Introduction

Welcome to the 70-642 Exam Cram! Whether this book is your first or your 15th Exam Cram series book, you’ll find information here that will help ensure your success as you pursue knowledge, experience, and certification. This book aims to help you get ready to take and pass the Microsoft certification exam “TS: Windows Server 2008 Network Infrastructure, Configuring” (Exam 70-642). After you pass this exam, you will earn the Microsoft Certified Technology Specialist: Windows Server 2008 Applications certification.

This introduction explains Microsoft’s certification programs in general and talks about how the Exam Cram series can help you prepare for Microsoft’s latest certification exams. Chapters 1 through 9 are designed to remind you of everything you’ll need to know to pass the 70-642 certification exam. The two sample tests at the end of the book should give you a reasonably accurate assessment of your knowledge and, yes, we’ve provided the answers and their explanations for these sample tests. Read the book, understand the material, and you’ll stand a very good chance of passing the real test.

Exam Cram books help you understand and appreciate the subjects and materials you need to know to pass Microsoft certification exams. Exam Cram books are aimed strictly at test preparation and review. They do not teach you everything you need to know about a subject. Instead, the author streamlines and highlights the pertinent information by presenting and dissecting the questions and problems he’s discovered that you’re likely to encounter on a Microsoft test.

Nevertheless, to completely prepare yourself for any Microsoft test, we recommend that you begin by taking the Self-Assessment that is included in this book, immediately following this introduction. The self-assessment tool helps you evaluate your knowledge base against the requirements for becoming a Microsoft Certified Technology Specialist (MCTS) and will be the first step in earning more advanced certifications, including Microsoft’s IT Professional and Professional Developer (MCITP and MCPD) and Architect (MCA).

Based on what you learn from the self-assessment, you might decide to begin your studies with classroom training or some background reading. On the other hand, you might decide to pick up and read one of the many study guides available from Microsoft or third-party vendors. We also recommend that you supplement your study program with visits to http://www.examcram.com to receive additional practice questions, get advice, and track the Windows certification programs.
This book also offers you an added bonus of access to Exam Cram practice tests online. This software simulates the Microsoft testing environment with similar types of questions to those you’re likely to see on the actual Microsoft exam. We also strongly recommend that you install, configure, and play around with the Microsoft Windows Vista and Windows Server 2008 operating systems. Nothing beats hands-on experience and familiarity when it comes to understanding the questions you’re likely to encounter on a certification test. Book learning is essential, but without a doubt, hands-on experience is the best teacher of all!

The Microsoft Certification Program

Microsoft currently offers multiple certification titles, each of which boasts its own special abbreviation. (As a certification candidate and computer professional, you need to have a high tolerance for acronyms.)

The certification for end users is

- **Microsoft Office Specialists**: For professionals recognized for demonstrating advanced skills with Microsoft desktop software (including Microsoft Office).

The older certifications associated with the Windows Server 2003 operating system and related network infrastructure are

- **Microsoft Certified Professional (MCP)**: For professionals who have the skills to successfully implement Microsoft products (such as Windows XP or Windows Server 2003) or technology as part of a business solution in an organization.

- **Microsoft Certified Desktop Support Technician (MCDST)**: For professionals who have the technical and customer service skills to troubleshoot hardware and software operation issues in Microsoft Windows environments.

- **Microsoft Certified Systems Administrators (MCSAs)**: For professionals who administer network and systems environments based on the Microsoft Windows operating systems. Specializations include MCSA: Messaging and MCSA: Security.

- **Microsoft Certified Systems Engineer (MCSE)**: For professionals who design and implement an infrastructure solution that is based on the Windows operating system and Microsoft Windows Server System software. Specializations include MCSE: Messaging and MCSE: Security.
The newer certifications based on Windows Vista, Windows Server 2008, and related server products are

- **Microsoft Certified Technology Specialist (MCTS):** For professionals who target specific technologies and distinguish themselves by demonstrating in-depth knowledge and expertise in the various Microsoft specialized technologies. The MCTS is a replacement for the MCP program.

- **Microsoft Certified IT Professional (MCITP):** For professionals who demonstrate comprehensive skills in planning, deploying, supporting, maintaining, and optimizing IT infrastructures. The MCITP is a replacement for the MCSA and MCSE programs.

- **Microsoft Certified Architect (MCA):** For professionals who are identified as top industry experts in IT architecture and who use multiple technologies to solve business problems and provide business metrics and measurements. Candidates for the MCA program are required to present to a review board—consisting of previously certified architects—to earn the certification.

For those who want to become or who are database professionals, the following certifications are based on the Microsoft SQL Server products:

- **Microsoft Certified Database Administrators (MCDBAs):** For professionals who design, implement, and administer Microsoft SQL Server databases.

For developers and programmers, the following certifications are based on the Microsoft .NET Framework and Visual Studio products:

- **Microsoft Certified Professional Developer (MCPD):** For professionals who are recognized as expert Windows Application Developers, Web Application Developers, or Enterprise Applications Developers. They demonstrate that you can build rich applications that target a variety of platforms such as the Microsoft .NET Framework 2.0.

- **Microsoft Certified Application Developers (MCADs):** For professionals who use Microsoft technologies to develop and maintain department-level applications, components, web or desktop clients, or back-end data services.
For trainers and curriculum developers, the following certifications are available:

- **Microsoft Certified Trainer (MCT):** For qualified instructors who are certified by Microsoft to deliver Microsoft training courses to IT professionals and developers.

- **Microsoft Certified Learning Consultant (MCLC):** Recognizes MCTs whose job roles have grown to include frequent consultative engagements with their customers and who are experts in delivering customized learning solutions that positively affect customer return on investment (ROI).

In 2008, Microsoft introduced two advanced certifications. The Master certifications identify individuals with the deepest technical skills available on a particular Microsoft product, such as Windows Server 2008, Exchange 2007, and SQL Server 2008. To achieve Master certification, candidates must attend several required sessions, successfully complete all in-class exams (written and lab), and successfully complete a qualification lab exam.

The highest-level certification is the Microsoft Certified Architect (MCA) program, focusing on IT architecture. Microsoft Certified Architects have proven experience with delivering solutions and can communicate effectively with business, architecture, and technology professionals. These professionals have three or more years of advanced IT architecture experience and possess strong technical and leadership skills. Candidates are required to pass a rigorous Review Board interview conducted by a panel of experts.

The best place to keep tabs on all Microsoft certifications is the following website: http://www.microsoft.com/learning/default.mspx.

Microsoft changes their website often, so if this URL does not work in the future, you should use the Search tool on Microsoft’s site to find more information on a particular certification.

**Microsoft Certified Technology Specialist (MCTS)**

Technology Specialist certifications enable professionals to target specific technologies and to distinguish themselves by demonstrating in-depth knowledge and expertise in their specialized technologies. Microsoft Technology Specialists are consistently capable of implementing, building, troubleshooting, and debugging a particular Microsoft technology.
At the time of the writing of this book, there are 28 Microsoft Certified Technology Specialist (MCTS) certifications:

MCTS: SQL Server 2008, Business Intelligence Development and Maintenance
MCTS: SQL Server 2008, Database Development
MCTS: SQL Server 2008, Implementation and Maintenance
MCTS: .NET Framework 3.5, Windows Presentation Foundation Applications
MCTS: .NET Framework 3.5, Windows Communication Foundation Applications
MCTS: .NET Framework 3.5, Windows Workflow Foundation Applications
MCTS: .NET Framework 2.0 Web Applications
MCTS: .NET Framework 2.0 Windows Applications
MCTS: .NET Framework 2.0 Distributed Applications
MCTS: SQL Server 2005
MCTS: SQL Server 2005 Business Intelligence
MCTS: BizTalk Server 2006
MCTS: Enterprise Project Management with Microsoft Office Project Server 2007
MCTS: Managing Projects with Microsoft Office Project 2007
MCTS: Microsoft Office Live Communications Server 2005
MCTS: Microsoft Exchange Server 2007, Configuration
MCTS: Microsoft Office SharePoint Server 2007, Configuration
MCTS: Microsoft Office SharePoint Server 2007, Application Development
MCTS: Windows Mobile 5.0, Applications
MCTS: Windows Mobile 5.0, Implementing and Managing
MCTS: Windows Server 2003 Hosted Environments, Configuration, and Management
MCTS: Windows Server 2008 Active Directory Configuration
MCTS: Windows Server 2008 Network Infrastructure Configuration
MCTS: Windows Server 2008 Applications Infrastructure Configuration
MCTS: Windows SharePoint Services 3.0, Application Development
MCTS: Windows SharePoint Services 3.0, Configuration
The new Microsoft Certified IT Professional (MCITP) credential lets you highlight your specific area of expertise. Now you can easily distinguish yourself as an expert in database administration, database development, business intelligence, or support. At the time of this writing, the following Microsoft Certified IT Professional certifications exist:

- IT Professional: Database Developer
- IT Professional: Database Administrator
- IT Professional: Business Intelligence Developer
- IT Professional: Enterprise Support Technician
- IT Professional: Consumer Support Technician
- IT Professional: Database Developer 2008
- IT Professional: Database Administrator 2008
- IT Professional: Enterprise Messaging Administrator
- IT Professional: Enterprise Project Management with Microsoft Office Project Server 2007
- IT Professional: Enterprise Administrator
- IT Professional: Server Administrator

At the time of this writing, details are just starting to be revealed on the Microsoft Certified Technology Specialist (MCTS) on Windows Server 2008. The MCTS on Windows Server 2008 helps you and your organization save time, reduce costs and take advantage of advanced server technology with the power to increase the flexibility of your server infrastructure. Transition certifications are available today for Windows Server 2003 certified professionals, and full certification paths will be available soon after the Windows Server 2008 product release. For more details about these certifications, visit the following website:


If the URL is no longer available, don’t forget to search for MCTS and Windows Server 2008 with the Microsoft search tool found on the Microsoft website.
Microsoft Certified Technology Specialist: Windows Server 2008 Applications Infrastructure

The Microsoft Certified Technology Specialist certifications enable professionals to target specific technologies and distinguish themselves by demonstrating in-depth knowledge and expertise in their specialized technologies. A Microsoft Certified Technology Specialist in Windows Vista, Configuration possesses the knowledge and skills to configure Windows Vista for optimal performance on the desktop, including installing, managing, and configuring the new security, network, and application features in Windows Vista.

To earn the Microsoft Certified Technology Specialist: Windows Server 2008 Network Infrastructure, Configuration certification, you must pass one exam that focuses on supporting end-user issues about network connectivity, security, applications installation and compatibility, and logon problems that include account issues and password resets:

Exam 70-642: TS: Windows Server 2008 Applications Infrastructure, Configuration

If you decide to take a Microsoft-recognized class, you would take several classes to cover all the material found on this exam. The preparation guide (including exam objectives) for Exam 70-642 TS: Windows Server 2008 Network Infrastructure, Configuring can be found at http://www.microsoft.com/learning/exams/70-642.mspx

Taking a Certification Exam

After you prepare for your exam, you need to register with a testing center. At the time of this writing, the cost to take exam 70-642 is (U.S.) $125, and if you don’t pass, you can take each again for an additional (U.S.) $125 for each attempt. In the United States and Canada, tests are administered by Prometric. Here’s how you can contact them:

- **Prometric**: You can sign up for a test through the company’s website, http://www.2test.com or http://www.prometric.com. Within the United States and Canada, you can register by phone at 800-755-3926. If you live outside this region, you should check the Prometric website for the appropriate phone number.
To sign up for a test, you must possess a valid credit card or contact Prometric for mailing instructions to send a check (in the United States). Only when payment is verified, or a check has cleared, can you actually register for a test.

To schedule an exam, you need to call the appropriate phone number or visit the Prometric websites at least one day in advance. To cancel or reschedule an exam in the United States or Canada, you must call before 3 p.m. Eastern time the day before the scheduled test time (or you might be charged, even if you don’t show up to take the test). When you want to schedule a test, you should have the following information ready:

- Your name, organization, and mailing address.
- Your Microsoft test ID. (In the United States, this means your Social Security number; citizens of other countries should call ahead to find out what type of identification number is required to register for a test.)
- The name and number of the exam you want to take.
- A method of payment. (As mentioned previously, a credit card is the most convenient method, but alternate means can be arranged in advance, if necessary.)

After you sign up for a test, you are told when and where the test is scheduled. You should arrive at least 15 minutes early. You must supply two forms of identification—one of which must be a photo ID—to be admitted into the testing room.

**Tracking Certification Status**

As soon as you pass a qualified Microsoft exam and earn a professional certification, Microsoft generates transcripts that indicate which exams you have passed. You can view a copy of your transcript at any time by going to the MCP secured site (this site may change as the MCP is retired) and selecting the Transcript Tool. This tool enables you to print a copy of your current transcript and confirm your certification status.

After you pass the necessary set of exams, you are certified. Official certification is normally granted after six to eight weeks, so you shouldn’t expect to get your credentials overnight. The package for official certification that arrives includes a Welcome Kit that contains a number of elements (see Microsoft’s website for other benefits of specific certifications):

- A certificate that is suitable for framing, along with a wallet card and lapel pin.
A license to use the related certification logo, which means you can use the logo in advertisements, promotions, and documents, and on letterhead, business cards, and so on. Along with the license comes a logo sheet, which includes camera-ready artwork. (Note that before you use any of the artwork, you must sign and return a licensing agreement that indicates you’ll abide by its terms and conditions.)

Access to the *Microsoft Certified Professional Magazine Online* website, which provides ongoing data about testing and certification activities, requirements, changes to the MCP program, and security-related information on Microsoft products.

Many people believe that the benefits of MCP certification go well beyond the perks that Microsoft provides to newly anointed members of this elite group. We’re starting to see more job listings that request or require applicants to have Microsoft and other related certifications, and many individuals who complete Microsoft certification programs can qualify for increases in pay and responsibility. As an official recognition of hard work and broad knowledge, a certification credential is a badge of honor in many IT organizations.

**About This Book**

Each topical Exam Cram chapter follows a regular structure and contains graphical cues about important or useful information. Here’s the structure of a typical chapter:

- **Opening hotlists:** Each chapter begins with a list of the terms, tools, and techniques that you must learn and understand before you can be fully conversant with that chapter’s subject matter. The hotlists are followed with one or two introductory paragraphs to set the stage for the rest of the chapter.

- **Topical coverage:** After the opening hotlists and introductory text, each chapter covers a series of topics related to the chapter’s subject. Throughout that section, we highlight topics or concepts that are likely to appear on a test, using a special element called an Exam Alert:

**EXAM ALERT**

This is what an Exam Alert looks like. Normally, an alert stresses concepts, terms, software, or activities that are likely to relate to one or more certification-test questions. For that reason, we think any information in an Exam Alert is worthy of unusual attentiveness on your part.
You should pay close attention to material flagged in Exam Alerts; although all the information in this book pertains to what you need to know to pass the exam, Exam Alerts contain information that is really important. You’ll find what appears in the meat of each chapter to be worth knowing, too, when preparing for the test. Because this book’s material is very condensed, we recommend that you use this book along with other resources to achieve the maximum benefit.

In addition to the Exam Alerts, we provide tips and notes that will help you build a better foundation for Windows Server 2008 knowledge. Although the information might not be on the exam, it is certainly related and it will help you become a better-informed test taker.

**TIP**

This is how tips are formatted. Keep your eyes open for these, and you’ll become a Windows Server 2008 guru in no time!

**NOTE**

This is how notes are formatted. Notes direct your attention to important pieces of information that relate to Windows Server 2008 and Microsoft certification.

Each chapter contains the following:

- **Exam prep questions:** Although we talk about test questions and topics throughout the book, this section at the end of each chapter presents a series of mock test questions and explanations of both correct and incorrect answers.

- **Details and resources:** Every chapter ends with a section titled “Need to Know More?” That section provides direct pointers to Microsoft and third-party resources that offer more details on the chapter’s subject. In addition, that section tries to rank or at least rate the quality and thoroughness of the topic’s coverage by each resource. If you find a resource you like in that collection, you should use it, but you shouldn’t feel compelled to use all the resources. On the other hand, we recommend only resources that we use on a regular basis, so none of our recommendations will be a waste of your time or money (but purchasing them all at once probably represents an expense that many network administrators and Microsoft certification candidates might find hard to justify).
The bulk of the book follows this chapter structure, but we’d like to point out a few other elements. Practice Exams #1 and #2—two practice exams and their answers (with detailed explanations)—help you assess your understanding of the material presented throughout the book to ensure that you’re ready for the exam.

Finally, the tear-out Cram Sheet attached next to the inside front cover of this Exam Cram book represents a condensed collection of facts and tips that we think are essential for you to memorize before taking the test. Because you can dump this information out of your head onto a sheet of paper before taking the exam, you can master this information by brute force; you need to remember it only long enough to write it down when you walk into the testing room. You might even want to look at it in the car or in the lobby of the testing center just before you walk in to take the exam.

We’ve structured the topics in this book to build on one another. Therefore, some topics in later chapters make the most sense after you’ve read earlier chapters. That’s why we suggest that you read this book from front to back for your initial test preparation. If you need to brush up on a topic or if you have to bone up for a second try, you can use the index or table of contents to go straight to the topics and questions that you need to study. Beyond helping you prepare for the test, we think you’ll find this book useful as a tightly focused reference to some of the most important aspects of Windows Vista.

The book uses the following typographical conventions:

- Command-line strings that are meant to be typed into the computer are displayed in special font, such as
  
  net use lpt1: \print_server_name\printer_share_name

- New terms are introduced in italics.

Given all the book’s elements and its specialized focus, we’ve tried to create a tool that will help you prepare for and pass Microsoft Exam 70-642. Please share with us your feedback on the book, especially if you have ideas about how we can improve it for future test takers. Send your questions or comments about this book via email to feedback@quepublishing.com. We’ll consider everything you say carefully, and we’ll respond to all suggestions. For more information on this book and other Que Certification titles, visit our website at http://www.quepublishing.com. You should also check out the new Exam Cram website at http://www.examcram.com, where you’ll find information, updates, commentary, and certification information.
Exam Layout and Design

Historically, there have been six types of question formats on Microsoft certification exams. These types of questions continue to appear on current Microsoft tests, and they are discussed in the following sections:

- Multiple-choice, single answer
- Multiple-choice, multiple answers
- Build-list-and-reorder (list prioritization)
- Create-a-tree
- Drag-and-connect
- Select-and-place (drag-and-drop)

The Single-Answer and Multiple-Answer Multiple-Choice Question Formats

Some exam questions require you to select a single answer, whereas others ask you to select multiple correct answers. The following multiple-choice question requires you to select a single correct answer. Following the question is a brief summary of each potential answer and why it is either right or wrong.

1. You have three domains connected to an empty root domain under one contiguous domain name: \( \text{tutu.com} \). This organization is formed into a forest arrangement, with a secondary domain called \( \text{frog.com} \). How many schema masters exist for this arrangement?

   - A. 1
   - B. 2
   - C. 3
   - D. 4

   1. The correct answer is A because only one schema master is necessary for a forest arrangement. The other answers (B, C, and D) are misleading because they try to make you believe that schema masters might be in each domain or perhaps that you should have one for each contiguous namespace domain.

This sample question format corresponds closely to the Microsoft certification exam format. The only difference is that on the exam, the questions are not followed by answers and their explanations. To select an answer, you position the
cursor over the option button next to the answer you want to select. Then you click the mouse button to select the answer.

Let’s examine a question for which one or more answers are possible. This type of question provides check boxes rather than option buttons for marking all appropriate selections.

2. What can you use to seize FSMO roles? (Choose two.)
   - A. The ntdsutil.exe utility
   - B. The Active Directory Users and Computers console
   - C. The secedit.exe utility
   - D. The utilman.exe utility

2. Answers A and B are correct. You can seize roles from a server that is still running through the Active Directory Users and Computers console, or in the case of a server failure, you can seize roles with the ntdsutil.exe utility. You use the secedit.exe utility to force group policies into play; therefore, Answer C is incorrect. The utilman.exe tool manages accessibility settings in Windows Server 2003; therefore, Answer D is incorrect.

This particular question requires two answers. Microsoft sometimes gives partial credit for partially correct answers. For Question 2, you have to mark the check boxes next to Answers A and B to obtain credit for a correct answer. Notice that to choose the right answers you also need to know why the other answers are wrong.

### The Build-List-and-Reorder Question Format

Questions in the build-list-and-reorder format present two lists of items—one on the left and one on the right. To answer the question, you must move items from the list on the right to the list on the left. The final list must then be reordered into a specific sequence.

These questions generally sound like this: “From the following list of choices, pick the choices that answer the question. Arrange the list in a certain order.” Question 3 shows an example of how these questions would look.

3. From the following list of famous people, choose those who have been elected president of the United States. Arrange the list in the order in which the presidents served.
   - Thomas Jefferson
   - Ben Franklin
   - Abe Lincoln
3. The correct answer is

1. George Washington
2. Thomas Jefferson
3. Andrew Jackson
4. Abe Lincoln

On an actual exam, the entire list of famous people would initially appear in the list on the right. You would move the four correct answers to the list on the left and then reorder the list on the left. Notice that the answer to Question 3 does not include all the items from the initial list. However, that might not always be the case.

To move an item from the right list to the left list on the exam, you first select the item by clicking it, and then you click the Add button (left arrow). After you move an item from one list to the other, you can move the item back by first selecting the item and then clicking the appropriate button (either the Add button or the Remove button). After you move items to the left list, you can reorder an item by selecting the item and clicking the up or down arrow buttons.

The Create-a-Tree Question Format

Questions in the create-a-tree format also present two lists—one on the left side of the screen and one on the right side of the screen. The list on the right consists of individual items, and the list on the left consists of nodes in a tree. To answer the question, you must move items from the list on the right to the appropriate node in the tree.

These questions can best be characterized as simply a matching exercise. Items from the list on the right are placed under the appropriate category in the list on the left. Question 4 shows an example of how they would look.

4. The calendar year is divided into four seasons:

1. Winter
2. Spring
3. Summer
4. Fall

Identify the season during which each of the following holidays occurs:

- Christmas
- Fourth of July
- Labor Day
- Flag Day
- Memorial Day
- Washington’s Birthday
- Thanksgiving
- Easter

4. The correct answers are

1. Winter
   - Christmas
   - Washington’s Birthday

2. Spring
   - Flag Day
   - Memorial Day
   - Easter

3. Summer
   - Fourth of July
   - Labor Day

4. Fall
   - Thanksgiving

In this case, you use all the items in the list. However, that might not always be the case.

To move an item from the right list to its appropriate location in the tree, you must first select the appropriate tree node by clicking it. Then you select the item to be moved and click the Add button. After you add one or more items to
a tree node, the node appears with a + icon to the left of the node name. You can click this icon to expand the node and view the items you have added. If you have added any item to the wrong tree node, you can remove it by selecting it and clicking the Remove button.

The Drag-and-Connect Question Format

Questions in the drag-and-connect format present a group of objects and a list of “connections.” To answer the question, you must move the appropriate connections between the objects.

This type of question is best described with graphics. For this type of question, it isn’t necessary to use every object, and you can use each connection multiple times.

The Select-and-Place Question Format

Questions in the select-and-place (drag-and-drop) format display a diagram with blank boxes and a list of labels that you need to drag to correctly fill in the blank boxes. To answer such a question, you must move the labels to their appropriate positions on the diagram. This type of question is best understood with graphics.

Special Exam Question Formats

Starting with the exams released for the Windows Server 2003 MCSE track, Microsoft introduced several new question types in addition to the more traditional types of questions that are still widely used on all Microsoft exams. These innovative question types have been highly researched and tested by Microsoft before they were chosen to be included in many of the “refreshed” exams for the MCSA/MCSE on the Windows 2000 track and for the new exams on the Windows Server 2003 and Windows Server 2008 track. These special question types are as follows:

- Hot area questions
- Active screen questions
- Drag-and-drop–type questions
- Simulation questions
Hot Area Question Types
Hot area questions ask you to indicate the correct answer by selecting one or more elements within a graphic. For example, you might be asked to select multiple objects within a list.

Active Screen Question Types
Active screen questions ask you to configure a dialog box by modifying one or more elements. These types of questions offer a realistic interface in which you must properly configure various settings, just as you would within the actual software product. For example, you might be asked to select the proper option within a drop-down list box.

Drag-and-Drop Question Types
New drag-and-drop questions ask you to drag source elements to their appropriate corresponding targets within a work area. These types of questions test your knowledge of specific concepts and their definitions or descriptions. For example, you might be asked to match a description of a computer program to the actual software application.

Simulation Question Types
Simulation questions ask you to indicate the correct answer by performing specific tasks, such as configuring and installing network adapters or drivers, configuring and controlling access to files, or troubleshooting hardware devices. Many of the tasks that systems administrators and systems engineers perform can be presented more accurately in simulations than in most traditional exam question types.

Microsoft’s Testing Formats
Currently, Microsoft uses three different testing formats:
- Fixed length
- Short form
- Case study

Other Microsoft exams employ advanced testing capabilities that might not be immediately apparent. Although the questions that appear are primarily multiple choice, the logic that drives them is more complex than that in older Microsoft tests, which use a fixed sequence of questions, called a *fixed-length test*. Some
questions employ a sophisticated user interface, which Microsoft calls a *simulation*, to test your knowledge of the software and systems under consideration in a more-or-less “live” environment that behaves just like the real thing. You should review the Microsoft Learning, Reference, and Certification Web pages at http://www.microsoft.com/learning/default.mspx for more detailed information.

In the future, Microsoft might choose to create exams using a well-known technique called *adaptive testing* to establish a test taker’s level of knowledge and product competence. In general, adaptive exams might look the same as fixed-length exams, but they discover the level of difficulty at which an individual test taker can correctly answer questions. Test takers with differing levels of knowledge or ability therefore see different sets of questions; individuals with high levels of knowledge or ability are presented with a smaller set of more difficult questions, whereas individuals with lower levels of knowledge are presented with a larger set of easier questions. Two individuals might answer the same percentage of questions correctly, but the test taker with a higher knowledge or ability level scores higher because his or her questions are worth more. Also, the lower-level test taker is likely to answer more questions than his or her more knowledgeable colleague. This explains why adaptive tests use ranges of values to define the number of questions and the amount of time it takes to complete the test.

**NOTE**

Microsoft does *not* offer adaptive exams at the time of this book’s publication.

Most adaptive tests work by evaluating the test taker’s most recent answer. A correct answer leads to a more difficult question, and the test software’s estimate of the test taker’s knowledge and ability level is raised. An incorrect answer leads to a less difficult question, and the test software’s estimate of the test taker's knowledge and ability level is lowered. This process continues until the test targets the test taker’s true ability level. The exam ends when the test taker’s level of accuracy meets a statistically acceptable value (in other words, when his or her performance demonstrates an acceptable level of knowledge and ability) or when the maximum number of items has been presented. (In which case, the test taker is almost certain to fail.)

Microsoft has also introduced a short-form test for its most popular tests. This test delivers 25 to 30 questions to its takers, giving them exactly 60 minutes to complete the exam. This type of exam is similar to a fixed-length test in that it
allows readers to jump ahead or return to earlier questions and to cycle through the questions until the test is done. Microsoft does not use adaptive logic in short-form tests, but it claims that statistical analysis of the question pool is such that the 25 to 30 questions delivered during a short-form exam conclusively measure a test taker’s knowledge of the subject matter in much the same way as an adaptive test. You can think of the short-form test as a kind of “greatest hits exam” (that is, it covers the most important questions) version of an adaptive exam on the same topic.

Because you won’t know which form the Microsoft exam might take, you should be prepared for either a fixed-length or short-form exam. The layout is the same for both fixed-length and short-form tests—you are not penalized for guessing the correct answer(s) to questions, no matter how many questions you answer incorrectly.

**The Fixed-Length and Short-Form Exam Strategy**

One tactic that has worked well for many test takers is to answer each question as well as you can before time expires on the exam. Some questions you will undoubtedly feel better equipped to answer correctly than others; however, you should still select an answer to each question as you proceed through the exam. You should click the Mark for Review check box for any question of which you are unsure. In this way, at least you have answered all the questions in case you run out of time. Unanswered questions are automatically scored as incorrect; answers that are guessed have at least some chance of being scored as correct. If time permits, after you answer all questions you can revisit each question that you have marked for review. This strategy also enables you to possibly gain some insight into questions of which you are unsure by picking up some clues from the other questions on the exam.

**TIP**

Some people prefer to read over the exam completely before answering the trickier questions; sometimes, information supplied in later questions sheds more light on earlier questions. At other times, information you read in later questions might jog your memory about facts, figures, or behavior that helps you answer earlier questions. Either way, you could come out ahead if you answer only those questions on the first pass that you’re absolutely confident about. However, be careful not to run out of time if you choose this strategy!
Fortunately, the Microsoft exam software for fixed-length and short-form tests makes the multiple-visit approach easy to implement. At the top-left corner of each question is a check box that permits you to mark that question for a later visit.

Here are some question-handling strategies that apply to fixed-length and short-form tests. Use them if you have the chance:

- When returning to a question after your initial read-through, read every word again; otherwise, your mind can miss important details. Sometimes, revisiting a question after turning your attention elsewhere lets you see something you missed, but the strong tendency is to see only what you’ve seen before. Avoid that tendency at all costs.

- If you return to a question more than twice, articulate to yourself what you don’t understand about the question, why answers don’t appear to make sense, or what appears to be missing. If you chew on the subject awhile, your subconscious might provide the missing details, or you might notice a “trick” that points to the right answer.

As you work your way through the exam, another counter that Microsoft provides will come in handy: the number of questions completed and questions outstanding. For fixed-length and short-form tests, it’s wise to budget your time by making sure that you’ve completed one-quarter of the questions one-quarter of the way through the exam period and three-quarters of the questions three-quarters of the way through.

If you’re not finished when only five minutes remain, use that time to guess your way through any remaining questions. Remember, guessing is potentially more valuable than not answering. Blank answers are always wrong, but a guess might turn out to be right. If you don’t have a clue about any of the remaining questions, pick answers at random or choose all As, Bs, and so on. (Choosing the same answer for a series of question all but guarantees you’ll get most of them wrong, but it also means you’re more likely to get a small percentage of them correct.)

**EXAM ALERT**

At the very end of your exam period, you’re better off guessing than leaving questions unanswered.
Question-Handling Strategies

For those questions that have only one right answer, usually two or three of the answers are obviously incorrect and two of the answers are plausible. Unless the answer leaps out at you (if it does, reread the question to look for a trick; sometimes those are the ones you’re most likely to get wrong), begin the process of answering by eliminating those answers that are most obviously wrong.

You can usually immediately eliminate at least one answer out of the possible choices for a question because it matches one of these conditions:

- The answer does not apply to the situation.
- The answer describes a nonexistent issue, an invalid option, or an imaginary state.

After you eliminate all answers that are obviously wrong, you can apply your retained knowledge to eliminate further answers. You should look for items that sound correct but refer to actions, commands, or features that are not present or not available in the situation that the question describes.

If you’re still faced with a blind guess among two or more potentially correct answers, reread the question. Picture how each of the possible remaining answers would alter the situation. Be especially sensitive to terminology; sometimes the choice of words (for example, “remove” instead of “disable”) can make the difference between a right answer and a wrong one.

You should guess at an answer only after you’ve exhausted your ability to eliminate answers and you are still unclear about which of the remaining possibilities is correct. An unanswered question offers you no points, but guessing gives you at least some chance of getting a question right; just don’t be too hasty when making a blind guess if you can eliminate one or two of the answers.

Numerous questions assume that the default behavior of a particular utility is in effect. If you know the defaults and understand what they mean, this knowledge will help you cut through many of the trickier questions. Simple “final” actions might be critical as well. If you must restart a utility before proposed changes take effect, a correct answer might require this step as well.
Mastering the Test-Taking Mindset

In the final analysis, knowledge breeds confidence, and confidence breeds success. If you study the materials in this book carefully and review all the practice questions at the end of each chapter, you should become aware of the areas where you need additional learning and study.

After you’ve worked your way through the book, take the practice exams in the back of the book. Taking these tests provides a reality check and helps you identify areas to study further. Make sure you follow up and review materials related to the questions you miss on the practice exams before scheduling a real exam. Don’t schedule your exam appointment until after you’ve thoroughly studied the material and you feel comfortable with the whole scope of the practice exams. You should score 80% or better on the practice exams before proceeding to the real thing. (Otherwise, obtain some additional practice tests so that you can keep trying until you hit this magic number.)

TIP

If you take a practice exam and don’t get at least 80% of the questions correct, keep practicing. Microsoft provides links to practice-exam providers and also self-assessment exams at http://www.microsoft.com/learning/mcpexams/prepare/default.asp.

Armed with the information in this book and with the determination to augment your knowledge, you should be able to pass the certification exam. However, you need to work at it, or you’ll spend the exam fee more than once before you finally pass. If you prepare seriously, you should do well.

The next section covers other sources that you can use to prepare for Microsoft certification exams.

Additional Resources

A good source of information about Microsoft certification exams comes from Microsoft itself. Because its products and technologies—and the exams that go with them—change frequently, the best place to go for exam-related information is online.

Microsoft offers training, certification, and other learning-related information and links at the http://www.microsoft.com/learning web address. If you haven’t already visited the Microsoft Training and Certification website, you should do so right now.
Sooner or later, all the information we’ve shared with you about the Microsoft Certified Professional pages and the other web-based resources mentioned throughout the rest of this book will go stale or be replaced by newer information. In some cases, the URLs you find here might lead you to their replacements; in other cases, the URLs will go nowhere, leaving you with the dreaded “404 File not found” error message. When that happens, don’t give up.

There’s always a way to find what you want on the web if you’re willing to invest some time and energy. Most large or complex websites—and Microsoft’s qualifies on both counts—offer search engines. All of Microsoft’s web pages have a Search button at the top edge of the page. As long as you can get to Microsoft’s site (it should stay at http://www.microsoft.com for a long time), you can use the Search button to find what you need.

The more focused (or specific) that you can make a search request, the more likely the results will include information you can use. For example, you can search for the string "training and certification" to produce a lot of data about the subject in general, but if you’re looking for the preparation guide for Exam 70-642, *Windows Server 2008 Network Infrastructure, Configuring*, you’ll be more likely to get there quickly if you use a search string similar to the following:

"Exam 70-642" AND "preparation guide"

Likewise, if you want to find the Training and Certification downloads, you should try a search string such as this:

"training and certification" AND "download page"

Finally, you should feel free to use general search tools—such as http://www.google.com, http://www.yahoo.com, http://www.excite.com, and http://www.ask.com—to look for related information. Although Microsoft offers great information about its certification exams online, there are plenty of third-party sources of information and assistance that need not follow Microsoft’s party line. Therefore, if you can’t find something where the book says it lives, you should intensify your search.
# Terms you’ll need to understand:
- Router
- Metric
- Hop
- Static routes
- Dynamic routes
- Router Information Protocol (RIP)
- Split-horizon
- Open Shortest Path First (OSPF)
- Firewall
- Stateful firewall
- Windows Firewall
- Windows Firewall with Advanced Security
- Usage profile
- Network address translation (NAT)

## Techniques/concepts you’ll need to master:
- Configure static routes using Router and Remote Access (RRAS) console and using the `Route.exe` command.
- Configure Router Information Protocol (RIP).
- Configure dial-up routing.
- Configure Network address translation.
A router is a device that manages the flow of data between network segments, or subnets. As multiple LANs or segments are connected together, multiple routes are created to get data from one LAN or segment to another. A router directs incoming and outgoing packets based on the information it holds about the state of its own network interfaces and a list of possible destinations for network traffic.

By projecting network traffic and routing needs, you can decide whether you want to use a dedicated hardware router, such as a Cisco router, or a software-based router, such as those included with Windows Server 2008. If you have heavy routing demands, you would almost always use dedicated hardware routers. For smaller networks, a software-based routing solution could be used. For routing, Microsoft Windows Server 2008 includes the Routing and Remote Access service.

**Routing and Routers**

When you send a packet from one computer to another computer, it first determines whether the packet is sent locally to another computer on the same LAN or to router so that it can be routed to the destination LAN. If the packet is meant to go to a computer on another LAN, it is sent to the router (or gateway). The router then determines the best route to take and forwards the packets to that route. The packet then goes to the next router and the entire process repeats itself until it gets to the destination LAN. The destination router then forwards the packets to the destination computer.

To determine the best route, the routes use complex routing algorithms, which take into account a variety of factors, including the speed of each transmission media, the number of network segments, and the network segment that carries the least traffic. Routers then share status and routing information to other routers so that they can provide better traffic management and bypass slow connections. In addition, routers provide additional functionality, such as the capability to filter messages and forward them to different places based on various criteria. Most routers are multiprotocol routers because they can route data packets using many different protocols.

A metric is a standard of measurement, such as hop count, that is used by routing algorithms to determine the optimal path to a destination. A hop is the trip a data packet takes from one router to another router or from a router to another intermediate point to another in the network. On a large network, the number of hops a packet has taken toward its destination is called the hop count. When a computer communicates with another computer, and the computer has to go through four routers, it has a hop count of four. With no other factors taken into
account, a metric of four would be assigned. If a router had a choice between a
route with four metrics and a route with six metrics, it would choose the route
with four metrics over the route with six metrics. Of course, if you want the
router to choose the route with six metrics, you can overwrite the metric for the
route with four hops in the routing table to a higher value.

To keep track of the various routes in a network, routers create and maintain
routing tables. Routers communicate with one another to maintain their routing
tables through a routing update message. The routing update message can consist
of all or a portion of a routing table. By analyzing routing updates from all other
routers, a router can build a detailed picture of network topology.

**Static Versus Dynamic Routes**

Static routing algorithms are hardly algorithms at all, but are table mappings
established by the network administrator prior to the beginning of routing.
These mappings do not change unless the network administrator alters them.
Algorithms that use static routes are simple to design and work well in environ-
ments where network traffic is relatively predictable and where network design
is relatively simple.

Because static routing systems cannot react to network changes, they generally
are considered unsuitable for today’s large, changing networks. Most of the
dominant routing algorithms are dynamic routing algorithms, which adjust to
changing network circumstances by analyzing incoming routing update messages.
If the message indicates that a network change has occurred, the routing software
recalculates routes and sends out new routing update messages. These messages
flow through the network, stimulating routers to rerun their algorithms and
change their routing tables accordingly.

**NOTE**

Dynamic routing algorithms can be supplemented with static routes where appropriate.

**Distance-Vector Versus Link-State Algorithm**

Routers use distance-vector–based routing protocols to periodically advertise or
broadcast the routes in their routing tables, but they send it to only their neighbor-
ing routers. Routing information exchanged between typical distance-vector–based
routers is unsynchronized and unacknowledged. Distance-vector–based routing
protocols are simple and easy to understand and easy to configure. The disad-
vantage is that multiple routes to a given network can reflect multiple entries in
the routing table, which leads to a large routing table. In addition, if you have a large routing table, network traffic increases as it periodically advertises the routing table to the other routers, even after the network has converged. Last, distance-vector protocol convergence of large internetworks can take several minutes.

Link-state algorithms are also known as shortest path first algorithms. Instead of using broadcast, link-state routers send updates directly (or by using multicast traffic) to all routers within the network. Each router, however, sends only the portion of the routing table that describes the state of its own links. In essence, link-state algorithms send small updates everywhere. Because they converge more quickly, link-state algorithms are somewhat less prone to routing loops than distance-vector algorithms. In addition, link-state algorithms do not exchange any routing information when the internetwork has converged. They have small routing tables because they store a single optimal route for each network ID. On the other hand, link-state algorithms require more CPU power and memory than distance-vector algorithms. Link-state algorithms, therefore, can be more expensive to implement and support and are considered harder to understand.

Routing Information Protocol

A popular routing protocol is the Routing Information Protocol (RIP), which is a distance-vector protocol designed for exchanging routing information within a small- to medium-size network. The biggest advantage of RIP is that it is extremely simple to configure and deploy.

RIP uses a single routing metric of hop counts (number of routers) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop-count value, which is typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router adds one to the metric value indicated in the update and enters the network in the routing table. The sender’s IP address is used as the next hop.

Because RIP uses only hop count to determine the best path to an internetwork. If RIP finds more than one link to the same remote network with the same hop count, it automatically performs a round-robin load balance. RIP can perform load balancing for up to six equal-cost links.

However, a problem with using hops as the only metric is when two links to a remote network have different bandwidths. For example, if you have one link that is a 56KB switched link and a T1 running at 1.544Mbps, there would be
some inefficiency when sending equal data through both pathways. This is known as pinhole congestion. To overcome pinhole congestion, you have to design a network with equal bandwidth links or use a routing protocol that takes bandwidth into account.

RIP prevents routing loops from continuing indefinitely by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops in a path is 15. If a router receives a routing update that contains a new or changed entry, and if increasing the metric value by one causes the metric to be infinity (in this case, 16), the network destination is considered unreachable. Of course, this makes it impossible for RIP to scale to large or very large internetworks. Note: The count-to-infinity problem is the reason why the maximum hop count of RIP for IP internetworks is set to 15 (16 for unreachable). Higher maximum hop count values would make the convergence time longer when count-to-infinity occurs.

Initially, the routing table for each router includes only the networks that are physically connected to it. A RIP router periodically (every 30 seconds) sends announcements that contain its routing table entries so that the other routers can update their routing tables. RIP version 1 uses IP broadcast packets for its announcements. RIP version 2 uses multicast or broadcast packets for its announcements. All RIP messages are sent over UDP port 520.

RIP routers can also communicate routing information through triggered updates, which are triggered when the network topology changes. Different from the scheduled announcements, the triggered updates are sent immediately rather than held for the next periodic announcement. For example, when a router detects a link or router failure, it updates its own routing table and sends the updated routes. Each router that receives the triggered update modifies its own routing table and propagates the change to the other routers.

You can configure each RIP router with a list of routers (by IP address) that accepts RIP announcements. By configuring a list of RIP peers, RIP announcements from unauthorized RIP routers are discarded. In addition, to prevent RIP traffic from being received by any node except neighboring RIP routers, you can set up some routers to use unicast RIP announcements to neighboring RIP routers.

Because the RIP is a distance-vector protocol, as internetworks grow larger in size, the periodic announcements by each RIP router can cause excessive traffic. Another disadvantage of RIP is its high convergence time. When the network topology changes, it may take several minutes before the RIP routers reconfigure themselves to the new network topology. As the network reconfigures itself, routing loops may form that result in lost or undeliverable data. To help prevent routing loops, RIP implements split-horizon.
To overcome some of RIP shortcomings, RIP Version 2 (RIP II) was introduced. RIP v2 provides the following features:

- You can use a password for authentication by specifying a key that is used to authenticate routing information to the router. Simple password authentication was defined in RFC 1723, but newer authentication mechanisms, such as Message Digest 5 (MD5), are available.

- RIP v2 includes the subnet mask in the routing information and supports variable-length subnets. Variable-length subnet masks can be associated with each destination, allowing an increase in the number of hosts or subnets that are possible on your network.

- The routing table can contain information about the IP address of the router that should be used to reach each destination. This helps prevent packets from being forwarded through extra routers on the system.

- Multicast packets speak only to RIP v2 routers and are used to reduce the load on hosts not listening to RIP v2 packets. The IP multicast address for RIP v2 packets is 224.0.0.9. Note: Silent RIP nodes must also be listening for multicast traffic sent to 224.0.0.9. If you are using Silent RIP, verify that your Silent RIP nodes can listen for multicasted RIP v2 announcements before deploying multicasted RIP v2.

**EXAM ALERT**

RIPv2 supports multicasting for updating the routing tables. RIPv1 does not support this feature. RIPv1 routers cannot communicate with RIPv2 routers that use multicasting for updates.

**Open Shortest Path First (OSPF)**

For small or medium networks, distributing data throughout the network and maintaining a route table at each router is not a problem. When the network grows to a size that includes hundreds of routers, the routing table can be quite large (several megabytes) and calculating routes requires significant time as the number of router interfaces goes up or down.

Some protocols, such as *Open Shortest Path First (OSPF)*, allow areas (grouping of contiguous networks) to be grouped together into an autonomous system (AS). Areas that make up the autonomous areas usually correspond to an administrative domain, such as a department, a building, or a geographic site. An AS can be a single network or a group of networks, which is owned and administered by a common network administrator or group of administrators.
OSPF is a link-state routing protocol used in medium-sized and large networks that calculates routing table entries by constructing a shortest-path tree. OSPF is designed for large internetworks (especially those spanning more than 15 router hops). The disadvantage of OSPF is that it’s generally more complex to set up and requires a certain amount of planning.

EXAM ALERT
The Open Shortest Path First (OSPF) routing protocol component in Routing and Remote Access has been removed from Windows Server 2008.

Routing and Remote Access Service (RRAS)

With Routing and Remote Access (RRAS), a computer running Windows Server 2008 can function as a network router, which routes IP packets between networks. This router service allows LANs and WANs to be interconnected easily. The routing technology is built into the operating system, providing small and large businesses with a cost-effective and secure way of interconnecting their networks.

You install the Routing and Remote Access service by using the Add Roles Wizard. To install the Routing and Remote Access service, follow these steps:

1. In the Server Manager main window, under Roles Summary, click Add roles. Or if you use the Initial Configuration Tasks window, under Customize This Server, click Add roles.

2. In the Add Roles Wizard, click Next.

3. In the list of server roles, select Network Policy and Access Services. Click Next twice.

4. In the list of role services, select Routing and Remote Access Services to select all the role services. You can also select individual server roles. Click Next.

5. Proceed through the steps in the Add Roles Wizard to complete the installation.

After you complete the installation, the Routing and Remote Access service is installed in a disabled state. To enable the Routing and Remote Access service, follow these steps:

2. By default, the local computer is listed as a server.

3. To add another server, in the console tree, right-click Server Status, and then click Add Server.

4. In the Add Server dialog box, click the applicable option, and then click OK.

5. In the console tree, right-click the server you want to enable, and then click Configure and Enable Routing and Remote Access. Click Next.

6. Click Custom Configuration and click Next.

7. To enable LAN routing, select LAN routing and click Next.

8. Click the Finish button.

To enable LAN and WAN routing after Routing and Remote Access service has been enabled:


2. Right-click the server name for which you want to enable routing and then click Properties.

3. On the General tab, select the appropriate IPv4 and IPv6 Router check boxes and select either Local Area Network (LAN) Routing Only or LAN and Demand-Dial Routing.

4. Click OK.

Creating Static Routes

In some instances you need to add a static route to your Windows Server 2008 router. This, of course, has its advantages and disadvantages. Creating a static route is simple; however, the routes you configure are not shared between routers. Static routes specify the network address and subnet mask that tell the router how to reach a certain destination. The router uses the information to determine to which gateway to forward the packet so that the packet can reach the destination host.

Static routes can be configured in one of two ways:

- Using the `route` command.

- Using the RRAS management console.
Using the Route Command

The route command is used to view and modify the network routing tables of an IP network. The route print command displays a list of current routes that the host knows (see Figure 5.1).

Routes added to a routing table are not made persistent unless the -p switch is specified. Non-persistent routes last only until the computer is restarted or until the interface is deactivated. The interface can be deactivated when the plug-and-play interface is unplugged (such as for laptops and hot-swap PCs), when the wire is removed from the media card (if the adapter supports media fault sensing), or when the interface is manually disconnected from the adapter in the Network and Dial-up Connections folder.

The usage for the route command is

```
ROUTE [-f] [-p] [command [destination]] [MASK netmask] [gateway] ➤ [METRIC metric]
```

- `-f`—Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared before the command is run.
Chapter 5: Routing and Filtering Network Traffic

- **-p**—When used with the `add` command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. When used with the `print` command, displays the list of registered persistent routes. Ignored for all other commands, which always affects the appropriate persistent routes.

- **Destination**—Specifies the network or host to which packets are being sent to.

- **MASK netmask**—Specifies a subnet mask to be associated with this route entry. If a `netmask` value is not specified, it defaults to 255.255.255.255.

- **gateway**—Specifies gateway or router.

- **METRIC metric**—Assigns an integer cost metric (ranging from 1 to 9,999) to be used in calculating the fastest, most reliable, and/or least expensive routes.

The commands usable in the preceding syntax are `PRINT`, `ADD`, `DELETE`, and `CHANGE`:

- **PRINT**—Displays a route
- **ADD**—Adds a route
- **DELETE**—Deletes a route
- **CHANGE**—Modifies an existing route

**EXAM ALERT**

Persistent routes are stored in the following Registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes
```

For example, to create a static route, you could type

```
route ADD 132.133.200.0 MASK 255.255.255.0 63.197.142.1 METRIC 2
```

After this command is executed, any packet that is sent to the 132.133.200.0 network or host with an IP address ranging between 132.133.200.1 and 132.133.200.254 will be forwarded to the router with a local host address of 63.197.142.1. If multiply entries specify these destination addresses, this route has a metric of two hops.
Using Routing and Remote Access

To add a static route to a Windows Server 2008 multihomed computer, you would use the Routing and Remote Access program located under Administrative Tools or use the appropriate MMC snap-in. Next, right-click Static Routes under IPv4 or IPv6 and select New Static Route for IP Networks (see Figure 5.2).

For a static IP route, in Interface, Destination, Network Mask, Gateway, and Metric, enter the interface, destination, network mask, gateway, and metric. If this is a demand-dial interface, Gateway is unavailable. You can also select the Use This Route to Initiate Demand-Dial Connections check box to initiate a demand-dial connection for traffic that matches the route.

For IP static addresses, the destination provides a space for you to type a destination for the route. The destination can be a host address, subnet address, network address, or the destination for the default route (0.0.0.0). The subnet mask provides a space for you to type the network mask for the static route. The network mask number is used in conjunction with the destination to determine when the route is used.

The mask of 255.255.255.255 means that only an exact match of the destination number can use this route. The mask of 0.0.0.0 means that any destination can use this route. The gateway provides a space for you to type the forwarding IP address for this route. For LAN interfaces, the gateway address must be configured and must be a directly reachable IP address for the network segment of the selected interface. Again, for demand-dial interfaces, the gateway address is not configured or used. The metric provides a space to type the cost associated with this route to reach the destination. The metric is commonly used to indicate the
number of routers (hops) to the destination. When deciding between multiple routes to the same destination, the route with the lowest metric is selected as the best route.

**Demand-Dial Routing**

Two types of demand-dial connections can be created for routing:

- On-demand connections
- Persistent connections

With demand-dial connections, a connection with the remote router is established only when necessary. A connection is established to route information and is terminated when the link is not in use. The benefit of this connection is obviously the cost savings associated with not using a dedicated link.

With persistent connections, the link does not need to be terminated. Even when it is not in use, it remains open. Connections between network routers can be one-way or two-way initiated, meaning that a connection can be initiated by only one router or by both the routers. With one-way–initiated connections, one router is designated as the answering router and the other is designated as the calling router, which is responsible for initiating any connections.

**One-Way Demand-Dial Routing**

Demand-dial connections can be created within the Routing and Remote Access snap-in. How you configure the connection depends on whether you are configuring a one-way– or two-way–initiated connection. To create a demand-dial interface on the calling router follow these steps:

1. Right-click Network Interfaces within the RRAS console and click New Demand-Dial Interface. This launches the Demand-Dial Interface Wizard. Click Next.
2. Type a name for the interface. Click Next.
3. Select the connection type. Click Next. Select the device that is used for making the connection. Click Next.
4. Type in the phone number of the remote server you are dialing. Click Next.
5. From the Protocols and Security window, select the necessary options:
Demand-Dial Routing

- Route IP Packets on This Interface
- Add a User Account So a Remote User Can Dial In
- Send a Plain-Text Password If That Is the Only Way to Connect
- Use Scripting to Complete the Connection with the Remote Router

6. Configure a static route to the remote network. Click Next.

7. From the Dial Out Credentials window, specify the username and password that the dial-out router will use to connect to the remote router. Click Next.

8. Click Finish.

**NOTE**

Before you attempt to create a new demand-dial interface, make sure the router is enabled for LAN and demand-dial routing rather than just LAN routing. You can enable this option by right-clicking the RRAS server and choosing Properties. From the General tab, select LAN and Demand-Dial Routing.

The answering router also needs to be configured for one-way demand-dial connections. A user account must be created on the answering router with dial-in permissions and the appropriate policy permissions. The user account is used to authenticate connections from the calling routers. A static route can then be configured on the user account. Also make sure when creating a user account that the Password Never Expires option is selected and the User Must Change Password at Next Logon option is not selected.

**EXAM ALERT**

When configuring the calling router, make sure that the dial-out credentials match the user account name configured on the answering router.

Two-Way Demand-Dial Routing

Creating a two-way demand-dial connection is similar to configuring a one-way connection, but there are a few distinct differences. A demand-dial interface is created on each RRAS server by the process outlined previously to create a one-way demand-dial connection. You must assign a name to the interface and specify the phone number to dial, the device to be used, the protocol and security settings,
Chapter 5: Routing and Filtering Network Traffic

and the dial-out credentials. You must also configure a user account, with the appropriate remote access permissions, on each RRAS server. Keep in mind that the user account name must be identical to the name assigned to the demand-dial interface of the calling router. Finally, you must configure a static route using the demand-dial interface.

**EXAM ALERT**

Remember when you are configuring two-way demand dialing that the user account names on the answering router must be identical to the demand-dial interface names on the calling routers.

**Configuring Demand-Dial Routing**

When a demand-dial connection has been created, you can configure it further using the Properties window for the connection. From the Options tab, configure the connection type: either demand-dial or persistent. You can also set the dialing policy by specifying the number of times that the calling router should redial if there is no answer and by specifying the interval between redial attempts.

The Security tab enables you to configure the security options for the dial-out connection. This configuration includes whether unsecured passwords are permitted, whether the connection requires data encryption, and whether a script will be run after dialing.

You can make several other configurations to a demand-dial interface. Demand-dial filtering enables you to control the type of IP traffic that can initiate a connection. You can allow or deny a connection based on the type of IP traffic. For example, you might want only web and FTP traffic to initiate the demand-dial connection. Dial-out hours determine the times of day that a connection can be initiated. This enables an administrator to control when the demand-dial connection is used.

**Managing RIP**

After the demand-dial or LAN interfaces have been created, configuring the appropriate routing protocol interfaces is the last step in configuring the RRAS server as a network router. You must first add the routing protocol by right-clicking the General node and choosing New Routing Protocol. The window that appears lists the protocols from which you can choose. Select RIPv2 and click OK.
After the routing protocol has been added, you must add the interfaces. To do so, right-click the appropriate routing protocol and select New Interface. After you select an interface and click OK, the Properties window for the interface appears, enabling you to configure it.

Every RIP interface has its own Properties window from which you can configure a number of options. Within the RRAS console, expand IP Routing, RIP; and then right-click one of the available interfaces and click Properties.

The General tab enables you to configure the operation mode. You can select either Autostatic Update Mode or Periodic Update Mode. With autostatic update, RIP announcements are sent when other routers request updates. Any routes learned while in autostatic update mode are marked as static and remain in the routing table until the administrator manually deletes them. In periodic update mode, announcements are sent out periodically. (The Periodic Announcement Interval determines how often.) These routes are automatically deleted when the router is stopped and restarted. The outgoing and incoming packet protocol enables you to configure the type of packets, such as RIPv1 or RIPv2, the router sends and accepts.

The Activate Authentication and Password options enable you to maintain an added level of security. If authentication is enabled, all outgoing and incoming packets must contain the password specified in the password field. When using authentication, make sure that all neighboring routers are configured with an identical password.

From the Security tab, an administrator can configure RIP route filters. The router can be configured to send and accept all routes, send and accept only routes from the ranges specified, or accept and send all routes except for those specified.

The Neighbors tab is used to configure how the router interacts with other RIP routers. The Advanced tab has several configurable options:

- **Periodic Announcement Interval**: Controls the interval at which periodic update announcements are made.
- **Time Before Route Expires**: Determines how long a route remains in the routing table before it expires.
- **Time Before Route Is Removed**: Determines how long an expired route remains in the routing table before being removed.
- **Enable Split Horizon Processing**: Ensures that routing loops do not occur because the routes learned from a router are not rebroadcast to that network.
Enable Triggered Updates: Controls whether changes in the routing table are sent out immediately.

Send Clean-Up Updates when Stopped: Controls whether the router sends an announcement when it is stopped to notify other routers that the routes for which it was responsible are no longer available.

Process Host Routes in Received Announcements: Controls whether host routes received in RIP announcements are accepted or denied.

Include Host Routes in Send Announcements: Controls whether host routes are included in RIP announcements.

Process Default Routes in Received Announcements: Controls whether default routes received in RIP announcements are accepted or denied.

Process Default Routes in Send Announcements: Controls whether default routes are included in RIP announcements.

Disable Subnet Summarization: This option is available only for RIPv2. It controls whether subnets are advertised to routers on different subnets.

EXAM ALERT
When a routing loop occurs, packets bounce back and forth between routers. When split-horizon processing is enabled, routes are not advertised back to the router from which they are learned. For example, if RouterB receives advertised routes from RouterA, RouterB does not advertise these routes back to RouterA. When Split Horizon with Poison Reverse is enabled, routes are advertised back to the router from which they were learned with a hop count of infinity.

Packet Filters
Packet filtering enables an administrator to specify the type of inbound and outbound traffic that is allowed to pass through a Windows Server 2008 router. When configuring packet filters, you can allow all traffic except traffic prohibited by filters. Or you can deny all traffic except traffic that is allowed by filters.

To add a packet filter, follow these steps:


2. In the console tree, click General under Routing and Remote Access/Server Name/[IPv4 or IPv6].
3. In the details pane, right-click the interface on which you want to add a filter, and then click Properties.

4. On the General tab, click either Inbound Filters or Outbound Filters.

5. In the Inbound Filters or Outbound Filters dialog box, click New.

6. In the Add IP Filter dialog box, type the settings for the filter, and then click OK.

7. In Filter action, select the appropriate filter action, and then click OK.

After a packet filter is created, you can edit it at any time by selecting the filter from the list and clicking Edit.

**Windows Firewall**

*Windows Firewall* is a packet filter and stateful host-based *firewall* that allows or blocks network traffic according to the configuration. A packet filter protects the computer by using an access control list (ACL), which specifies which packets are allowed through the firewall based on IP address and protocol (specifically the port number). A *stateful firewall* monitors the state of active connections and uses the information gained to determine which network packets are allowed through the firewall. Typically, if the user starts communicating with an outside computer, it remembers the conversation and allows the appropriate packets back in. If an outside computer tries to start communicating with a computer protected by a stateful firewall, those packets are dropped automatically unless access was granted by the ACL.

**EXAM ALERT**

*Windows Firewall* is on by default. Any program or service that needs to communicate on a network must be opened in a firewall, including sharing files, pinging the server, or providing basic services, such as DNS and DHCP.

Compared to Windows Firewall introduced with Windows XP SP2, the Windows Firewall used with Windows Server 2008 has some major improvements, including the following:

- Windows Firewall supports IPv6 connection filtering.
- By using outbound packet filtering, you can help protect the computer against spyware and viruses that attempt to contact outside computers.
With the advanced packet filter, rules can also be specified for source and destination IP addresses and port ranges.

Rules can be configured for services by the service name chosen from a list, without needing to specify the full path filename.

IPSec is fully integrated with Windows Firewall, allowing connections to be allowed or denied based on security certificates, Kerberos authentication, and so on. Encryption can also be required for any kind of connection.

A new management console snap-in named Windows Firewall with Advanced Security provides access to many advanced options and enables remote administration.

You can use separate firewall profiles for when computers are domain-joined or connected to a private or public network.

**Basic Configuration**

Windows Firewall is on by default. When Windows Firewall is on, most programs are blocked from communicating through the firewall. If you want to unblock a program, you can add it to the Exceptions list (on the Exceptions tab). For example, you might not be able to send photos in an instant message until you add the instant messaging program to the Exceptions list. To add a program to the Exceptions list, click the Add program button and select it from the available list or browse for it by clicking the Browse button.

To turn on or off Windows Firewall, follow these steps:

1. Open Windows Firewall by clicking the Start button, clicking Control Panel, clicking Security, and then clicking Windows Firewall.

2. Click Turn Windows Firewall On or Off (see Figure 5.3). If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
If you want the firewall to block everything, including the programs selected on the Exceptions tab, select the Block All Incoming Connections check box. Block All Incoming Connections blocks all unsolicited attempts to connect to your computer. Use this setting when you need maximum protection for your computer, such as when you connect to a public network in a hotel or airport, or when a computer worm is spreading over the Internet. With this setting, you are not notified when Windows Firewall blocks programs, and programs on the Exceptions list are ignored.

The Windows Firewall Settings interface has three tabs:

- **General**: Enables you to turn Windows Firewall on and off, as well as to block all incoming connections, no matter how you have configured the exceptions.

- **Exceptions**: Enables you to configure programs and ports for which you want to allow communication into and out from your Windows Vista computer. Only create an exception that is specifically required, and remove exceptions that you no longer need. Never create an exception for a program when you are unsure of the functionality of that program.

- **Advanced**: Enables you to select the network interfaces that you want Windows Firewall to protect.
To configure programs as exceptions,


2. Click Allow a program through Windows Firewall. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

3. In the Windows Firewall dialog box, select the Exceptions tab and then click Add Program.

4. In the Add A Program dialog box, select the program in the Programs list or click Browse to use the Browse dialog box to find the program.

5. By default, any computer, including those on the Internet, can access this program remotely. To restrict access further, click Change Scope.

6. Click OK three times to close all open dialog boxes.

To open a port in Windows Firewall,

1. Open Windows Firewall by clicking the Start button, clicking Control Panel, clicking Security, and then clicking Windows Firewall.

2. Click Allow a program through Windows Firewall. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

3. Click Add port.

4. In the Name box, type a name that will help you remember what the port is used for.

5. In the Port number box, type the port number.

6. Click TCP or UDP, depending on the protocol.

7. By default, any computer, including those on the Internet, can access this program remotely. To change scope for the port, click Change scope, and then click the option that you want to use. (“Scope” refers to the set of computers that can use this port opening.)

8. Click OK two times to close all open dialog boxes.
Windows Firewall with Advanced Security

Similar to the Windows Firewall with Advanced Security introduced in Windows Vista, the Windows Firewall with Advanced Security in Windows Server 2008 is a Microsoft Management Console (MMC) snap-in that allows you to set up and view detailed inbound and outbound rules and integrate with Internet Protocol security (IPSec).

The Windows Firewall with Advanced Security management console enables you to configure:

- **Inbound rules**: Windows Firewall will block all incoming traffic unless solicited or allowed by a rule.

- **Outbound rules**: Windows Firewall will allow all outbound traffic unless blocked by a rule.

- **Connection security rules**: Windows Firewall uses a connection security rule to force two peer computers to authenticate before they can establish a connection and to secure information transmitted between the two computers. Connection security rules use IPsec to enforce security requirements. Connection security rules will be explained more in the next chapter.

- **Monitoring**: Windows Firewall uses the monitoring interface to display information about current firewall rules, connection security rules, and security associations.

Windows Firewall is on by default. When Windows Firewall is on, most programs are blocked from communicating through the firewall. If you want to unblock a program, you can add it to the Exceptions list (on the Exceptions tab). For example, you might not be able to send photos in an instant message until you add the instant messaging program to the Exceptions list. To add a program to the Exceptions list, see Allow a program to communicate through Windows Firewall.

To turn on or off Windows Firewall:


2. Click the Windows Firewall Properties.

3. Under Firewall state, Select either On (recommended) or Off (not recommended) and click the OK button. See Figure 5.4.
Chapter 5: Routing and Filtering Network Traffic

Creating Inbound and Outbound Rules

You create inbound rules to control access to your computer from the network. Inbound rules can prevent

- Unwanted software being copied to your computer
- Unknown or unsolicited access to data on your computer
- Unwanted configuration of your computer from remote locations

To configure advanced properties for a rule using the Windows Firewall with Advanced Security, follow these steps:

1. Right-click the name of the inbound rule and click Properties.
2. From the properties dialog box for an inbound rule, configure settings on the following tabs:
   - **General**: The rule’s name, the program to which the rule applies, and the rule’s action (allow all connections, allow only secure connections, or block).
Windows Firewall

- **Programs and Services**: The programs or services to which the rule applies.

- **Users and Computers**: If the rule’s action is to allow only secure connections, the computer accounts that are authorized to make protected connections.

- **Protocols and Ports**: The rule’s IP protocol, source and destination TCP or UDP ports, and ICMP or ICMPv6 settings.

- **Scope**: The rule’s source and destination addresses.

- **Advanced**: The profiles or types of interfaces to which the rule applies.

You can also use the Windows Firewall with Advanced Security to create outbound rules to control access to network resources from your computer. Outbound rules can prevent:

- Utilities on your computer accessing network resources without your knowledge.

- Utilities on your computer downloading software without your knowledge.

- Users of your computer downloading software without your knowledge.

**Determining a Firewall Profile**

A firewall profile is a way of grouping settings, such as firewall rules and connection security rules that are applied to the computer, depending on where the computer is connected. On computers running this version of Windows, there are three profiles for Windows Firewall with Advanced Security. Only one profile is applied at a time.

The available profiles are

- **Domain**: Applied when a computer is connected to a network in which the computer’s domain account resides.

- **Private**: Applied when a computer is connected to a network in which the computer’s domain account does not reside, such as a home network. The private settings should be more restrictive than the domain profile settings.
Public: Applied when a computer is connected to a domain through a public network, such as those available in airports and coffee shops. The public profile settings should be the most restrictive because the computer is connected to a public network where the security cannot be as tightly controlled as within an IT environment.

Using netsh Command to Configure the Windows Firewall

To view the current firewall configuration, including ports that have been opened, use the following command:

netsh firewall show state

NOTE

If the Firewall status shows that the Operational mode is set to Enable, this means that the Windows Firewall is enabled but no specific ports have been opened.

To open ports at the firewall for DNS (port 53), use the following command:

netsh firewall add portopening ALL 53 DNS-server

To view the firewall configuration, use the following command:

netsh firewall show config

To enter the netsh advfirewall context, at the command prompt, type

netsh

When you enter the netsh context, the command prompt displays the >netsh prompt. At the >netsh prompt, enter the advfirewall context type:

advfirewall

After you are in the advfirewall context, you can type commands in that context. Commands include the following:

- Export: Exports the current firewall policy to a file.
- Help: Displays a list of available commands.
- Import: Imports a policy from the specified file.
Network Address Translation

- **Reset**: Restores Windows Firewall with Advanced Security to the default policy.

- **Set**: Supports the following commands:
  - `set file`: Copies the console output to a file.
  - `set machine`: Sets the current machine on which to operate.
  - `show`: Shows the properties for a particular profile. Examples include `show allprofiles`, `show domainprofile`, `show privateprofile` and `show publicprofile`.

In addition to the commands available for the `advfirewall` context, `advfirewall` also supports several subcontexts. To enter a subcontext, type the name of the subcontext at the `netsh advfirewall>` prompt. The available subcontexts are

- **consec**: Enables you to view and configure computer security connection rules
- **Firewall**: Enables you to view and configure firewall rules
- **Monitor**: Enables you to view and set monitoring configuration

Managing Windows Firewall with Advanced Security via Group Policy

To centralize the configuration of large numbers of computers in an organization network that uses the Active Directory directory service, you can deploy settings for Windows Firewall with Advanced Security through Group Policy. Group Policy provides access to the full feature set of Windows Firewall with Advanced Security, including profile settings, rules, and computer connection security rules.

Network Address Translation

Because IPv4 addresses are a scare resource, most ISPs provide only one address to a single customer. In majority of cases, this address is assigned dynamically, so every time a client connects to the ISP, a different address is provided. Big companies can buy more addresses, but for small businesses and home users, the cost of doing so is prohibitive. Because such users are given only one IP address, they can have only one computer connected to the Internet at one time.
NAT Overview

Network address translation (NAT) technology was developed to provide a temporary solution to the IPv4 address-depletion problem. NAT is a method of connecting multiple computers to the Internet (or any other IP network) using just one IP address. With a NAT gateway running on this single computer, it is possible to share that single address between multiple local computers and connect them all at the same time. The outside world is unaware of this division and thinks that only one computer is connected.

To combat certain types of security problems, a number of firewall products are available. These are placed between the user and the Internet to verify all traffic before allowing it to pass through. This means, for example, that no unauthorized user is allowed to access the company's file or email server.

NAT automatically provides firewall-style protection without any special setup. The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address. The TCP/IP protocols include a multiplexing facility so that any computer can maintain multiple simultaneous connections with a remote computer. For example, an internal client can connect to an outside FTP server, but an outside client cannot connect to an internal FTP server because it would have to originate the connection and NAT does not allow that. It is still possible to make some internal servers available to the outside world via inbound mappings, which map certain well known TCP ports (for example, 21 for FTP) to specific internal addresses, thus making services such as FTP or web available in a controlled way.

A modern NAT gateway must change the source address on every outgoing packet to be its single public address. It therefore also renumbers the source ports to be unique, so that it can keep track of each client connection. The NAT gateway uses a port mapping table to remember how it renumbered the ports for each client's outgoing packets. The port mapping table relates the client's real local IP address and source port plus its translated source port number to a destination address and port. The NAT gateway can therefore reverse the process for returning packets and route them back to the correct clients.
Enabling NAT

To enable NAT addressing, follow these steps:

2. To add NAT, right-click General under IPv4 and select New Routing Protocol. Select NAT and click OK.
3. In the console tree, click NAT under IPv4.
4. Right-click NAT and then click Properties.
5. On the Address Assignment tab, select Automatically Assign IP Addresses by Using the DHCP Allocator check box.
6. (Optional) To allocate to DHCP clients on the private network, in IP address and Mask, configure the range of IP addresses.
7. (Optional) To exclude addresses from allocation to DHCP clients on the private network, click Exclude, click Add, and then configure the addresses.

To specify the internal and external interfaces, right-click NAT under IPv4 and select New Interface. Select the physical interface and click OK. Specify either Private Interface Connected to the Private Network or Public Interface Connected to the Internet. If you select Public Interface Connected to the Internet, you would then select Enable NAT on This Interface. Click OK.

To forward a protocol to a specific internal server through the NAT server, follow these steps:

1. Right-click the public interface and select Properties.
2. Select the Services and Ports tab.
3. Select the protocol that you want to forward.
4. When the Edit Services dialog box appears, specify the private address and click OK to close the Edit Services dialog box.
5. Click OK to close the Properties dialog box.
**NAT and Teredo**

IPv6 traffic that is tunneled with Teredo is not subject to the IPv4 packet filtering function of typical NATs. Although this might sound like Teredo is bypassing the NAT and allowing potentially malicious IPv6 traffic on private networks, consider the following:

- Teredo does not change the behavior of NATs. Teredo clients create dynamic NAT translation table entries for their own Teredo traffic. The NAT forwards incoming Teredo traffic to the host that created the matching NAT translation table entry. The NAT does not forward Teredo traffic to computers on the private network that are not Teredo clients.

- Teredo clients that use a host-based, stateful firewall that supports IPv6 traffic (such as Windows Firewall) are protected from unsolicited, unwanted, incoming IPv6 traffic. Windows Firewall is enabled by default for Windows XP with SP2, Windows Vista, and Windows Server 2008.

If you wish for Teredo to communicate through a Windows Server 2008 computer with the firewall enabled, you have to configure the firewall to allow the use of Teredo.
Exam Prep Questions

1. You have a Windows Server 2008 computer at the corporate office and a Windows Server 2008 computer at a remote site. You want to configure the routing on the server at the branch office. What should you do?
   ❍ A. Install the Routing and Remote Access role and enable the IPv4 LAN routing.
   ❍ B. Run the `netsh interface ipv4 enable` command.
   ❍ C. Enable NAT by executing the `netsh NAT enable` command.
   ❍ D. Install the NPS role on the server.

2. You have a Windows Server 2008 server. You need to add a new static route to the routing table on the server. The new route is to the network ID 192.168.126.0 with a subnet mask of 255.255.255.0, using the default gateway of 192.168.125.1. What command do you need to execute?
   ❍ A. `route -p 192.168.126.0 mask 255.255.255.0 192.168.125.1 metric 2`
   ❍ B. `route add 192.168.126.0 mask 255.255.255.0 192.168.125.1 metric 2`
   ❍ C. `route add 192.168.126.0 255.255.255.0 192.168.125.1 metric 2`
   ❍ D. `route add 192.168.126.0 mask 255.255.255.0 gateway 192.168.125.1 metric 2`

3. You have a network with several subnets. Windows Server 2008 routers are used to connect the subnets. You need to configure a static route. The static router must not be deleted from the routing table if the computer is restarted. Which of the following parameters should you use with the `route` command?
   ❍ A. `/f`
   ❍ B. `/s`
   ❍ C. `/r`
   ❍ D. `/p`

4. You have a server that runs Windows Server 2008. You need to prevent the server from establishing communication sessions to other computers by using TCP port 21. What should you do?
   ❍ A. From Windows Firewall, add an exception.
   ❍ B. From Windows Firewall, enable the Block All Incoming Connections option.
5. You have a Windows Server 2008 computer. You want to disable all incoming connections to the server. What should you do?

- A. From the Services snap-in, disable the Server service.
- B. From the Services snap-in, disable the Net Logon service.
- C. Disable the Windows Firewall with Advanced Security.
- D. From the Windows Firewall, enable the Block All Connections option on the Domain Profile.

6. Your internetwork consists of seven subnets. All subnets are connected by Windows Server 2008 computers with RRAS. Nonpersistent demand-dial connections have been configured. You do not want to be burdened with updating the routing tables, and you want any changes to the network topology to be propagated immediately. Which of the following routing options should you implement?

- A. Static routes
- B. ICMP
- C. OSPF
- D. RIPv2

7. The network consists of three different subnets. Dynamic routing is being implemented on three multihomed computers running Windows Server 2008 on which Routing and Remote Access has been enabled. You open the Routing and Remote Access console on the first server and configure the computer for LAN routing. You select New Routing Protocol from the General node of the IP Routing node, and you choose RIP version 2 for Internet Protocol from the New Routing Protocol dialog box. What should you do next?

- A. Add the IP address of the DHCP server to the properties dialog box for the DHCP Relay Agent.
- B. Add the interface that RIP will run, using the RIP node.
- C. Use the route command to configure the routes to the remote subnets.
- D. Use the route command to delete all static routers from the routing tables.
8. You are the network administrator for your company. All servers are running Microsoft Windows Server 2008. Several of the servers are configured as routers with RIP enabled. You want to eliminate any routing loops from occurring. You open the properties window for the interface assigned to the RIP protocol and select the Advanced tab. Which of the following options meets these requirements?

- **A.** Enable split-horizon processing.
- **B.** Enable triggered updates.
- **C.** Process host routes in received announcements.
- **D.** Disable subnet summarization.

9. You have a network with several Windows Server 2008 computers. Your company has opened a new remote office. You are in charge of configuring a two-way demand-dial connection between your corporate office and the new remote office. You configure the demand-dial routers with the following settings:

Corporate Office Router Settings:

- **Interface:** SRV02_Public
- **User Account:** SRV02
- **Calling Number:** 555-3434

Site Router Settings:

- **Interface:** SRV01_Public
- **User Account:** SRV01
- **Calling Number:** 555-1212

When you go to test your configuration, neither of the routers can establish a connection. What should you do?

- **A.** Change the interface name on the router in the head office to SRV01_Public.
- **B.** Change the demand-dial interface name on each router to match the name of the user account on the remote answering router.
- **C.** Change the interface name on the router in the branch office to SRV02_Public.
- **D.** Change the names assigned to the user accounts on each router so they are identical.
Chapter 5: Routing and Filtering Network Traffic

10. You have a Windows Server 2008 configured as a NAT server. You need to ensure that administrators can access a server named FS1 by using FTP. What should you do?

- A. Configure NAT1 to forward ports 20 and 21 to FS1.
- B. Configure NAT1 to forward ports 80 and 443 to FS1.
- C. Configure NAT1 to forward port 25 to FS1.
- D. Configure NAT1 to forward port 3389 to FS1.

11. You have a Windows Server 2008 computer with IPv4 and IPv6 and NAT at the corporate office and each of your site offices. What do you need to allow IPv6 computers from the corporate office and the various sites to use Teredo to communicate with each other?

- A. Configure dynamic NAT on the firewall.
- B. Configure the firewall to allow the use of Teredo.
- C. Enable a static route between the two networks.
- D. Load the Teredo emulator.

Answers to Exam Prep Questions

1. Answer A is correct. You need to install the Routing and Remote Access role and you then need to enable IPv4 LAN routing. Answer B is incorrect because the `netsh` command is not used to enable routing; instead, it could be used to configure a network interface. Answer C is incorrect because NAT would not enable routing and you do not use the `netsh` command to enable NAT. Answer D is incorrect because NPS does not enable routing. NPS is used as a RADIUS server and for implementing RAS policies.

2. Answer B is correct. The correct syntax when adding new static routes using the `route` command is `route add mask metric`. Answers A, C, and D are incorrect because they do not use the proper syntax.

3. Answer D is correct. You use the `/p` parameter to add a persistent route to the routing table. The route is not removed from the routing table when the router is restarted. Therefore, answers A, B, and C are incorrect.

4. Answer D is correct. You need create an outbound rule using the Windows Firewall with Advanced Security snap-in to block port 21. Answers A and B are incorrect because you should be using the Windows Firewall with Advanced Security snap-in with Windows Server 2008 computers for the fine control that it offers over standard Windows Firewall. In addition, an exception would be used to allow traffic, and if you block all incoming connections, other protocols would also be blocked and no traffic
would be able to go through the server. Answer C is incorrect because you want an outbound rule, not an inbound rule because the traffic from this server to the other servers would be outbound.

5. Answer D is correct. You could quickly open the Windows Firewall, and enable Block All Connections to disable all incoming connections. The Domain profile is applied when a computer is connected to a network in which the computer's domain account resides. Answer A is incorrect because the Server service stops file and print sharing. The Net Logon service prevents logins but not necessarily all connections. Answer C is incorrect because disabling a firewall allows all traffic to flow.

6. Answer D is correct. To have changes propagated throughout the network when changes occur and to reduce the administrative overhead associated with updating the routing tables, a routing protocol is required. Because OSPF cannot be used with non-persistent connections and OSPF is not available in Windows Server 2008, RIPv2 must be used. Therefore, answers A and C are incorrect. Answer B is incorrect because ICMP is not a routing protocol.

7. Answer B is correct. You should use the context menu of the Routing Interface Protocol (RIP) node to add at least one interface to RIP. When you add a routing protocol, the protocol is not configured by default to use an interface, so you must identify one or more interfaces, such as a LAN connection, that the protocol can use. Answer A is incorrect because the scenario does not indicate that there is a DHCP server on the network. Answer C is incorrect because the routing tables are built automatically. Answer D is incorrect because there is no need to remove all static routes from the routing table.

8. Answer A is correct. The correct answer is enable split-horizon processing. You must select this option to ensure that any routes learned from a network are not sent as RIP announcements on the network. With this option enabled, a router cannot advertise a route on the same connection from which it was learned. Answers B, C, and D do not help eliminate routing loops.

9. Answer B is correct. You must change the user account name on each router to match that of the name assigned to the demand-dial interface name on the answering routing. For a two-way demand-dial connection to work, the user account names used for authentication must be identical to the name assigned to the demand-dial interface. The name of the demand-dial interface on the branch office router must be changed to SRV02. The name of the demand-dial interface on the head office routing must be changed to SRV01. Answer D is incorrect because the user accounts used for remote authentication between the demand-dial routers do not need to be identical. Answers A and C are incorrect because the demand-dial interface name on the calling router must be identical to the user account name on the calling router.

10. Answer A is correct. You need to forward the port 20 and 21 to FS1. Ports 20 and 21 are the ports used by FTP. Answer B is incorrect because port 80 and 443 are used by web servers. Answer C is incorrect because port 25 is used for SMTP. Answer D is incorrect because port 3389 is used by Remote Desktop Protocol.
11. Answer B is correct. By default, the firewall is started and Teredo is blocked. Answer A is incorrect because you already have NAT. Answer C is incorrect because there are already routes between the sites. Answer D is incorrect because there is no such thing as a Teredo emulator.

Need to Know More?


For more information about Windows Firewall with Advanced Security and IPSec, visit the following website:


For more information on Teredo, view the following website:


Index

Numerics

3Com IP address white paper website, 123
6to4 addresses, 100
80/20 rule, 201
802.1X
   enforcement (NAP), 286
   RADIUS servers, configuring, 293-294

A

A (Host Address) records, 135
AAA (Host Address) records, 135
access
   dial-up, 248
      authentication protocols, 249-252
      logging, 260-262
      NPS as RADIUS client, 257-258
      NPS server registration, 259-260
      RADIUS, 255-257, 261-262
      remote access clients, 248-249
      remote access server, configuring, 253-255
   IPSec, 262
      configuring with Windows
         Firewall with Advanced Security, 268-271
      driver, 264
      implementing, 264-266
      modes, 262-264
      Monitor tool, 272-274
      policies, creating, 265-266
      policy agents, 264
      policy configuration, 266-268
      protocols, 263
      tunnels, configuring, 266
      website, 303
   NAP, 280-281
      enforcement methods, 285-286
      NPS, 281-283
      SHVs, 283-285
      previous versions of shadow copies, 349-350
      printers, modifying, 401
      public folders, 317
      shared folders, 322-323
   VPNs
      configuring, 277-280
      overview, 274
      protocols, 275-276
      remote access, 275
      site-to-site, 275
      website, 303
   wireless, 286
      adapters, 287-289
      certificates, 292-293
      configuring, 289-290
      encryption, 288
      managing, 291-292
      personal mode, 288
      policies, configuring, 295
      RADIUS servers, configuring, 293-294
      standards, 287

accessing Control Panel, 46
Active Directory
   BitLocker Drive Encryption recovery
      information, 333
   printers, listing, 387
Active Directory integrated zones, 131-134, 144
   updates, 162
AD DS (Active Directory Domain Services), 259-260
Add Printer dialog box, 383
Add Printer Wizard, local printers, 383
adding
- DHCP Relay Agent, 198-199
- fault tolerance to DHCP, 201

addresses
- 6to4, 100
- classful, 77-81
- global unicast, 97-98
- IP, 75
  - anycast, 94
  - broadcast, 94
  - CIDR, 86-90
  - classes, 77-78
  - configuring with GUI interface, 104, 106-107
  - configuring with netsh command, 107-108
  - multicasting, 94
  - NAT, 90-92
  - planning, 82-86
  - proxy servers, 92-93
  - ranges, 82
  - resources, 123
  - unicast, 93
- IPv4, 77, 100
  - configuring, 104
- IPv6, 96-97
  - configuring, 105
  - global unicast, 97-98
  - link local unicast, 98-99
  - migration from IPv4, 100-101
  - multicast, 99
- ISATAP, 100
  - link local unicast, 98-99
- MAC, 75
  - multicast, 94
  - IPv6, 99
  - network, classful addresses, 78-79
  - private networks, 79
  - teredo, 101

ADMIN$ shared folder, 321
administrative shared folders, 321-322
Administrative Tools, 47
  - Computer Management Console, 48-49

adapters, wireless, 287-289
AH (Authentication Header), 263
alert actions, configuring, 59
algorithms
  - distance-vector, 215
  - dynamic routing, 215
  - link-state, 216
  - static routing, 215
aliases, Network Monitor, 432-433
all option (ipconfig command), 110-111
anxiety, dealing with, 37-38
anycast addresses, 94
application log, 52
Applications and Services Logs, 51
ARIN (American Registry for Internet Numbers), 83
ARP (Address Resolution Protocol), 75
arp -a command, 77
arp tables, viewing, 77
assigning NTFS permissions, 307-310
asynchronous backups, 203
authentication
  - certificates, wireless connections, 292-293
  - protocols, 249-250
    - CHAP, 251-252
    - EAP, 252
    - MS-CHAPv2, 252
    - PAP, 251
    - PEAP, 252
  - RADIUS, 255
    - enabling, 257
    - proxies, 256
Authentication Methods tab (IPSec policy Properties window), 267
authorizing DHCP server, 199, 201
AutoPlay dialog box, 290

backing up
  - DHCP database, 203
  - encryption certificates, 327
  - WINS databases, 172
Backup Once Wizard, 356
Backup Schedule Wizard, 356
clients

backups
catalogs, 359-360
creating, 352
GFS rotation, 354
resources, 376
types, 353-354
wbadmin command, 358-359
Windows Server Backup, 354
  scheduling, 356-358
  server backups, 355
  snap-in, 355
  storage, 357
tools, installing, 355
  volumes, 356
BACP (Bandwidth Allocation Control Protocol), 254
BAP (Bandwidth Allocation Protocol), 254
binary number systems, 489, 491-492
BIND (Berkeley Internet Name Domain), 127
bindings, 197-198
BitLocker Drive Encryption
disabling, 332
EFS, compared, 325
enabling, 332
overview, 329-333
recovery information, 333
system requirements, 331
TPM, 329-331
website, 376
BitLocker Drive Encryption dialog box, 332
BitLocker setup wizard, 332
biz domains, 128
BOOTP
  DHCP, 188
    client reservation, 193
    conflict detection, 193-194
    installing, 190
    new features, 189
    options, 194-195
    vendor classes, creating, 196-197
    requests, 189
    scope, defining, 190-193
broadcast addresses, IP addresses, 94
Browse for Folder dialog box, 322
burst handling (WINS), 165
business domains, 128

caching-only DNS servers, 132, 146
cancelling print jobs, 398
Canonical Name (CNAME) records, 135
capture options (Network Monitor), 435
capture sessions, creating/saving, 431
Catalog Recovery Wizard, 360
catalogs (backup), 359-360
CBCP (Callback Control Protocol), 249
Certificate Export Wizard, 328
Certificate Import Wizard, 329
certificates
  encryption
    adding to shared files, 329
    backing up, 327
    exporting, 328
    importing, 329
  wireless connections, 292-293
certification, qualifications for candidates, 26-27
  educational background, 28
  experience needed, 29-30
Certification Mode, 497
CHAP (Challenge Handshake Authentication Protocol), 251-252
CIDR (Classless Internetwork Domain Routing), 86
  address blocks, 87
  defined, 86
  VLSM, compared, 88
Cisco Corporation domain, 128
classful addresses, 77-78
  host address identification, 78-79
  network address identification, 78-79
  subnetting, 80-81
client reservation (DHCP), 193
clients
  dial-up remote access, 248-249
  NAP, 281
  NFS, starting, 362
WINs, 166-167  
WSUS, configuring, 419-422

CMAK (Connection Manager Administration Kit), 279
installing, 280  
VPNs, configuring, 279-280

CNAME (Canonical Name) records, 135

com domains, 128

commands
arp -a, 77
ipconfig, troubleshooting IP addresses, 110-111
mount, 363
NBTSTAT, 174
netsh
  IP address configuration, 107-108
  resources, 123
netstat, troubleshooting IP addresses, 115
ntbackup, 355
pathping, 114
ping, troubleshooting IP addresses, 111-112
route, static route configurations, 221-222
tracert
  IP addresses, troubleshooting, 113-114
  options, 113
  wbadmin, 355, 358-359

commercial domains, 128

components of DFS namespaces, 336

compression
NTFS, 334
zipping folders, 333

Computer Management Console, 48-49

conditional forwarders, 139

configuring
clients for WSUS, 419-422
demand-dial routing, 226
dial-up remote access servers, 253-255
  authentication methods, 255
  ports, 254
  PPP options, 254
disk quotas, 360

DNS
  dynamic updates, 152
  suffix searches, 156

DNS servers, 146, 160
forwards, 153
IP addresses
  with GUI interface, 104-107
  with netsh command, 107-108

IPSec
  policies, 266-268
  tunnels, 266
  with Windows Firewall with Advanced Security, 268-270
IPv4 addresses, 104
IPv6 addresses, 105
name server lists, 151-152
network policies, 282
Performance Monitor alert actions, 59
printers, 389, 401
public folder sharing, 317
RADIUS servers, 802.1X
wireless/wired connections, 293-294
root hints, 153
Server Core resources, 123
services, 50
SHVs, 284

SNMP
  agent properties, 425-426
  security, 427-428
  traps, 426
SOA records, 148
static routes, 220
  route command, 221-222
  RRAS management console, 223-224

VPNs, 277-278
  CMAK, 279-280
  with network connections, 278-279
Windows Firewall, 230-232
WINs replication, 171
wireless connections, 289-290
USB drives, 290
wireless policies, 295
zone transfers, 151-152
conflict detection (DHCP), 193-194
Connection Security Properties dialog box, 269
Connection Security Rule wizard, 269
Connection Type tab (IPSec policy Properties window), 268
connections
demand-dial, 224
configuring, 226
one-way, 224-225
two-way, 225
DFS Replication, creating, 343-344
printers, deploying, 386-387
consoles
DNS Manager, 145
advanced options, 154-155
caching-only DNS servers, creating, 146
DNS servers, configuring, 146
dynamic updates, 152
forward/reverse lookup zones, 147
forwarders, 153
name server lists, configuring, 151-152
resource records, adding, 149
resource records, scavenging, 150-151
root hints, 153
SOA records, configuring, 148
subdomains, creating, 148
zone replication scopes, 154
zone transfers, configuring, 151-152
Print Management, 402-404
RRAS, static route configurations, 223-224
Windows Firewall with Advanced Security, 233
configurations, viewing, 236-237
inbound/outbound rules, 234-235
managing, 237
profiles, 235
WINS, 169-170
database backups, 172
database compaction, 173
database consistency, 173
NetBIOS name resolution, 174
replication, configuring, 171
server statistics, 172
tombstoning, 172-173
contacting technical support, 500
contributor permission, 319
Control Panel, 46-49
cooperative domains, 128
copy backups, 353
copying files, NTFS, 311-312
country domains, 128
Create New Health Policy dialog box, 284
creating
shortcut to MeasureUp practice test, 499
vendor classes, 196-197
Custom Mode, 498
Customize Start Menu, 323
Customize Start Menu dialog box, 323
-D
-d option, tracert command, 113
Data Properties dialog box, NTFS permissions, 309
databases, WINS
backing up/restoring, 172
compacting, 173
consistency, 173
DCHP Relay Agent, adding, 198-199
DCHP Server service
authorizing, 199, 201
bindings, 197-198
DCS (Data Collector Set), 56
creating for Performance Monitor, 58-59
decimal number systems, 489
decrypting files/folders, 327
default Event Viewer logs, 51-52
default gateways, 79
defining DHCP scope, 190-191
multicast scopes, 192-193
superscopes, 192
deleting resource records, 162
demand-dial connections, 224
  configuring, 226
  one-way, 224-225
  two-way, 225
Deploy with Group Policy dialog box, 386
deploying printer connections, 386-387
device drivers, digital signatures, 381
DFS (Distributed File System), 335
  Management snap-in, 335
  namespaces, 336-339
    adding servers to domain-based namespaces, 337
  components, 336
  creating, 336-337
  domain controller polling, 338
  folder targets, adding, 338
  folders, creating, 338
  hierarchy, 337
  referrals, 339
Replication, 339-347
  connections, creating, 343-344
  diagnostic reports, 347
  enabling/disabling, 344
  folder targets, 340
  folders, sharing, 344
  forcing, 344
  primary members, 341
  RDC, 340
  replication group members, adding, 342-343
  replication groups, creating, 340-341
  schedules, editing, 344
  topology, 345-346
DHCP (Dynamic Host Configuration Protocol), 141, 188
  client reservation, 193
  conflict detection, 193-194
  databases
    backing up, 203
    managing, 202
  fault tolerance, adding, 201
  installing, 190
  JetPack program, launching, 202-203
  logging, enabling, 202
  multihomed servers, 197
  new features, 189
  options, 194-195
    vendor classes, creating, 196-197
  performance counters, 205
  requests, 189
  scope, defining, 190-191
    multicast scopes, 192-193
  superscopes, 192
  troubleshooting, 203-204
DHCP enforcement (NAP), 285
dhcploc.exe command, 200
diagnostic reports, DFS Replication, 347
dial-up networking, 248
  authentication protocols, 249-250
    CHAP, 251-252
    EAP, 252
    MS-CHAPv2, 252
    PAP, 251
    PEAP, 252
  logging, 260-262
  NPS
    as RADIUS client, 257-258
    server registration, 259-260
  RADIUS, 255
    accounting, 261-262
    enabling, 257
    proxies, 256
  remote access clients, 248-249
  remote access server, configuring, 253
  authentication methods, 255
  ports, 254
  PPP options, 254
dialog boxes
  Add Printer, 383
  AutoPlay, 290
  BitLocker Drive Encryption, 332
  Browse for Folder, 322
  Connection Security Properties, 269
  Create New Health Policy, 284
  Data Properties, NTFS permissions, 309
  Deploy with Group Policy, 386
Map Network Drive, 322
Specify Access Permissions, 283
Windows Firewall with Advanced Security Properties, 270
Windows Security, file/folder ownership, 313
differential backups, 353
digital signatures, device drivers, 381
disabling
BitLocker Drive Encryption, 332
DFS Replication, 344
disk quotas, NTFS, 360-361
distance-vector algorithms, 215
Distributed File System. See DFS
DNS (Domain Name System), 76, 127
BIND, 127
countries, 128
defined, 127
domains, 127
dynamic, 140-142, 152
forwarders, configuring, 153
FQDNs, 130
Manager console, 145
    advanced options, 154-155
    caching-only DNS servers, creating, 146
    DNS servers, configuring, 146
dynamic updates, 152
forward/reverse lookup zones, 147
forwarders, 153
name server lists, configuring, 151-152
resource records, adding, 149
resource records, scavenging, 150-151
root hints, 153
SOA records, configuring, 148
subdomains, creating, 148
zone replication scopes, 154
zone transfers, configuring, 151-152
monitoring/troubleshooting
DnsCmd, 159-163
DNSLint, 158
NSLookup, 157
name resolution process, 137
conditional forwarders, 139
forwarders, 139
LLMNR, 140
recursive/iterative queries, 137-138
reverse queries, 140
root hints, 139
round-robin, 140
name space, 127, 130
naming guidelines/conventions, 130
resource records, 135-136
adding, 149, 162
cache memory, 162
deleting, 162
scavenging, 150-151
root domains, 127
root hints, configuring, 153
second-level domains, 128
server configurations
    servers
        caching-only, 146
        configuring, 146, 160
        installing, 145
subdomains, 127-130, 148
suffix searches, 156
top-level domains, 127-128
zone transfers
    Active Directory, 144
    overview, 142-143
    security, 143-144
zones, 131
    Active Directory integrated, 131-134, 144, 162
    adding, 160
caching-only servers, 132
forward/reverse lookup, 147
GlobalNames, 175-176
replication scopes, 154
standard primary, 131-132
standard secondary, 131-132
stub, 131, 134
DNS (Domain Name System)

transfers, 131, 151-152
updates, 161
zone files, 134
Dnscmd utility, DNS monitoring/troubleshooting, 159-163
DNSLint utility, DNS monitoring/troubleshooting, 158
Domain Name System. See DNS
domain names, 76
domains, 127
  naming guidelines/conventions, 130
  root, 127
  second-level, 128
  subdomains, 129-130, 148
  suffix searches, 156
  top-level, 127-128
downstream servers, 417-418
Drive letter$ shared folder, 321
drivers
  digital signatures, 381
  IPSec, 264
  print, defined, 378
drives, mapping to shared files/folders, 322
dynamic DNS, 140-142, 152
Dynamic Host Configuration Protocol. See DHCP
dynamic routing algorithms, 215

E

EAP (Extensible Authentication Protocol), 252
editing DFS Replication group schedules, 344
edu domains, 128
educational background of Microsoft certification candidates, 28
educational domains, 128
EFS
  BitLocker Drive Encryption, compared, 325
certificates
    adding to shared files, 329
    backing up, 327
    exporting, 328
  importing, 329
decrypting, 327
file sharing, 328
file/folder encryption, 327
overview, 326-329
enabling
  BitLocker Drive Encryption, 332
  conflict detection, 193
  DFS Replication, 344
  DHCP logging, 202
  file sharing, 318
  NAT, 239
  public folder sharing, 317
  RADIUS, 257
  RRAs, 219
  shadow copies, 347-349
enclosed CD, installing, 498-499
encryption, 325-326
  BitLocker Drive Encryption, 325, 329-333
    disabling, 332
    enabling, 332
    recovery information, 333
    system requirements, 331
    TPM, 329-331
    website, 376
certificates, wireless connections, 292-293
EFS, 325-326, 328-329
certificates, 327-329
decrypting, 327
file sharing, 328
file/folder encryption, 327
files
  BitLocker Drive Encryption, 330
  EFS, 327
  wireless, 288
encryption certificates
  adding to shared files, 329
  backing up, 327
  exporting, 328
  importing, 329
errors, 52
ESP (Encapsulating Security Payload), 263
Event Collector, 53-55
event header information, 53
event logging, print spoolers, 400
Event Viewer
  default logs, 51-52
  Event Collector, 53-55
  event header information, 53
events, 52
exam, preparing for, 31-38
experience needed for Microsoft certification candidates, 29-30
explicit permissions, 310-311
exporting EFS certificates, 328
Extension Headers, IPv6, 95

failure audit events, 53
FAT (File Allocation Table), 306
FAT32, 306
fault tolerance, adding to DHCP, 201
FAX$ shared folder, 322
features, 42, 45
  of Server Core, 65
File Server Resource Manager, 362
file sharing
  access, 322-323
  EFS, 328
  managing, 323
  offline settings, 324-325
File Sharing Wizard, 320
file systems, 306
  DFS, 335
    Management snap-in, 335
    namespaces, 336-339
    Replication, 339-347
  FAT, 306
  FAT32, 306
  NFS, 362
    clients, starting, 362
    mount options, 362-363
  NTFS, 306
    compression, 334
    permissions, 307-313
    resources, 376
    resources, 376
files
  backups
    catalogs, 359-360
    creating, 352
    GFS rotation, 354
    resources, 376
    testing, 353
    types, 353-354
    wbadmin command, 358-359
    Windows Server Backup, 354-358
  compression, 333
    NTFS, 334
  zipping folders, 333
  copying/moving, NTFS permissions, 311-312
  encryption, 325-326
    BitLocker Drive Encryption, 325, 329-333
    EFS, 325-329
  ownership, 313
  sharing, 313-314
  zone, 134
filters
  Network Monitor, 433-435
  packet filters, 228-229
  printers, 403-404
firewalls
  stateful, 229
  Windows Firewall, 229-230
    configuring, 230-232
    new features, 229
    ports, opening, 232
    turning on/off, 230
  Windows Firewall with Advanced Security, 233
    configurations, viewing, 236-237
    inbound/outbound rules, 234-235
    managing, 237
    profiles, 235
folders
  backups
    catalogs, 359-360
    creating, 352
    GFS rotation, 354
folders

resources, 376
testing, 353
types, 353-354
wbadmin command, 358-359
Windows Server Backup, 354-358
compression, 333
    NTFS, 334
    zipping folders, 333
DFS namespaces, creating, 338
NTFS folder permissions, 308
ownership, 313
shadow copies, 347
    enabling, 347-349
    previous versions, accessing, 349-350
    VSSAdmin tool, 350-351
sharing, 313-314
    access, 322-323
    administrative shares, 321-322
    EFS, 328
    managing, 323
    network discovery/browsing, 314-316
    offline settings, 324-325
    public folders, 316-318
    replicated, 344
    special shares, 321-322
    standard, 318-320
forcing DFS Replication, 344
formatting
    IPv4 addresses, 77
    MAC addresses, 75
forward lookup zones, 147
forwarders, 139, 153
FQDNs (Fully Qualified Domain Names), 126, 130
full backups, 353
gateways, default, 79
GFS (grandfather, father, son) backup rotation, 354
global unicast addresses, 97-98
GlobalNames zones, 175-176
government domains, 128

GPMC, offline file sharing restrictions, 325
gpupdate command, 268
group policies, configuring wireless policies, 295
groups, replication
    creating, 340-341
    members, adding, 342-343
    schedules, editing, 344
GUI interface, IP address configuration, 104-107

-h option, tracert command, 113
headers, IPv6, 95
hexadecimal number systems, 493-495
hierarchy, DFS namespaces, 337
hops, 214
Host Address (A) records, 135
host addresses, classful addresses, 78-79
hostnames, 76
hosts, 74, 77
    IP address planning, 85
hosts bits, 81

IEEE (Institute of Electrical and Electronics Engineers), 75, 287
IEEE 802.11 (Wireless Network) Policies, 295
implementing IPSec, 264-266
importing EFS certificates, 329
inbound rules, Windows Firewall with Advanced Security, 234-235
incremental backups, 353
information events, 52
informational domains, 128
infrastructures (network)
    MBSA, 422
    Microsoft updates, 416
        approving, 419
        client configurations, 419-422
downstream servers, 417-418
    installing WSUS, 416-417
    managing WSUS, 418
Network Monitor
aliases, 432-433
capture options, 435
capture sessions, 431
filters, 433-435
installing, 431
overview, 429-430
packet captures, 435
placement, 430-431
SNMP, 423
agent properties, configuring, 425-426
communities, 424-425
community names, 424
installing, 425
overview, 423-425
security, configuring, 427-428
traps, 424
traps, configuring, 426
versions, 425
inherited permissions, 311
Initial Configuration Tasks window, 60
installing
CMAK, 280
DFS Management snap-in, 335
DHCP, 190
DNS servers, 145
enclosed CD, 498-499
Network Monitor, 431
printers, 382
local, 383-385
networks, 385-386
RRAS, 219
SNMP, 425
Windows Server Backup tools, 355
WSUS, 416-417
int domains, 128
interfaces (GUI), IP address configuration, 104-107
international domains, 128
Internet printing, 391-392
IP (Internet Protocol), 74
IP addresses, 75
anycast, 94
broadcast, 94
CIDR, 88
    address blocks, 87
defined, 86
supernetting, 88-90
VLSM, compared, 88
classes, 77-78
    host address identification, 78-79
network address identification, 78-79
configuring, 104
    with GUI interface, 104-107
    with netsh command, 107-108
IPv6, 94
    addresses, 96-99
    headers, 95
migration from IPv4, 100-101
security, 95
TCP/IP networking benefits, 94
multicasting, 94
NAT, 90-92
planning, 82-86
    hosts, 85
    subnets, 84
pools, 189
proxy servers, 92-93
ranges, 82
resources, 123
subnetting
    classful addresses, 80-81
    ranges, 82
    subnets/hosts, 81-82
troubleshooting, 108
    ipconfig command, 110-111
    ping command, 111-112
    tracert command, 113-114
unicast, 93
IP Filter List tab (IPSec policy Properties window), 267
IPC$ shared folder, 322
ipconfig command, troubleshooting IP addresses, 110-111
IPP (Internet Print Protocol), 391-392
IPSec (Internet Protocol Security), 95, 262
configuring with Windows Firewall with Advanced Security, 268-271
drivers, 264
implementing, 264-266
modes, 262-264
Monitor tool, 272-274
policies
configuring, 266-268
creating, 265-266
policy agents, 264
protocols, 263
tunnels, configuring, 266
IPSec enforcement (NAP), 286
IPSec tab (Windows Firewall with Advanced Security Properties dialog box), 270
IPv4, 77
configuring, 104
migration to IPv6, 100-101
IPv4-mapped addresses, 100
IPv6, 94
addresses, 96-97
  global unicast, 97-98
  link local unicast, 98-99
  multicast, 99
configuring, 105
headers, 95
IPv4 migration, 100-101
security, 95
TCP/IP networking benefits, 94
ISAKMP/Oakley Key Management Service, 264
ISASTAP addresses, 100
ISPs (Internet Service Providers), 90
iterative queries, DNS name resolution, 137-138

**J-K**

-j option, tracert command, 114
JetPack program, launching, 202-203

**L**

L2F (Layer 2 Forwarding), 276
L2TP (Layer 2 Tunneling Protocol), 276
launching JetPack program, 202-203
Layer 2 Forwarding. See L2F, 276
Layer 2 Tunneling Protocol (L2TP), 276
LCP (Link Control Protocol), 248
Line Printer Daemon (LPD) Service, 399
link local unicast addresses, 98-99
Link-Local Multicast Name Resolution, (LLMNR), 140
link-state algorithms, 216
LLDT (Link Layer Topology Discovery), 314
LLMNR (Link-Local Multicast Name Resolution), 140
local printers
  installing, 383-385
  network printers, compared, 379-380
logging dial-up networking, 260-262
logging DHCP, enabling, 202
logical names, 76
LPD (Line Printer Daemons) Service, 399

**M**

MAC addresses (Media Access Control), 75
MADCAP (Multicast Address Dynamic Client Allocation Protocol), 192-193
Mail Exchanger (MX) records, 136
managing
  DHCP databases, 202
  print jobs, 398-399
  print spoolers, 392-394
  RIP, 226-228
  shadow copies, 350-351
  shared files/folders, 323
  Windows Firewall with Advanced Security, 237
  wireless connections, 291-292
  WSUS, 418
Map Network Drive dialog box, 322
mapping network drives to shared files/folders, 322
MBSA (Microsoft Baseline Security Analyzer), 422
MD5 (Message Digest 5), 251
MeasureUp practice tests
  Certification Mode, 497
  creating shortcut to, 499
  Custom Mode, 498
Study Mode, 497
Message Digest 5 (MD5), 251
metrics, 214
Microsoft Calculator, 495
Microsoft Corporation domain, 128
Microsoft updates, 416
WSUS
client configurations, 419-422
downstream servers, 417-418
installing, 416-417
managing, 418
migrating
IPv4 to IPv6, 100-101
print servers, 387, 389
military domains, 128
miscellaneous organization domains, 128
MMC snap-ins, 47
Server Core, managing, 65-66
Windows Reliability and Performance Monitor, 56
Performance Monitor, 57-59
Reliability Monitor, 60
Resource view, 56
modes for wireless adapters, 287
monitoring
DHCP, 203-204
DNS
Dnscmd, 159-163
DNSLint, 158
NSLookup, 157
printer performance, 401-402
security, 272-274
mount command, 363
mount options (NFS), 362-363
moving files with NTFS, 311-312
MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2), 252
MTI University domain, 128
multicast addresses, 94, 99
multicast scopes, 192-193
multicasting, 78
multihomed DHCP servers, 197
museum domains, 128
MX (Mail Exchanger) records, 136
name domains, 128
name resolution
DNS, 137
BIND, 127
conditional forwarders, 139
countries, 128
defined, 127
domains, 127
dynamic, 140-142
forwarders, 139
FQDNs, 130
LLMNR, 140
name space, 127, 130
naming guidelines/conventions, 130
record verification, 158
recursive/iterative queries, 137-138
resource records, 135-136, 162-163
reverse queries, 140
root domains, 127
root hints, 139
round-robin, 140
second-level domains, 128
server information, viewing, 157
servers, configuring, 160
services. See DNS, services, 145
subdomains, 127, 129-130
suffix searches, 156
top-level domains, 127-128
updates, 161-162
zone files, 134
zone transfers, 142-144
zones, 131-134
zones, adding, 160
WINS, 163-164
burst handling, 165
clients, 166-167
console, 169-170
database backups, 172
database compaction, 173
database consistency, 173
GlobalNames zones, 175-176
NetBIOS name resolution, 174
proxy agents, 169
registration, 164-165
replication, configuring, 171
server replication, 168-169
server statistics, 172
tombstoning, 172-173

Name Server (NS) records, 135
name server lists, configuring, 151-152

names
  domain, 76
  hostnames, 76
  logical, 76
  SNMP community names, 424

namespaces, DFS, 336-339
  adding servers to domain-based namespaces, 337
  components, 336
  creating, 336-337
  domain controller polling, 338
  folder targets, adding, 338
  folders, creating, 338
  hierarchy, 337
  referrals, 339

NAP (Network Access Protection), 280-281
  clients, 281
  enforcement methods, 285-286
  NPS, 281-283
  SHVs, 283-285

NAT (Network Address Translation), 90-92
  enabling, 239
  overview, 238
  Teredo, 240

NBTSTAT command, 174
net domains, 128
NetBIOS (Network Basic Input/Output System), 174, 313
NETLOGON shared folder, 322
netsh command
  IP address configuration, 107-108
  resources, 123
netstat command, troubleshooting IP addresses, 115

Network Access Protection Agent, 281
network addresses, classful addresses, 78-79

Network and Sharing Center, 314
  Show Me All the Files and Folders I am Sharing, 320

network drives, mapping to shared files/folders, 322

network infrastructures
  MBSA, 422
  Microsoft updates, 416
    approving, 419
    client configurations, 419-422
    downstream servers, 417-418
    installing WSUS, 416-417
    managing WSUS, 418

Network Monitor
  aliases, 432-433
  capture options, 435
  capture sessions, 431
  filters, 433-435
  installing, 431
  overview, 429-430
  packet captures, 435
  placement, 430-431

SNMP, 423
  agent properties, configuring, 425-426
  communities, 424-425
  community names, 424
  installing, 425
  overview, 423-425
  security, configuring, 427-428
  traps, 424
  traps, configuring, 426
  versions, 425

Network Monitor
  aliases, 432-433
  capture options, 435
  capture sessions, 431
  filters, 433-435
  installing, 431
  overview, 429-430
placing protocol analyzers

classifiers analyzers, 435
placement, 430-431

network policies
configuring, 282
overview, 281

network printers
installing, 385-386
local printers, compared, 379-380

network-related domains, 128
Network Solutions, Inc., 128
New Network Policy wizard, 282
NFS (Network File System), 362-363
normal backups, 353
North Atlantic Treaty Organization domain, 128
NPS (Network Policy Server), 260, 281-283
as RADIUS client, 257-258
RADIUS accounting, 261-262
server registration, 259-260
NS (Name Server) records, 135
NSLookup utility, DNS monitoring/troubleshooting, 157
ntbackup command, 355
NTFS (New Technology File System), 306
compression, 334
disk quotas, 360-361
permissions, 307
assigning, 307-310
copying/moving files, 311-312
explicit, 310-311
folder, 308
inherited, 311
ownership, 313
resources, 376

number systems, 489
binary, 489, 491-492
decimal, 489
hexadecimal, 493-495
Microsoft Calculator, 495

O
offline file sharing, 324-325
one-way demand-dial routing, 224-225
opening ports for Windows Firewall, 232

options
ipconfig command, 110
NBTSTAT command, 174
tracert command, 113

org domains, 128
OSPF (Open Shortest Path First), 218
outbound rules, Windows Firewall with Advanced Security, 234-235
Owner/Co-owner permission, 319

P
packet filtering, 228-229
packets, capturing with protocol analyzers, 435
PAP (Password Authentication Protocol), 251
pathping command, 114
pausing print jobs, 398
PEAP (Protected Extensible Authentication Protocol), 252
performance counters, DHCP-related, 205
Performance Monitor (Windows Reliability and Performance Monitor), 57
alert actions, configuring, 59
DCS, creating, 58-59
permissions, 307
file sharing, 318-320
NTFS, 307
assigning, 307-310
copying/moving files, 311-312
explicit, 310-311
folder, 308
inherited, 311
ownership, 313
printers, 390
personal domains, 128
ping command, troubleshooting IP addresses, 111-112
placing protocol analyzers, 430-431
planning IP addresses, 82-86
Pointer (PTR) records, 135
policies
  IPSec
    configuring, 266-268
    creating, 265-266
  network
    configuring, 282
    overview, 281
  wireless, configuring, 295
pools, 189
ports
  opening in Windows Firewall, 232
  registered well-known port numbers, 103
  TCP/IP, 101-102
POSIX (Portable Operating System Interface), 45
PPP (Point-to-Point Protocol), 248
PPTP (Point-to-Point Tunneling Protocol), 275-276
preparing for exam, 31-32, 35-38
Prime Minister of Australia domain, 128
print devices, defined, 378
print drivers, defined, 378
print jobs
  cancelling, 398
  managing, 398-399
  pausing, 398
  redirecting, 400
Print Management console, 402-404
print spoolers, managing, 392-394
PRINT$ shared folder, 322
Printer Migration Wizard, 387-389
printer pools, 395-398
printers
  access, modifying, 401
  defined, 378
  deploying, 386-387
  filters, 403-404
  installing, 382
    local, 383-385
    networks, 385-386
  Internet, 391-392
  listing in Active Directory, 387
  logs, 400
  LPD Service, 399
  performance, 401-402
  permissions, 390
  printer pools, 397-398
  printing process, 381-382
  priorities, 395-397
  properties, 389
  scheduling, 395-397
  servers, migrating, 387-389
  troubleshooting, 404-406
printing
  local versus network, 379-380
  performance, 401-402
  print devices, 378
  print drivers, 378
  print jobs
    cancelling, 398
    managing, 398-399
    pausing, 398
    redirecting, 400
  Print Management console, 402-404
  print spoolers, managing, 392-394
  process, 381-382
  spoolers, 378
  troubleshooting, 404-406
priorities, setting for printers, 395-397
private network addresses, 79
professional domains, 128
profiles, Windows Firewall with Advanced Security, 235
protocol analyzers
  overview, 429-430
  packet captures, 435
  placement, 430-431
protocols
  AH, 263
  ARP, 75
  authentication, 249-250
    CHAP, 251-252
    EAP, 252
    MS-CHAPv2, 252
    PAP, 251
    PEAP, 252
    CBCP, 249
recursive queries, DNS name resolution

CHAP, 251-252
DHCP, 141
EAP, 252
ESP, 263
IP, 74
IPP, 391-392
IPSec, 262
configuring with Windows
- Firewall with Advanced Security, 268-271
driver, 264
implementing, 264-266
modes, 262, 264
Monitor tool, 272, 274
policies, creating, 265-266
policy agents, 264
policy configuration, 266-268
protocols, 263
tunnels, configuring, 266
website, 303
L2TP, 276
LCP, 248
MS-CHAPv2, 252
OSPF, 218
PAP, 251
PEAP, 252
PPP, 248
PPTP, 275-276
RIP, 216-218, 226-228
SMB, 314
SNMP, 423
agent properties, configuring, 425-426
- communities, 424-425
- community names, 424
installing, 425
overview, 423-425
security, configuring, 427-428
traps, 424
traps, configuring, 426
versions, 425
SSTP, 276
TCP/IP, 74
- hosts, 74, 77
- ports, 101-102
- sockets, 103
TKIP, 288
VPNs, 275
- L2TP, 276
- PPTP, 275-276
- SSTP, 276
proxy agents (WINS), 169
proxy servers, 92-93
PTR (Pointer) records, 135
public folders, 316-318
publishing printers in Active Directory, 387

Q-R
QoS (Quality of Service), 95
qualifications for Microsoft certification candidates, 26-27
- educational background, 28
- experience, 29-30
queries
- iterative, DNS name resolution, 137-138
- recursive, DNS name resolution, 137-138
- reverse, 140
RADIUS (Remote Authentication Dial-In User Service), 255
- accounting, 261-262
- enabling, 257
- NPS as client, 257-258
- proxies, 256
- servers, configuring, 293-294
ranges of IP addresses, 82
RDC (Remote Differential Compression), 340
reader permission, 319
readiness for exam, testing, 34-35
records (resource)
- adding, 149, 162
- deleting, 162
- DNS, 135-136
- scavenging, 150-151
recursive queries, DNS name resolution, 137-138
redirecting print jobs, 400
referrals, DFS namespaces, 339
registering
NPS servers, 259-260
WINS, 164-165
Reliability Monitor (Windows Reliability
and Performance Monitor), 60
remote access, dial-up
remote access servers, configuring
dial-up, 253-255
   authentication methods, 255
   clients, 248-249
   ports, 254
   PPP options, 254
remote access VPNs, 275
replication
   DFS, 339-347
      connections, creating, 343-344
      diagnostic reports, 347
      enabling/disabling, 344
      folder targets, 340
      folders, sharing, 344
      forcing, 344
      primary members, 341
      RDC, 340
      replication group members,
         adding, 342-343
      replication groups, creating,
         340-341
      schedules, editing, 344
      topology, 345-346
      WINS, configuring, 171
reports, DFS Replication diagnostic, 347
requests (DHCP), 189
resource records
   adding, 149, 162
   cache memory, 162
   deleting, 162
   DNS, 135-136
   scavenging, 150-151
Resource view (Windows Reliability and
Performance Monitor), 56
resources
   backup and recovery, 376
   file systems, 376
   IP addresses, 123
   netsh command, 123
   NTFS, 376
   RRAS, 303
   Server Core configuration, 123
   Windows updates, 441
restoring WINS databases, 172
reverse lookup zones, 147
reverse queries, 140
rights, 307
RIP (Routing Information Protocol),
   216-218, 226, 228
RIPv2, 218
roles for Server Core, 64
root domains, 127
root hints
   configuring, 153
   DNS, 139
round-robin, 140
route command, static route
   configurations, 221-222
routers
   defined, 214
   hops, 214
   routing overview, 214-215
routing
   demand-dial connections, 224
      configuring, 226
      one-way, 224-225
      two-way, 225
   distance-vector routing algorithms, 215
   dynamic routing algorithms, 215
   link-state routing algorithms, 216
NAT
   enabling, 239
   overview, 238
   Teredo, 240
OSPF, 218
overview, 214-215
packet filters, 228-229
RIP, 216-218, 226-228
RRAS, 219-220
static routes, configuring, 220
   route command, 221-222
RRAS management console, 223-224
static routing algorithms, 215
Windows Firewall
configuring, 230-232
new features, 229
ports, opening, 232
turning on/off, 230
Windows Firewall with Advanced Security, 233
configurations, viewing, 236-237
inbound/outbound rules, 234-235
managing, 237
profiles, 235
RRAS (Routing and Remote Access Service)
enabling, 219
installing, 219
LAN/WAN routing, enabling, 220
logging, 260-262
resources, 303
static route configurations, 223-224
RSAT (Microsoft Remote Server Administration Tools), 61-63
Rules tab (IPSec policy Properties window), 267
S
SAs (Security Associations), 264
saving
aliases, 433
capture sessions, 431
scheduling
backups, 356-358
DFS Replication groups, 344
printers, 395-397
searching DNS suffixes, 156
second-level domains, 128
security
authentication, wireless certificates, 292-293
encryption
files, 326
wireless, 288
wireless certificates, 292-293
IPSec, 262
configuring with Windows Firewall with Advanced Security, 268-271
driver, 264
implementing, 264-266
modes, 262-264
Monitor tool, 272-274
policies, creating, 265-266
policy agents, 264
policy configuration, 266-268
protocols, 263
tunnels, configuring, 266
website, 303
IPv6, 95
MBSA, 422
monitoring, 272-274
NAP, 280-281
clients, 281
enforcement methods, 285-286
NPS, 281-283
SHVs, 283-285
SNMP, configuring, 427-428
Windows Firewall, 229-230
configuring, 230, 232
new features, 229
ports, opening, 232
turning on/off, 230
Windows Firewall with Advanced Security, 233
configurations, viewing, 236-237
inbound/outbound rules, 234-235
managing, 237
profiles, 235
zone transfers, 143-144
Security Associations (SAs), 264
security logs, 52
server bindings (DHCP), 197-198
Server Core, 63
administrative tools, running, 65-66
configuring, 123
features, 65
roles, 64
Server Manager console, 49
server roles, 40-42

servers
backing up, 355
caching-only, DNS zones, 132
dial-up remote access, configuring, 253-255
DNS
  caching-only, 146
  configuring, 146, 160
  installing, 145
downstream, 417-418
namespace, adding to domain-based namespaces, 337
NPS, 259-260, 281-283
print, migrating, 387-389
proxy, 92-93
RADIUS, configuring for 802.1X wireless/wired connections, 293-294
System State, 356
upstream, 417
WINS replication, 168-169

Service (SRV) records, 136

services, 50
  configuring, 50
  ISAKMP/Oakley Key Management, 264
  Line Printer Daemon, 399
  RRAS, 219-220
  enabling, 219
  installing, 219
  LAN/WAN routing, enabling, 220

shadow copies, 347
  enabling, 347-349
  previous versions, accessing, 349-350
  VSSAdmin tool, 350-351

Shared Folders snap-in, 323

sharing folders/files, 313-314
  access, 322-323
  administrative shares, 321-322
  EFS, 328
  managing, 323
  network discovery/browsing, 314-316
  offline settings, 324-325
  public folders, 316-318
  replicated, 344
  shadow copies, 347
  special shares, 321-322
  standard, 318-320

shortcut to MeasureUp practice test, creating, 499

SHVs (Security Health Validators), 283-285

site-to-site VPNs, 275

SMB (Server Message Block) protocol, 314

snap-ins
  DFS Management, 335
  Shared Folders, 323
  Windows Server Backup, 355

SNMP (Simple Network Management Protocol), 423
  agent properties, configuring, 425-426
  communities, 424-425
  community names, 424
  installing, 425
  overview, 423-425
  security, configuring, 427-428
  traps, 424
  traps, configuring, 426
  versions, 425

SOA (Start of Authority) records, 135, 148

sockets, TCP/IP, 103

SoH (Statement of Health), 283

special shared folders, 321-322

Specify Access Permissions dialog box, 283

spoolers, 378

SRV (Service) records, 136

SSID (Service Set IDentifiers), 289

SSTP (Secure Socket Tunneling Protocol), 276

standard file sharing, 318-320
  enabling, 318
  Network and Sharing Center, Show Me All the Files and Folders I am Sharing option, 320
  permissions, 318-320
  shared folders, creating, 319

standard primary zones, 131-132

standard secondary zones, 131-132

standards, wireless, 287
starting
  NFS clients, 362
  wecsvc, 55
stateful firewalls, 229
static routes, configuring, 220
  route command, 221-222
  RRAS management console, 223-224
static routing algorithms, 215
storing backups, 357
stub zones, 131, 134
Study Mode, 497
studying for exam, 32-33
subdomains, 127, 129-130, 148
subnet masks, 79
subnetting, 79
  classful addresses, 80-81
  IP addresses
    network planning, 82-86
    ranges, 82
    subnets and hosts, 81-82
subscriptions, creating for Event
  Collector, 54-55
success audit events, 53
suffix searches, 156
supernetting with CIDR, 88-90
superscopes, 192
switches for ipconfig command, 111
synchronous backups, performing on
  DHCP database, 203
system log, 52
system requirements, BitLocker Drive
  Encryption, 331
tables (ARP), viewing, 77
TCP/IP (Transmission Control
  Protocol/Internet Protocol)
  hosts, 74, 77
  ports, 101-102
  sockets, 103
technical support, contacting, 500
Teredo, 101, 240
test anxiety, dealing with, 37-38
testing readiness for exam, 34-35
timeout_value option (tracert command),
  114
TKIP (Temporal Key Integrity Protocol), 288
tombstoning, 172-173
tools
  File Server Resource Manager, 362
  IPSec Monitor, 272-274
  VSSAdmin, 350-351
  Windows Server Backup, installing,
    355
top-level domains, 127-128
topologies, DFS Replication, 345-346
TPM (Trusted Platform Module), 329-331
tracert command, 113-114
transport mode (IPSec), 263
troubleshooting
  DHCP, 203-204
  DNS
    Dnscmd, 159-163
    DNSLint, 158
    NSLookup, 157
  IP addresses, 108, 115
    ipconfig command, 110-111
    ping command, 111-112
    tracert command, 113-114
  NetBIOS name resolution, 174
  printing, 404-406
Trusted Platform Module. See TPM,
  329-331
TS Gateway enforcement (NAP), 286
TTL (Time to Live), 137
tunnel mode (IPSec), 263
Tunnel Setting tab (IPSec policy
  Properties window), 268
tunnels (IPSec), configuring, 266
two-way demand-dial routing, 225
types of VPNs, 275

U

UNC (Universal Naming Convention), 336
unicast addresses, 93
United States Army domain, 128
United States Department of Education
  domain, 128
updates
Active Directory integrated zones, 162
DNS zones, 161
dynamic DNS, 141-142, 152
Microsoft, 416
approving, 419
client configurations, 419-422
downstream servers, 417-418
installing WSUS, 416-417
managing WSUS, 418
resources, 441
upstream servers, 417
USB drives, wireless connection configurations, 290
utilities, monitoring/troubleshooting DNS
Dnscmd, 159-163
DNSLint, 158
NSLookup, 157
vendor classes, creating, 196-197
viewing
arp tables, 77
printer logs, 400
Windows Firewall with Advanced Security configurations, 236-237
WINS server statistics, 172
volumes, backups, 356
VPNs enforcement (NAP), 285
VPNs (Virtual Private Networks), 274
configuring, 277-278
CMAK, 279-280
with network connection, 278-279
overview, 274
protocols, 275
L2TP, 276
PPTP, 275-276
SSTP, 276
types of, 275
website, 303
VSSAdmin tool, 350-351
wbadmin command, 355, 358-359
websites
3Com IP address white paper, 123
backup and recovery, 376
BitLocker Drive Encryption, 376
country domain codes, 128
file systems, 376
IPSec, 303
MBSA download, 423
Microsoft updates, 416
netsh command, 123
Network Solutions, Inc., 128
NTFS, 376
RRAS Troubleshooting Reference, 303
Server Core configuration, 123
VPNs, 303
well-known port numbers, 103
Windows Firewall with Advanced Security and IPSec, 303
Windows updates, 441
WSUS administration, 418
wecsvc, starting, 55
wecutil.exe, 55
WEP (Wireless Equivalency Protection), 288
Windows Features, 42, 45
Windows Firewall, 229-230
configuring, 230-232
new features, 229
ports, opening, 232
turning on/off, 230
Windows Firewall with Advanced Security, 233
configurations, viewing, 236-237
inbound/outbound rules, 234-235
IPSec, configuring, 268-271
managing, 237
profiles, 235
website, 303
Windows Firewall with Advanced Security Properties dialog box, 270
Windows Reliability and Performance Monitor, 56
Performance Monitor, 57
DCS, creating, 58-59
Reliability Monitor, 60
Resource view, 56
Windows Security dialog box, file/folder ownership, 313
Windows Server 2008 Administration Tools for Features, 63
Windows Server 2008 Administration Tools for Roles, 62
Windows Server Backup, 354
scheduling, 356-358
server backups, 355
snap-in, 355
storage, 357
tools, installing, 355
volumes, 356
WINS (Windows Internet Name Service), 163-164
burst handling, 165
clients, 166-167
console, 169-170
database, 172-173
GlobalNames zones, 175-176
NetBIOS name resolution, 174
proxy agents, 169
registration, 164-165
replication, configuring, 171
server replication, 168-169
server statistics, 172
tombstoning, 172-173
WinSock, 103
wireless connections, 286
adapters, 287-289
certificates, 292-293
configuring, 289-290
encryption, 288
managing, 291-292
personal mode, 288
policies, configuring, 295
RADIUS servers, configuring, 293-294
standards, 287
wireless network (IEEE 802.11) policies, 295

wizards
Add Printer, 383
Backup Once, 356
Backup Schedule, 356
BitLocker setup, 332
Catalog Recovery, 360
Certificate Export, 328
Certificate Import, 329
Connection Security Rule, 269
File Sharing, 320
New Network Policy, 282
Printer Migration, 387-389

World Wide Web Consortium domain, 128
WPA (WiFi Protected Access), 288
WPA2 (WiFi Protected Access Version 2), 288
WSUS (Windows Server Update Services), 416
client configurations, 419-422
downstream servers, 417-418
installing, 416-417
managing, 418

X-Y-Z

zipping folders, 333
zone files, 134
zones, DNS, 131
Active Directory integrated, 131-134, 144
Active Directory integrated zone updates, 162
adding, 160
caching-only servers, 132
forward/reverse lookup, 147
GlobalNames, 175-176
replication scopes, 154
standard primary, 131-132
standard secondary, 131-132
stub, 131, 134
transfers, 131, 142-144
transfers, configuring, 151-152
updates, 161
zone files, 134