows Explorer. Expand My Computer. Right-click Local Disk (C:) and select New ➢ Folder. Name the new folder Test Share.
2. Right-click the Test Share folder and select Sharing And Security.
3. On the Sharing tab, select Share This Folder. For the share name, type **Test Share**, and for the description, enter **Share used for testing the Active Directory**. Leave the User Limit, Permissions, and Caching settings as their defaults. Click OK to create the share.
4. To verify that the share has been created, choose Start ➢ Run and type the UNC path for the local server. For instance, if the server is named sybex1, you would type **\\sybex1**. This connects you to the local computer, where you can view any available network resources. Verify that the Test Share folder exists, then close the window.
5. Open the Active Directory Users And Computers tool. Expand the current domain and right-click the RD OU. Select New ➢ Shared Folder.
6. In the New Shared Folder dialog box, type **Shared Folder Test** for the name of the folder. Then type the UNC path to the share (for example, **\\sybex1\Test Share**). Click OK to create the share. Leave the Active Directory Users and Computers Tool open for now. If you wish to close the tool, please make sure you save your settings, as explained in the help documentation.

Planning Security for Active Directory

In this section, you will plan and manage security in the Active Directory using techniques such as configuring security-related GPO options and preparing for smart card authentication.

This section corresponds to Chapter 6, "Planning Security for Active Directory," in the *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 6.1: Creating and Managing Users and Groups
- Exercise 6.2: Creating and Using User Templates
- Exercise 6.3: Delegating Control of Active Directory Objects
- Exercise 6.4: Applying Security Policies by Using Group Policy
- Exercise 6.5: Preparing a Smart Card Certificate Enrollment Station
- Exercise 6.6: Setting Up a Smart Card for User Logon
- Exercise 6.7: Configuring Group Policy to Require Smart Card Logon
- Exercise 6.8: Using the Security Configuration And Analysis Utility
- Exercise 6.9: Enabling Auditing of Active Directory Objects
- Exercise 6.10: Enabling Auditing for a Specific OU
- Exercise 6.11: Generating and Viewing Audit Logs

Exercise 6.1: Creating and Managing Users and Groups

In this exercise, you learn how to create and manage users and groups.

1. If it's not already open, open the Active Directory Users And Computers tool.
2. Create the following top-level OUs:
   - Sales
   - Marketing
   - Engineering
   - HR
3. Create the following User objects within the Sales container (use the defaults for all fields not listed):

   First Name: **John**

   Last Name: **Sales**

   User Logon Name: **JSales**

   First Name: **Linda**

   Last Name: **Manager**

   User Logon Name: **LManager**

4. Create the following User objects within the Marketing container (use the defaults for all fields not listed):

   First Name: **Jane**

   Last Name: **Marketing**

   User Logon Name: **JMarketing**

   First Name: **Monica**

   Last Name: **Manager**

   User Logon Name: **MManager**

5. Create the following User object within the Engineering container (use the defaults for all fields not listed):

   First Name: **Bob**

   Last Name: **Engineer**

   User Logon Name: **BEngineer**

6. Right-click the HR container and select New ➢ Group. Use the name **Managers** for the group, and specify Global for the group scope and Security for the group type. Click OK to create the group.

7. To assign users to the Managers group, right-click the Group object and select Properties. Change to the Members tab and click Add. Enter Linda Manager and Monica Manager, then click OK. You will see the group membership list. Click OK to finish adding the users to the group.

8. Leave the window open for the next lab.

Exercise 6.2: Creating and Using User Templates

In this exercise, you create a user template, make configuration changes, and create a new user based on the template. This exercise shows you that the new user you create will belong to the same group as the user template that you copied it from. You should have completed the previous exercise before you begin this one.

1. In the Active Directory Users And Computers tool, create the following User object within the Sales container (use the defaults for all fields not listed):

   First Name: **Sales User**

   Last Name: **Template**

   User Logon Name: **SalesUserTemplate**

2. Create a new global security group called **Sales Users** and add SalesUserTemplate to the group membership.

3. Right-click the SalesUserTemplate user object and select Copy from the context menu.

4. Enter the username, first name, and last name for the new "real" user. Click the Next button to move on to the password screen and enter the new user's password information. Close the Copy Object–User dialog box when you're done.
5. Right-click the user you created in step 4, select Properties, and click the Member Of tab.
6. Verify that the new user is a member of the Sales Users group and click OK.
7. Leave the window open for the next lab.

Exercise 6.3: Delegating Control of Active Directory Objects

This exercise walks you through the steps required to delegate control of OUs. In order to complete the steps in this exercise, you must have already completed Exercise 6.1.

1. In the Active Directory Users And Computers tool, create a new user within the Engineering OU, using the following information (use the default settings for any fields not specified):

   First Name: **Robert**

   Last Name: **Admin**

   User Logon Name: **radmin**
2. Right-click the Sales OU and select Delegate Control. This starts the Delegation of Control Wizard. Click Next.
3. To add users and groups to which you want to delegate control, click the Add button. In the Add dialog box, enter **Robert Admin** for the name of the user to add. Note that you could specify multiple users or groups using this option. Click OK to add the account to the delegation list, which is shown in the Users Or Groups page. Click Next to continue.
4. On the Tasks To Delegate page, you must specify which actions you want to allow the selected user to perform within this OU. Select Delegate The Following Common Tasks and place a check mark next to the following options:

   Create, Delete, And Manage User Accounts

   Reset User Passwords And Force Password Change At Next Logon

   Read All User Information

   Create, Delete, And Manage Groups

   Modify The Membership Of A Group
5. Click Next to continue. The wizard provides you with a summary of the selections that you have made on the Completing The Delegation Of Control Wizard page. To complete the process, click Finish to have the wizard commit the changes.

   Now when the user Robert Admin logs on (using "radmin" as his logon name), he will be able to perform common administrative functions for all of the objects contained within the Sales OU.
6. Leave the window open for the next lab.

Exercise 6.4: Applying Security Policies by Using Group Policy

This exercise walks you through the steps required to create a basic Group Policy for the purpose of enforcing security settings. In order to complete the steps of this exercise, you must have already completed Exercise 6.1.

1. In the Active Directory Users And Computers tool, right-click the domain name and select Properties.
2. Change to the Group Policy tab and select the Default Domain Policy.
3. To specify the Group Policy settings, click Edit.
4. In the Group Policy window, expand Computer Configuration, Windows Settings, Security Settings, Account Policies, Password Policy object.
5. In the right pane, double-click the Minimum Password Length setting.
6. In the Security Policy Setting dialog box, place a check mark next to the Define This Policy Setting option. Decrease the value to 7 characters. Click OK to return to the Group Policy Object Editor window.
7. Open User Configuration, Administrative Templates, Control Panel object. Double-click Prohibit Access To The Control Panel, select Enabled, then click OK.
8. Close the Group Policy window to save the settings you chose. Click OK to enable the Security Group Policy.
9. To view the security permissions for a Group Policy object, right-click the domain name and select Properties. On the Group Policy tab, highlight the Default Domain Policy Group Policy object and select Properties.
10. Select the Security tab of Default Domain Policy Properties dialog box. Click Add and enter **Linda Manager**. Click OK to add this account to the list of users and groups that will be affected by these Group Policy settings. This takes you back to the Default Domain Policy Properties dialog box. Highlight Linda Manager and allow this user the Read and Write permissions.
11. Click OK twice to save the changes. Linda Manager will now be able to view and change information for objects in the Sales OU.
12. You will not need to use Active Directory Users And Computers until a little later on, but leave the window open anyway so that you do not lose your work. If you want to close the tool now, be sure to save your settings.

Exercise 6.5: Preparing a Smart Card Certificate Enrollment Station

This exercise walks you through the process of configuring a smart card enrollment station.

1. Open an MMC console by selecting Start ➢ Run and entering **mmc** in the Run dialog box.

2. Add the Certificates snap-in by selecting File ➢ Add/Remove Snap-In. Click Add in the Add Standalone Snap-In dialog box. Select the Certificates snap-in and click the Add button. Click Close and click OK to return to the MMC and display the newly added snap-in.
3. Double-click the Certificates–Current User node in the MMC window.
4. Right-click the Personal node and select All Tasks ➢ Request New Certificate.
5. In the Certificate Request wizard, select the Enrollment Agent certificate template. Enter a name and description for the template. When prompted, click Install Certificate. Close the lab window.

Exercise 6.6: Setting Up a Smart Card for User Logon

Follow the steps in this exercise to enroll a smart card for user logon. Note that you must complete Exercise 6.5 before continuing. In addition, you must have a smart card reader and at least one blank smart card available.

1. Open Internet Explorer by selecting Start ➢ Internet Explorer.
2. In the Address field, enter the address of the CA that issues smart card certificates and press Enter.
3. In the IE window, click Request A Certificate, then click Advanced Certificate Request.
4. Click Request A Certificate For A Smart Card On Behalf Of Another User Using The Smart Card Certificate Enrollment Station. If prompted, click Yes to accept the smart card signing certificate.
5. Click Smart Card Logon on the Smart Card Certificate Enrollment Station web page.
6. Under Certification Authority, select the CA you want to issue the smart card certificate.
7. Under Cryptographic Service Provider, select the cryptographic service provider of the smart card's manufacturer.
8. Under Administrator Signing Certificate, click the Enrollment Agent certificate from the previous exercise.
9. Under User To Enroll, click Select User. Select the user to enroll and click Enroll.
10. When prompted, insert the smart card into the smart card reader and click OK. When prompted, enter a new PIN for the smart card. Close the lab window.

Exercise 6.7: Configuring Group Policy to Require Smart Card Logon

This exercise shows you how to configure group policy to require smart card authentication.

1. The Active Directory Users And Computers Utility should still be open from Exercise 6.4. Return to it now.

2. Create a new top-level OU called Smart Card Test.
3. Right-click the Smart Card Test OU and select Properties.
4. In the Smart Card Test Properties dialog box, switch to the Group Policy tab and click Add. Click OK to accept the default GPO name, then click the Edit button.
5. In the Group Policy Object Editor window, expand Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options.
6. Double-click the Interactive Logon: Require Smart Card policy.
7. In the Interactive Logon: Require Smart Card dialog box, first select Define This Policy Setting, then select Enabled and click OK.
8. You will not need to use Active Directory Users And Computers until a little later on, but leave the window open anyway so that you do not lose your work. If you want to close the tool now, be sure to save your settings.

Exercise 6.8: Using the Security Configuration And Analysis Utility

This exercise walks you through the steps you need to take to use the Security Configuration And Analysis utility. In this exercise, you will use this utility to create and modify security configurations.

1. Click Start ➢ Run, type **mmc**, and press Enter. This opens a blank MMC.
2. In the File menu, select Add/Remove Snap-In. Click Add. In the Add Standalone Snap-In dialog box, select the Security Configuration And Analysis item, then click Add, then click Close.
3. You will see that the Security Configuration And Analysis snap-in has been added to the configuration. Click OK to continue.
4. Within the MMC, right-click Security Configuration And Analysis and select Open Database. This displays a standard file selection (Open) dialog box. Change to a local directory on your computer and create a new security database file named `SecurityTest.sdb`. Note the location of this file because you'll need it in later steps. Click Open.
5. You'll be prompted to open a Security Template file. By default, these files are stored within the `Security\Templates` directory of your Windows system root. On the Import Database dialog box, select `DC security.inf`, and place a check mark in the Clear This Database Before Importing box. Click Open to load the Security Template file.
6. Now that you have created a security database file and opened a template, you can start performing useful security tasks. Within the Security Configuration And Analysis utility, you have access to several tasks.
7. To analyze the security configuration of the local computer, right-click the Security Configuration And Analysis utility and select Analyze Computer Now.

8. When prompted, enter the path to a local directory with the filename `securityTest.log`. Click OK to begin the analysis process.
9. When the process has been completed, you can view the current security settings for the local computer. Navigate through the various items to view the current security configuration.
10. To make changes to this template, expand the Password Policy object under Account Policies. Double-click the Enforce Password History item. On the Enforce Password History Properties dialog box, place a check mark next to the Define This Policy In The Database option and type **2** for Passwords Remembered.
11. Click OK to make the setting change. Note that this change in setting was not enabled for the local computer—the change was implemented only within the security database file.
12. To save the changes to the security database file, right-click the Security Configuration And Analysis object and select Save.
13. To export the current settings to a template file, right-click the Security Configuration And Analysis object and select Export Template. You are prompted for the location and filename to which these settings should be saved. Be sure to choose a meaningful name so that other systems administrators will understand the purpose of this template.
14. The configuration change we made has not yet been applied to any machines. To apply the change to the local computer, right-click the Security Configuration And Analysis object and select Configure Computer Now. You are prompted to enter the path for a Log file. Enter any path on the local computer and specify `SecurityTest2.log` as the filename. Click OK.
15. To quickly view the contents of the Log file for the most recent operation, right-click the Security Configuration And Analysis object and select View Log.
16. When you are finished, exit the Security Configuration And Analysis tool by closing the MMC.

Exercise 6.9: Enabling Auditing of Active Directory Objects

This exercise walks you through the steps you must take to implement auditing of Active Directory objects on domain controllers. In order to complete the steps in this exercise, you must have already completed Exercise 6.1.

1. Open the Domain Controller Security Policy tool (located in the Administrative tools program group).
2. Expand Security Settings, Local Policies, Audit Policy.
3. Double-click the Audit Directory Service Access policy.
4. In the Audit Directory Service Access Properties dialog box, place a check mark next to the option for Define These Policy Settings, and check marks at Success and Failure. Click OK to save the settings.

5. Expand Security Settings, Event Log to see the options associated with the event logs.
6. Double-click the Maximum Security Log Size item in the right pane of the Domain Controller Security Policy tool, and set the value to 2048KB in the Maximum Security Log Size dialog box. Click OK.
7. In the right pane of the Domain Controller Security utility, double-click the Retain Security Log item and specify that events should be overwritten after seven days in the Retain Security Log dialog box. Click OK. You will be notified that the Retention Method For Security Log option will also be changed. Click OK to accept the changes.
8. When you are finished enabling auditing options, close the Domain Controller Security Policy tool.

Exercise 6.10: Enabling Auditing for a Specific OU

Once you have enabled auditing of Active Directory objects, it's time to specify exactly which actions and objects should be audited. This exercise walks you through the steps required to enable auditing for a specific OU. In order to complete the steps in this exercise, you must have already completed Exercise 6.1 and Exercise 6.9.

1. The Active Directory Users And Computers tool should still be open from Exercise 6.7. Return to it now.
2. To enable auditing for a specific object, right-click the Engineering OU and select Properties. Select the Group Policy tab on the Engineer Properties dialog box.
3. Highlight the Engineering Security Policy object, if present, and select Properties.
4. Select the Security tab on the GPO Properties dialog box, then click Advanced. Select the Auditing tab. You will see the current auditing settings for this Group Policy object.
5. Click the Edit button. Notice that you can view and change auditing settings based on the objects and/or properties. To retain the current settings, click OK.
6. To exit the configuration for the Engineering object, click OK three more times.
7. Leave the window open for the next lab.

Exercise 6.11: Generating and Viewing Audit Logs

This exercise walks you through the steps you must take to generate some auditing events and to examine the data collected for these actions. In this exercise, you will perform some actions that will be audited, and then you will view the information recorded within the audit logs. In order to complete this exercise, you must have already completed the steps in Exercise 6.1 and Exercise 6.10.

1. In the Active Directory Users And Computers tool, navigate to the Engineering OU, right-click the Bob Engineer User account, and select Properties.
2. On the Bob Properties dialog box, add the middle initial A for this user account and specify Software Developer in the Description box. Click OK to save the changes.
3. Within the Engineering OU, right-click the Robert Admin User account and select Properties.
4. On the Bob Properties dialog box, add a description of Engineering IT Admin, and click OK.
5. Close the Active Directory Users And Computers tool.
6. Open the Event Viewer tool from the Administrative Tools program group. Select the Security item. You will see a list of audited events categorized under Directory Service Access. Note that you can obtain more details about a specific item by double-clicking it.
7. When you are finished viewing the security log, close the Event Viewer tool.

Planning, Implementing, and Managing Group Policy

In this section, you will use Group Policy to make configuration changes that affect Active Directory users and computers.

This section corresponds to Chapter 8, "Planning, Implementing, and Managing Group Policy," in the *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 8.1: Creating a Group Policy Object Using MMC
- Exercise 8.2: Linking GPOs to the Active Directory
- Exercise 8.3: Filtering Group Policy Using Security Groups
- Exercise 8.4: Delegating Administrative Control of Group Policy
- Exercise 8.5: Managing Inheritance and Filtering of GPOs
- Exercise 8.6: Configuring Automatic Certificate Enrollment in Group Policy
- Exercise 8.7: Configuring Folder Redirection in Group Policy
- Exercise 8.8: Running RSoP in Logging Mode
- Exercise 8.9: Running RSoP in Planning Mode

Exercise 8.1: Creating a Group Policy Object Using MMC

This exercise walks you through the process of creating a custom MMC snap-in for editing Group Policy settings.

1. Click Start ➢ Run, type **mmc**, and press Enter.
2. On the File menu, click Add/Remove Snap-In.
3. Click the Add button. In the Add Standalone Snap-In dialog box, select Group Policy Object Editor from the list and click Add.
4. In the Select Group Policy Object Wizard, click Browse (note that you can set the scope to Domains/OUs, Sites, or Computers).
5. On the Domains/OUs tab, click the New Policy button (located to the right of the Look In drop-down list).
6. To name the new object, type Test Domain Policy. Click OK to select the Policy object.
7. Place a check mark next to the Allow The Focus Of The Group Policy Snap-In To Be Changed When Launching From The Command Line option. This will allow the context of the snap-in to be changed when you launch the MMC item.
8. Click Finish to create the Group Policy object. Click Close in the Add Standalone Snap-In dialog box. Finally, click OK in the Add/Remove Snap-In dialog box to add the new snap-in.
9. Next, we'll make some changes to the default settings for this new GPO. Expand the following items: Test Domain Policy, Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options.
10. Double-click the Interactive Logon: Do Not Display Last User Name option.
11. On the Template Security Policy Setting dialog box, place a check mark next to the Define This Policy Setting In The Template option, then select Enabled. Click OK to save the setting.
12. In the Group Policy Object Editor, double-click the Interactive Logon: Message Text For Users Attempting To Log On option.
13. Place a check mark next to the Define This Policy Setting In The Template option, and then type the following: **By logging onto this domain, you specify that you agree to the usage policies as defined by the IT department.** Click OK to save the setting.
14. In the Group Policy Object Editor, double-click the Interactive Logon: Message Title For Users Attempting To Log On option.
15. Place a check mark next to the Define This Policy Setting In The Template option, then type **Test Policy Logon Message.** Click OK to save the setting.
16. To make changes to the user settings, expand the following objects in the Group Policy Object Editor: Test Domain Policy, User Configuration, Administrative Templates, Start Menu & Task Bar.

17. Double-click the Add Logoff To The Start Menu option. Note that you can get a description of the purpose of this setting by clicking the Explain tab. You can also see this description in the right pane of the MMC when the policy is selected. Select Enabled, then click OK.
18. On the Group Policy Object Editor, expand the following objects: Test Domain Policy, User Configuration, Administrative Templates, System.
19. Double-click the Don't Run Specified Windows Applications option.
20. In the Don't Run Specified Windows Applications Properties dialog box, select Enabled, then click the Show button. To add to the list of disallowed applications, click the Add button. When prompted to enter the item, type **wordpad.exe**. To save the setting, click OK three times.
21. To change network configuration settings, click Test Domain Policy, User Configuration, Administrative Templates, Network, Offline Files. Note that you can change the default file locations for several different network folders.
22. To change script settings, click Test Domain Policy ➢ Computer Configuration ➢ Windows Settings ➢ Scripts (Startup/Shutdown). Note that you can add script settings by double-clicking either the Startup or the Shutdown item.
23. The changes you have made for this GPO are automatically saved. You can optionally save this customized MMC console by selecting Save As from the Console menu. Then provide a name for the new MMC snap-in (such as **Group Policy Test**). You will now see this item in the Administrative Tools program group.
24. When you are finished modifying the Group Policy settings, close the MMC tool.

Exercise 8.2: Linking GPOs to the Active Directory

This exercise walks you through the steps you must take to assign a GPO to an OU within the local domain. In this exercise, you will link the Test Domain Policy GPO to an OU. In order to complete the steps in this exercise, you must have first completed Exercise 8.1.

1. Open the Active Directory Users And Computers tool.
2. Create a new top-level OU called **Group Policy Test**.
3. Right-click the Group Policy Test OU and click Properties.
4. On the Group Policy Test Properties dialog box, select the Group Policy tab. To add a new policy at the OU level, click New.
5. Enter a descriptive name for the GPO, such as Group Policy Test GPO. Note that you can also add additional GPOs to this OU. When multiple GPOs are assigned, you can also control the order in which they apply by using the Up and Down buttons. Finally, you can edit the GPO by clicking the Edit button, and you can remove the link (or, optionally, delete the GPO entirely) by clicking the Delete button.
6. To save the GPO link, click OK in the OU Properties dialog box.
7. Leave the Active Directory Users And Computers tool open for the next lab.

Exercise 8.3: Filtering Group Policy Using Security Groups

In this exercise, you will filter Group Policy using security groups. In order to complete the steps in this exercise, you must have first completed Exercises 8.1 and 8.2.

1. In the Active Directory Users And Computers tool, create two new Global Security groups within the Group Policy Test OU and name them **PolicyEnabled** and **PolicyDisabled**.
2. Right-click the Group Policy Test OU and select Properties. Select the Group Policy tab.
3. Highlight Test Domain Policy and click the Properties button.
4. On the Security tab of the GPO Properties dialog box, click Add and enter the PolicyEnabled and the PolicyDisabled groups. Click OK.
5. Highlight the PolicyDisabled group and select Deny for the Read and Apply Group Policy permissions. This prevents users in the PolicyDisabled group from being affected by this policy.
6. Highlight the PolicyEnabled group and select Allow for the Read and Apply Group Policy permissions. This ensures that users in the PolicyEnabled group will be affected by this policy.
7. Click OK to save the Group Policy settings. You will be warned that Deny takes precedence over any other security settings. Select Yes to continue.
8. Click OK to save the change to the properties of the OU.
9. Leave the Active Directory Users And Computers tool open for the next lab.

Exercise 8.4: Delegating Administrative Control of Group Policy

This exercise walks you through the steps you must take to grant the appropriate permissions to a User account. Specifically, the process involves delegating the ability to manage Group Policy links on an Active Directory object (such as an OU). In order to complete this exercise, you must have first completed Exercises 8.1 and 8.2.

1. In the Active Directory Users And Computers tool, expand the local domain and create a user named **Policy Admin** within the Group Policy Test OU.
2. Right-click the Group Policy Test OU and select Delegate Control.
3. Click Next to start the Delegation Of Control Wizard.
4. On the Users Or Groups page, click Add. Enter the Policy Admin account and click OK. Click Next to continue.
5. On the Tasks To Delegate page, select Delegate The Following Common Tasks and place a check mark next to the Manage Group Policy Links item. Click Next to continue.

6. Finally, click Finish on the final page of the wizard to complete the Delegation Of Control Wizard and assign the appropriate permissions. Specifically, this will allow the Policy Admin user to create GPO links to this OU (and, by default, any child OUs).
7. Leave the window open for the next lab.

Exercise 8.5: Managing Inheritance and Filtering of GPOs

This exercise walks you through the steps you need to take to manage inheritance and filtering of GPOs.

1. In the Active Directory Users And Computers tool, create a top-level OU called **Parent**.
2. Right-click the Parent OU and select Properties. Select the Group Policy tab and click the New button to create a new GPO. Name the new object **Master GPO**.
3. Click the Options button on the Group Policy tab.
4. On the Master GPO Options dialog box, place a check mark next to the No Override option. This ensures that administrators of OUs contained within the Parent OU will not be able to override the settings defined in this GPO. To save the settings, click OK. Notice that a check mark appears next to the Master GPO in the No Override column in the list of Group Policy object links.
5. On the Group Policy tab of the Parent OU Properties dialog box, create another GPO and name it **Optional GPO**. Click the OK button to save the changes.
6. Within the Parent OU, create another OU called **Child**.
7. Right-click the Child OU and select Properties.
8. Select the Group Policy tab, and place a check mark in the Block Policy Inheritance checkbox. This option prevents the inheritance of GPO settings from the Parent OU for the Optional GPO settings. Note that since the No Override setting for the Master GPO was enabled on the Parent OU, the settings in the Master GPO will take effect on the Child OU regardless of the setting of the Block Policy Inheritance box. Click OK to save the changes.
9. Leave the window open for the next lab.

Exercise 8.6: Configuring Automatic Certificate Enrollment in Group Policy

In this exercise, you will learn how to configure automatic certificate enrollment in Group Policy. You must have completed the other exercises in this section in order to proceed with this exercise.

1. In the Active Directory Users And Computers tool, open the Master GPO by taking the following steps: right-click the Parent OU, select Properties, select the Group Policy tab, select Master GPO, and click the Edit button.
2. Expand Computer Configuration, Windows Settings, Security Settings, Public Key Policies.
3. Double-click Autoenrollment Settings in the right pane.
4. The Autoenrollment Settings Properties dialog box will appear. Notice that the Enroll Certificates Automatically setting is enabled by default. Check the Renew Expired Certificates, Update Pending Certificates, Remove Revoked Certificates and the Update Certificates That User Certificate Templates checkboxes.
5. Click OK to close the Autoenrollment Settings Properties dialog box.
6. Leave the window open for the next lab.

Exercise 8.7: Configuring Folder Redirection in Group Policy

To configure folder redirection, follow the steps in this exercise. You must have completed the other exercises in this chapter in order to proceed with this exercise.

1. In the Active Directory Users And Computers tool, open the Parent OU that you created in the previous exercises and open the Master GPO. Click Edit to open the GPO in the GPO editor.
2. Open User Configuration, Windows Settings, Folder Redirection, My Documents.
3. Right-click My Documents and select Properties.
4. On the Target tab of the My Documents Properties dialog box, choose the Basic–Redirect Everyone's Folder To The Same Location selection from the Setting drop-down list.
5. Leave the default option for the Target Folder Location drop-down list and specify a network path in the Root Path field.
6. Click the Settings tab. All of the default settings are self-explanatory and should typically be left on the default. Click OK when you are done.
7. Leave the window open for the next lab.

Exercise 8.8: Running RSoP in Logging Mode

In this exercise, you'll learn how to run RSoP in Logging mode. Note that you must have completed the previous exercises in this chapter to complete this exercise.

1. In the Active Directory Users And Computers tool, open the Parent OU you created in the previous exercises. Make several changes to the Desktop policies in the Optional GPO and the Master GPO. Be sure to refresh the GPO settings with the `gpupdate` command.

2. Open the Child OU and add a user named **TestUser1**.
3. Log on to the network as TestUser1 to establish an RSoP log, then log off and log on as an administrator.
4. Open the Active Directory Users And Computers administrative tool.
5. Right-click the TestUser1 account and select All Tasks ➢ Resultant Set Of Policy (Logging) to open the Resultant Set Of Policy Wizard.
6. On the Computer Selection page, select the computer that TestUser1 used to log on to the network in step 3. Click Next.
7. TestUser1 should already be selected on the User Selection page, so click Next to continue.
8. Verify that the information on the Summary Of Selections page is correct and click Next.
9. Click the Finish button on the Completing The Resultant Set Of Policy Wizard page to open the Resultant Set Of Policy window.
10. Check some of the Desktop settings that you changed in step 1. Right-click a setting and select Properties from the pop-up menu. You should see the resultant policy on the Settings tab and the order of precedence on the Precedence tab.
11. Leave the window open for the next lab.

Exercise 8.9: Running RSoP in Planning Mode

This exercise shows you how to run RSoP in Planning mode. Note that you must have completed the previous exercises in this chapter to continue.

1. In the Active Directory Users And Computers tool, open the Parent OU you created in the previous exercises.
2. Right-click the Parent OU and select All Tasks ➢ Resultant Set Of Policy (Planning) to open the Resultant Set Of Policy Wizard.
3. On the User And Computer Selection page, the Parent OU information should be filled in for you for both the user and computer. You could make changes to this screen if desired—for example, if you wanted to view the RSoP for users in one OU who log on to computers in another OU. Click Next to continue.
4. On the Advanced Simulation Options page, don't make any changes at this time. This screen is used to simulate special network conditions such as slow network connections or loopback processing. Click Next to continue.
5. On the User Security Groups page, select hypothetical security groups that you would place users into under the planned scenario. Click Next to continue.
6. On the Computer Security Groups page, select hypothetical security groups that you would place computers into under the planned scenario. Click Next to continue.

7. On the WMI Filters For Users page, you can specify any Windows Management Instrumentation filters that you may have applied to GPOs. WMI filters go beyond the scope of this book, so just click Next and leave the default settings.
8. On the WMI Filters For Computers page, click Next and leave the default settings.
9. The Summary Of Selections page appears. This displays a summary of the selections you made in the wizard. You can elect to gather extended error information, and you can choose a domain controller on which to run the simulated RSoP. Click Next when you are ready to run the simulation.
10. Click Finish on the Completing The Resultant Set Of Policy Wizard page to open the Resultant Set Of Policy window.
11. Click through the various policy settings in the Resultant Set Of Policy window to see the GPO settings for a user and computer stored in the Parent OU. Close the RSOP window.

Software Deployment through Group Policy

In this section, you will manage software deployment in Group Policy. This makes it easy to distribute new software and software updates to users and computers in the Active Directory.

This section corresponds to Chapter 9, "Software Deployment through Group Policy," in the *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide*.

You will perform the following labs:

- Exercise 9.1: Creating a Software Deployment Share
- Exercise 9.2: Publishing and Assigning Applications Using Group Policy
- Exercise 9.3: Configuring Software Update Services in Group Policy

Exercise 9.1: Creating a Software Deployment Share

This exercise walks you through the process of creating a software distribution share point. In this exercise, you will prepare for software deployment by creating a directory share and placing certain types of files in this directory.

1. Using Windows Explorer, create a folder called **Software** that you can use with application sharing.
2. Within the Software folder, create a folder called **Office2003**.

3. Right-click the Software folder (created in step 1), and select Sharing And Security. In the folder properties dialog box, choose Share This Folder, and type **Software** in the Share Name text box and **Software Distribution Share Point** in the Description text box. Leave all other options as the default, and click OK to create the share.
4. At this point, you would copy all of the Office 2003 installation files to the Office 2003 folder. For purposes of this simulator, the next exercise assumes that you have completed this step.

Exercise 9.2: Publishing and Assigning Applications Using Group Policy

This exercise walks you through the steps you need to take to publish and assign applications. In this exercise, you will create and assign applications to specific Active Directory objects using Group Policy objects. In order to complete the steps in this exercise, you must have first completed Exercise 9.1.

1. Open the Active Directory Users And Computers tool from the Administrative Tools program group.
2. Expand the domain and create a new top-level OU called **Software**.
3. Within the Software OU, create a user named **Jane User** with a login name of **juser** (choose the defaults for all other options).
4. Right-click the Software OU and select Properties.
5. On the Software Properties dialog box, select the Group Policy tab and click New.
6. For the name of the new GPO, type **Software Deployment**.
7. To edit the Software Deployment GPO, click Edit. Expand the Computer Configuration ➢ Software Settings object.
8. Right-click the Software Installation item and select New ➢ Package.
9. The simulator automatically opens to the Office2003 folder that you created in Exercise 9.1.
10. Select the appropriate MSI file depending on the version of Office2003 that you have. Office XP Professional is being used in this example, so you'll see that the PRO11.MSI file is chosen. Click Open.
11. In the Deploy Software dialog box, choose Advanced. Click OK to return to the Deploy Software dialog box.
12. To examine the deployment options of this package, click the Deployment tab. Accept the default settings by clicking OK.
13. Within the Group Policy Object Editor, expand the User Configuration ➢ Software Settings object.
14. Right-click the Software Installation item and select New ➢ Package.
15. The simulator automatically opens to the Office2003 folder that you created in Exercise 9.1.
16. You'll see that the PRO11.MSI file is chosen. Click Open.

17. For the Software Deployment option, select Published in the Deploy Software dialog box and click OK. Click OK to close the Microsoft Office Pro Edition 2003 Properties window. Close the GPO Editor to return to Active Directory Users and Computers. Leave the window open for the next lab.

Exercise 9.3: Configuring Software Update Services in Group Policy

In this exercise, you learn how to configure Software Update Services in Group Policy on a Windows Server 2003 domain controller.

1. In the Active Directory Users And Computers tool, right-click the domain and select Properties.
2. Click the Group Policy tab on the domain Properties dialog box and select the Default Domain Policy. Click the Edit button.
3. Expand Default Domain Policy, Computer Configuration, Administrative Templates, Windows Components, Windows Update to access the Windows Update settings.
4. Double-click the Configure Automatic Updates option.
5. The Configure Automatic Updates Properties dialog box appears. On the Settings tab, you can configure whether automatic updates are not configured, enabled, or disabled. If automatic updates are enabled, you can select Notify For Download And Notify For Install, Auto Download And Notify For Install, or Auto Download And Schedule The Install. You can also specify the schedule that will be applied for the install day and the install time.
6. To configure which server will provide automatic updates, click the Next Setting button in the Configure Automatic Updates Properties dialog box. This brings up the Specify Intranet Microsoft Update Service Location Properties dialog box. You can configure the status of the intranet Microsoft update service location as Not Configured, Enabled, or Disabled; you can also configure the HTTP name of the server that will provide intranet service updates and the HTTP name of the server that will act as the intranet SUS statistics server.
7. To configure rescheduling of automatic updates, click the Next Setting button in the Specify Intranet Microsoft Update Service Location Properties dialog box. This brings up the Reschedule Automatic Updates Scheduled Installations Properties dialog box. You can enable and schedule the amount of time that Automatic Updates waits after system startup before it attempts to proceed with a scheduled installation that was previously missed.
8. To configure auto-restart for scheduled automatic updates installations, click the Next Setting button in the Reschedule Automatic Updates Scheduled Installations Properties dialog box. This brings up the No Auto-Restart For Scheduled Automatic Updates Installations dialog box. You use this option if the computer needs to restart after an update. You can choose to wait until the next time the computer is restarted or to restart the computer automatically as a part of the update.
9. When you are done making setting changes, click the OK button.