EXAM CRAM

CompTIA

Network+®

N10-005

Fourth Edition

CD FEATURES MORE THAN 200
PRACTICE QUESTIONS

PEARSON

CompTIA AUTHORIZED

EMMETT DULANEY
MIKE HARWOOD

EXAM CRAM

CompTIA Network+

N10-005 Authorized

Emmett Dulaney
Mike Harwood

que®

800 East 96th Street, Indianapolis, Indiana 46240 USA

CompTIA Network+ N10-005 Authorized Exam Cram

ISBN-13: 978-0-7897-4905-5
ISBN-10: 0-7897-4905-X

Library of Congress Cataloging-in-Publication data is on file.

Second Printing: May 2012

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

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

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

International Sales
international@pearsoned.com

Publisher
Paul Boger

Associate Publisher
David Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Box Twelve Communications, Inc.

Managing Editor
Sandra Schroeder

Project Editor
Seth Kerney

Copy Editor
Apostrophe Editing Services

Indexer
Ken Johnson

Proofreader
Williams Woods Publishing Services

Technical Editor
Chris Crayton

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Tim Warner

Book Designer
Gary Adair

Page Layout
Bronkella Publishing

Contents at a Glance

Table of Contents

About the Authors

Emmett Dulaney (Network+, A+, Security+, ManyOthers+) is the author of numerous books on certifications and operating systems. He is a columnist for CertCities and an associate professor at Anderson University. In addition to the *Network+ Exam Cram*, he is the author of the *CompTIA A+ Complete Study Guide* and the *CompTIA Security+ Study Guide*.

Mike Harwood (MCSE, A+, Network+, Server+, Linux+) has more than 14 years experience in information technology and related fields. He has held a number of roles in the IT field including network administrator, instructor, technical writer, website designer, consultant, and online marketing strategist. Mike has been a regular on air technology contributor for CBC radio and has coauthored numerous computer books, including the *Network+ Exam Cram* published by Pearson.

About the Technical Editor

Christopher A. Crayton is an author, a technical editor, a technical consultant, a security consultant, a trainer and a SkillsUSA state-level technology competition judge. Formerly, he worked as a computer and networking instructor at Keiser College (2001 Teacher of the Year); a network administrator for Protocol, a global electronic customer relationship management (eCRM) company; and at Eastman Kodak Headquarters as a computer and network specialist. Chris has authored several print and online books, including The *A+ Exams Guide*, Second Edition (Cengage Learning, 2008), *Microsoft Windows Vista 70-620 Exam Guide Short Cut* (O'Reilly, 2007), *CompTIA A+ Essentials 220-601 Exam Guide Short Cut* (O'Reilly, 2007), *The A+ Exams Guide*, *The A+ Certification and PC Repair Handbook* (Charles River Media, 2005), *The Security+ Exam Guide* (Charles River Media, 2003) and *A+ Adaptive Exams* (Charles River Media, 2002). He is also co-author of the *How to Cheat at Securing Your Network* (Syngress, 2007). As an experienced technical editor, Chris has provided many technical edits and reviews for several major publishing companies, including Pearson Education, McGraw-Hill, Cengage Learning, Wiley, O'Reilly, Syngress, and Apress. He holds MCSE, A+ and Network+ certifications.

Dedication

For Karen, Kristin, Evan, and Spencer: the backbone of my network.
—Emmett Dulaney

Acknowledgments

I would like to thank Mike Harwood for creating a great book of which I was honored to join with this edition. Thanks are due to a wonderful team of talented individuals, three of whom deserve special attention: Betsy Brown, Jeff Riley, and Christopher A. Crayton. They represent the best in the business.

—Emmett Dulaney

We Want to Hear from You!

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

As an associate publisher for Pearson, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

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

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
Associate Publisher
Pearson
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

CompTIA Security+

- Designed for IT professionals focused on system security.
- Covers network infrastructure, cryptography, assessments, and audits.
- Security+ is mandated by the U.S. Department of Defense and is recommended by top companies such as Microsoft, HP, and Cisco.

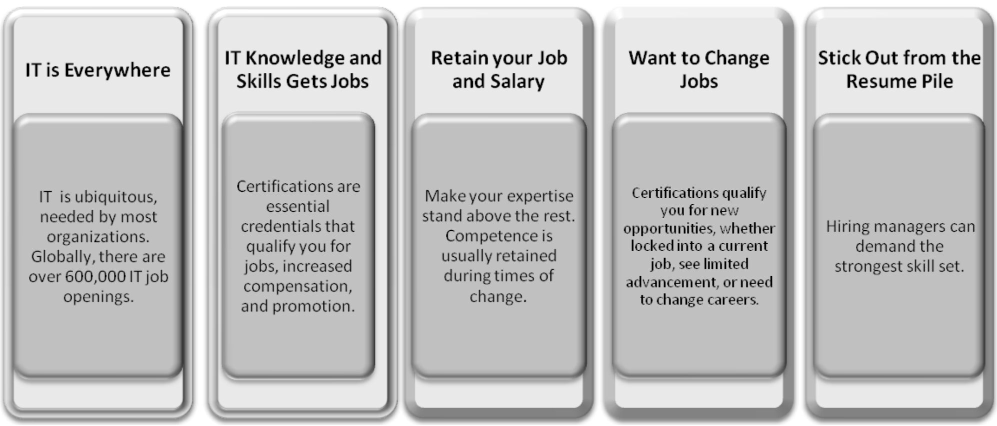
It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill. Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.

Security is one of the highest demand job categories. Growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.

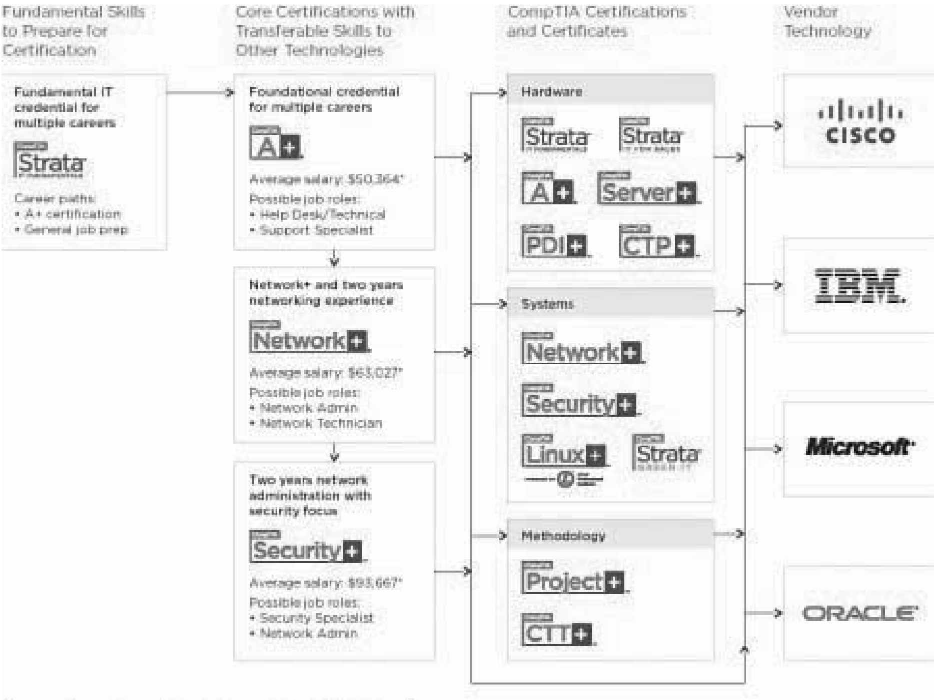
- **Jobs for security administrators are expected to increase by 18%** -the skill set required for these types of jobs map to CompTIA Security+ certification.
- **Network Security Administrators -** can earn as much as $106,000 per year.
- **CompTIA Security+ is the first step -** in starting your career as a Network Security Administrator or Systems Security Administrator.
- **CompTIA Security+ is regularly used in organizations -** such as Hitachi Information Systems, Trendmicro, the McAfee Elite Partner program, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

How Certification Helps Your Career



CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.



*Source: *Computerworld* Salary Survey 2010—U.S. salaries only

Steps to Getting Certified and Staying Certified	
Review Exam Objectives	Review the certification objectives to make sure you know what is covered in the exam. http://www.comptia.org/certifications/testprep/examobjectives.aspx
Practice for the Exam	After you have studied for the certification, take a free assessment and sample test to get an idea what type of questions might be on the exam. http://www.comptia.org/certifications/testprep/practicetests.aspx
Purchase an Exam Voucher	Purchase your exam voucher on the CompTIA Marketplace, which is located at: www.comptiastore.com
Take the Test!	Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: http://www.comptia.org/certifications/testprep/testingcenters.aspx
Stay Certified! **Continuing Education**	Effective January 1, 2011, new CompTIA Security+ certifications are valid for three years from the date of your certification. There are a number of ways the certification can be renewed. For more information go to: http://certification.comptia.org/getCertified/steps_to_certification/stayCertified.aspx

Join the Professional Community

Join IT Pro Community http://itpro.comptia.org	The free IT Pro online community provides valuable content to students and professionals. • Career IT Job Resources ▪Where to start in IT ▪Career Assessments ▪Salary Trends ▪US Job Board • Forums on Networking, Security, Computing and Cutting Edge Technologies • Access to blogs written by Industry Experts • Current information on Cutting Edge Technologies • Access to various industry resource links and articles related to IT and IT careers

Content Seal of Quality

This courseware bears the seal of **CompTIA Approved Quality Content.** This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

Why CompTIA?

- **Global Recognition** – CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA's certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.
- **Valued by Hiring Managers -** Hiring managers value CompTIA certification because it is vendor and technology independent validation of your technical skills.
- **Recommended or Required by Government and Businesses** - Many government organizations and corporations either recommend or require technical staff to be CompTIA certified. (e.g. Dell, Sharp, Ricoh, the U.S. Department of Defense and many more)
- **Three CompTIA Certifications ranked in the top 10**. In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to obtain more information

- **Visit CompTIA online** - www.comptia.org to learn more about getting CompTIA certified.
- **Contact CompTIA** - call 866-835-8020 ext. 5 or email questions@comptia.org
- **Join the IT Pro Community** – http://itpro.comptia.org to join the IT community to get relevant career information.
- **Connect with us :**

Introduction

Welcome to the *Network+ Exam Cram*. This book is designed to prepare you to take—and pass—the CompTIA Network+ exam. The Network+ exam has become the leading introductory-level network certification available today. It is recognized by both employers and industry giants as providing candidates with a solid foundation of networking concepts, terminology, and skills. The Network+ exam covers a broad range of networking concepts to prepare candidates for the technologies they are likely to work with in today's network environments.

About Network+ Exam Cram

Exam Crams are designed to give you the information you need to know to prepare for a certification exam. They cut through the extra information, focusing on the areas you need to get through the exam. With this in mind, the elements within the *Exam Cram* titles are aimed at providing the exam information you need in the most succinct and accessible manner.

In this light, this book is organized to closely follow the actual CompTIA objectives for exam N10-005. As such, it is easy to find the information required for each of the specified CompTIA Network+ objectives. The objective focus design used by this *Exam Cram* is an important feature because the information you need to know is easily identifiable and accessible. To see what we mean, compare the CompTIA objectives to the book's layout, and you can see that the facts are right where you would expect them to be.

Within the chapters, potential exam hot spots are clearly highlighted with Exam Alerts. They have been carefully placed to let you know that the surrounding discussion is an important area for the exam. To further help you prepare for the exam, a Cram Sheet is included that you can use in the final stages of test preparation. Be sure to pay close attention to the bulleted points on the Cram Sheet because they pinpoint the technologies and facts you probably will encounter on the test.

Finally, great effort has gone into the questions that appear throughout the chapter and the practice tests to ensure that they accurately represent the look and feel of the ones you will see on the real Network+ exam. Be sure, before taking the exam, that you are comfortable with both the format and content of the questions provided in this book.

About the Network+ Exam

The Network+ (N10-005 Edition) exam is a revised version of the original exam. The new Network+ objectives are aimed toward those who have at least 9 months of experience in network support and administration. CompTIA believes that new Network+ candidates require more hands-on experience in network administration and troubleshooting, but this should not discourage those who do not. Quite simply, the nature of the questions on the new exam is not dissimilar to the old, and you can get by without actual hands-on experience. Still, a little hands-on experience never hurt anyone and can certainly add to your confidence going into the exam.

You will have a maximum of 90 minutes to answer the 100 questions on the exam. The allotted time is quite generous, so when you finish, you probably will have time to double-check a few of the answers you were unsure of. By the time the dust settles, you need a minimum score of 720 to pass the Network+ exam. This is on a scale of 100 to 900. For more information on the specifics of the Network+ exam, refer to CompTIA's main website at http://certification.comptia.org/.

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (that is, *objectives*) and specific topics under each general topic (that is, *subobjectives*) for the CompTIA Network+ N10-005 exam. This table also lists the chapter in which each exam topic is covered. Some objectives and subobjectives are addressed in multiple chapters.

TABLE I-1 **CompTIA Network+ Exam Topics**

Chapter	N10-005 Exam Objective	N10-005 Exam Subobjective
1 (Introduction to Networking)	3.0 Network Media and Topologies	3.5 Describe different network topologies.
2 (OSI and TCP/IP Models and Network Protocols)	1.0 Network Concepts 2.0 Network Installation and Configuration 4.0 Network Management	1.1 Compare the layers of the OSI and TCP/IP models. 1.6 Explain the function of common network protocols. 1.7 Summarize DNS concepts and its components. 2.3 Explain the purpose and properties of DHCP. 4.4 Given a scenario, use the appropriate network resource to analyze traffic.

TABLE I-1 **Continued**

Chapter	N10-005 Exam Objective	N10-005 Exam Subobjective
3 (Addressing and Routing)	1.0 Network Concepts 2.0 Network Installation and Configuration	1.3 Explain the purpose and properties of IP addressing. 1.4 Explain the purpose and properties of routing and switching. 1.5 Identify common TCP and UDP default ports. 2.1 Given a scenario, install and configure routers and switches.
4 (Components and Devices)	1.0 Network Technologies 4.0 Network Management	1.2 Classify how applications, devices, and protocols relate to the OSI model layers. 1.9 Identify virtual network components. 4.1 Explain the purpose and features of various network appliances. 3.7 Compare and contrast different LAN technologies.
5 (Installation and Configuration)	2.0 Network Installation and Configuration 3.0 Network Media and Topologies	2.6 Given a set of requirements, plan and implement a basic SOHO network. 3.4 Categorize WAN technology types and properties.
6 (Cabling and Wiring)	3.0 Network Media and Topologies	3.1 Categorize standard media types and associated properties. 3.2 Categorize standard connector types based on network media. 3.7 Compare and contrast different LAN technologies. 3.8 Identify components of wiring distribution.
7 (Wireless)	2.0 Network Installation and Configuration 3.0 Network Media and Topologies 5.0 Network Security	2.2 Given a scenario, install and configure a wireless network. 2.4 Given a scenario, troubleshoot common wireless problems. 3.3 Compare and contrast different wireless standards. 5.1 Given a scenario, implement appropriate wireless security measures.
8 (Network Management)	4.0 Network Management	4.2 Given a scenario, use appropriate hardware tools to troubleshoot connectivity issues. 4.3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues. 4.4 Given a scenario, use the appropriate network monitoring resource to analyze traffic. 4.5 Describe the purpose of configuration management documentation.

TABLE I-1 **Continued**

Chapter	N10-005 Exam Objective	N10-005 Exam Subobjective
9 (Network Optimization)	4.0 Network Management	4.6 Explain different methods and rationales for network performance optimization.
10 (Network Security)	5.0 Network Security	5.2 Explain the methods of network access security. 5.3 Explain methods of user authentication. 5.4 Explain common threats, vulnerabilities, and mitigation techniques. 5.5 Given a scenario, install and configure a basic firewall. 5.6 Categorize different types of network security appliances and methods.
11 (Network Troubleshooting)	1.0 Network Technologies 2.0 Network Installation and Configuration 3.0 Network Media and Topologies	1.8 Given a scenario, implement a given troubleshooting methodology. 2.5 Given a scenario, troubleshoot common router and switch problems. 3.6 Given a scenario, troubleshoot common physical connectivity problems.

Booking and Taking the Network+ Certification Exam

Unfortunately, testing is not free. You're charged $246 for each test you take, whether you pass or fail. In the United States and Canada, tests are administered by Sylvan Prometric or VUE testing services. To book a test with Prometric or to locate a Prometric testing center near you, refer to the website at http://securereg3.prometric.com/ or call 1-888-895-6116. To access the VUE contact information and book an exam, refer to the website at http://www.vue.com or call 1-877-551-7587. When booking an exam, you need to provide the following information:

- Your name as you would like it to appear on your certificate.
- Your Social Security or Social Insurance number.
- Contact phone numbers (to be called in case of a problem).
- Mailing address, which identifies the address to which you want your certificate mailed.
- Exam number and title.

- Email address for contact purposes. This often is the fastest and most effective means to contact you. Many clients require it for registration.
- Credit-card information so that you can pay online. You can redeem vouchers by calling the respective testing center.

What to Expect from the Exam

If you haven't taken a certification test, the process can be a little unnerving. Even if you've taken numerous tests, it is not much better. Mastering the inner mental game often can be as much of a battle as knowing the material. Knowing what to expect before heading in can make the process a little more comfortable.

Certification tests are administered on a computer system at a Prometric or VUE authorized testing center. The format of the exams is straightforward: Each question has several possible answers to choose from. The questions in this book provide a good example of the types of questions you can expect on the exam. If you are comfortable with them, the test should hold few surprises. Many of the questions vary in length; some of them are longer scenario questions, whereas others are short and to the point. Carefully read the questions; the longer questions often have a key point that will lead you to the correct answer.

Most of the questions on the Network+ exam require you to choose a single correct answer, but a few require multiple answers. When there are multiple correct answers, a message at the bottom of the screen prompts you to "Choose all that apply." Be sure to read these messages.

A Few Exam Day Details

It is recommended that you arrive at the examination room at least 15 minutes early, although a few minutes earlier certainly would not hurt. This will give you time to prepare and will give the test administrator time to answer any questions you might have before the test begins. Many people suggest that you review the most critical information about the test you're taking just before the test. (*Exam Cram* books provide a reference—the Cram Sheet, located inside the front of this book—that lists the essential information from the book in distilled form.) Arriving a few minutes early will give you some time to compose yourself and mentally review this critical information.

You will be asked to provide two forms of ID, one of which must be a photo ID. Both of the identifications you choose should have a signature. You also might need to sign in when you arrive and sign out when you leave.

Be warned: The rules are clear about what you can and cannot take into the examination room. Books, laptops, note sheets, and so on are not allowed in the examination room. The test administrator will hold these items, to be returned after you complete the exam. You might receive either a wipe board or a pen and a single piece of paper for making notes during the exam. The test administrator will ensure that no paper is removed from the examination room.

After the Test

Whether you want it or not, as soon as you finish your test, your score displays on the computer screen. In addition to the results appearing on the computer screen, a hard copy of the report prints for you. Like the onscreen report, the hard copy displays the results of your exam and provides a summary of how you did on each section and on each technology. If you were unsuccessful, this summary can help you determine the areas you need to brush up on.

When you pass the Network+ exam, you will have earned the Network+ certification, and your certificate will be mailed to you within a few weeks. Should you not receive your certificate and information packet within 5 weeks of passing your exam, contact CompTIA at fulfillment@comptia.org, or call 1-630-268-1818 and ask for the fulfillment department.

Last-Minute Exam Tips

Studying for a certification exam is no different than studying for any other exam, but a few hints and tips can give you the edge on exam day:

- **Read all the material**: CompTIA has been known to include material not expressly specified in the objectives. This book has included additional information not reflected in the objectives to give you the best possible preparation for the examination.
- **Watch for the Exam Tips and Notes**: The Network+ objectives include a wide range of technologies. Exam Tips and Notes found throughout each chapter are designed to pull out exam-related hot spots. These can be your best friends when preparing for the exam.

- **Use the questions to assess your knowledge**: Don’t just read the chapter content; use the exam questions to find out what you know and what you don’t. If you struggle, study some more, review, and then assess your knowledge again.
- **Review the exam objectives**: Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck!

This page intentionally left blank

CHAPTER 3

Addressing and Routing

This chapter covers the following official Network+ objectives:

- Explain the purpose and properties of IP addressing.
- Explain the purpose and properties of routing and switching.
- Identify common TCP and UDP default ports.
- Given a scenario, install and configure routers and switches.

For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the "Introduction."

Without question, the TCP/IP suite is the most widely implemented protocol on networks today. As such, it is an important topic on the Network+ exam. To pass the exam, you definitely need to understand the material presented in this chapter.

This chapter deals with the individual protocols within the protocol suite. It looks at the functions of the individual protocols and their purposes. It starts by discussing one of the more complex facets of TCP/IP: addressing.

IP Addressing

- **Explain the purpose and properties of IP addressing.**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. How many octets does a Class A address use to represent the network portion?
2. What is the range that Class C addresses span in the first octet?
3. What are the reserved IPv4 ranges for private networks?

Answers

1. A Class A address uses only the first octet to represent the network portion, a Class B address uses two octets, and a Class C address uses three octets.
2. Class C addresses span from 192 to 223, with a default subnet mask of 255.255.255.0.
3. A private network is any network to which access is restricted. Reserved IP addresses are 10.0.0.0, 172.16.0.0 to 172.31.0.0, and 192.168.0.0.

IP addressing is one of the most challenging aspects of TCP/IP. It can leave even the most seasoned network administrators scratching their heads. Fortunately, the Network+ exam requires only a fundamental knowledge of IP addressing. The following sections look at how IP addressing works for both IPv4 and the newest version of IP: IPv6.

To communicate on a network using TCP/IP, each system must be assigned a unique address. The address defines both the number of the network to which the device is attached and the number of the node on that network. In other words, the IP address provides two pieces of information. It's a bit like a street name and house number in a person's home address.

Each device on a logical network segment must have the same network address as all the other devices on the segment. All the devices on that network segment must then have different node addresses.

In IP addressing, another set of numbers, called a subnet mask, defines which portion of the IP address refers to the network address and which refers to the node address.

IP addressing is different in IPv4 and IPv6. The discussion begins by looking at IPv4.

IPv4

An IPv4 address is composed of four sets of 8 binary bits, which are called *octets*. The result is that IP addresses contain 32 bits. Each bit in each octet is assigned a decimal value. The leftmost bit has a value of 128, followed by 64, 32, 16, 8, 4, 2, and 1, left to right.

Each bit in the octet can be either a 1 or a 0. If the value is 1, it is counted as its decimal value, and if it is 0, it is ignored. If all the bits are 0, the value of the octet is 0. If all the bits in the octet are 1, the value is 255, which is 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1.

By using the set of 8 bits and manipulating the 1s and 0s, you can obtain any value between 0 and 255 for each octet.

Table 3.1 shows some examples of decimal-to-binary value conversions.

TABLE 3.1 **Decimal-to-Binary Value Conversions**

Decimal Value	Binary Value	Decimal Calculation
10	00001010	8 + 2 = 10
192	11000000	128 + 64 = 192
205	11001101	128 + 64 + 8 + 4 + 1 = 205
223	11011111	128 + 64 + 16 + 8 + 4 + 2 + 1 = 223

IP Address Classes

IP addresses are grouped into logical divisions called *classes*. The IPv4 address space has five address classes (A through E); although, only three (A, B, and C) assign addresses to clients. Class D is reserved for multicast addressing, and Class E is reserved for future development.

Of the three classes available for address assignments, each uses a fixed-length subnet mask to define the separation between the network and the node address. A Class A address uses only the first octet to represent the network portion; a Class B address uses two octets; and a Class C address uses the first three octets. The upshot of this system is that Class A has a small number of network addresses, but each Class A address has a large number of possible host addresses. Class B has a larger number of networks, but each Class B address has a smaller number of hosts. Class C has an even larger number of networks, but each Class C address has an even smaller number of hosts. The exact numbers are provided in Table 3.2.

ExamAlert

Be prepared for questions asking you to identify IP class ranges, such as the IP range for a Class A network.

TABLE 3.2 **IPv4 Address Classes and the Number of Available Network/Host Addresses**

Address Class	Range	Number of Networks	Number of Hosts Per Network	Binary Value of First Octet
A	1 to 126	126	16,777,214	0xxxxxxx
B	128 to 191	16,384	65,534	10xxxxxx
C	192 to 223	2,097,152	254	110xxxxx
D	224 to 239	N/A	N/A	1110xxxx
E	240 to 255	N/A	N/A	1111xxxx

Note

Notice in Table 3.2 that the network number 127 is not included in any of the ranges. The 127.0.0.1 network ID is reserved for the IPv4 local loopback. The local loopback is a function of the protocol suite used in the troubleshooting process.

ExamAlert

For the Network+ exam, you should be prepared to identify into which class a given address falls. You should also be prepared to identify the IPv4 loopback address. The actual loopback address is 127.0.0.1.

Subnet Mask Assignment

Like an IP address, a *subnet mask* is most commonly expressed in 32-bit dotted-decimal format. Unlike an IP address, though, a subnet mask performs just one function—it defines which parts of the IP address refer to the network address and which refer to the node address. Each class of the IP address used for address assignment has a default subnet mask associated with it. Table 3.3 lists the default subnet masks.

TABLE 3.3 **Default Subnet Masks Associated with IP Address Classes**

Address Class	Default Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

ExamAlert

You will likely see questions about address class and the corresponding default subnet mask. Review Table 3.3 before taking the exam.

Subnetting

Now that you have looked at how IP addresses are used, you can learn the process of subnetting. *Subnetting* is a process by which the node portions of an IP address create more networks than you would have if you used the default subnet mask.

To illustrate subnetting, for example, suppose that you have been assigned the Class B address 150.150.0.0. Using this address and the default subnet mask, you could have a single network (150.150) and use the rest of the address as node addresses. This would give you a large number of possible node addresses, which in reality is probably not useful. With subnetting, you use bits from the node portion of the address to create more network addresses. This reduces the number of nodes per network, but you probably will still have more than enough.

Following are two main reasons for subnetting:

- It enables you to more effectively use IP address ranges.
- It makes IP networking more secure and manageable by providing a mechanism to create multiple networks rather than having just one. Using multiple networks confines traffic to the network that it needs to be on, which reduces overall network traffic levels. Multiple subnets also create more broadcast domains, which in turn reduces networkwide broadcast traffic. A difference exists between broadcast domains and collision domains: The latter is all the connected nodes, whereas the former is all the logical nodes that can reach each other. As such, collision domains are typically subsets of broadcast domains.

ExamAlert

Subnetting does not increase the number of IP addresses available. It increases the number of network IDs and, as a result, decreases the number of node IDs per network. It also creates more broadcast domains. Broadcasts are not forwarded by routers, so they are limited to the network on which they originate.

Identifying the Differences Between IPv4 Public and Private Networks

IP addressing involves many considerations, not the least of which are public and private networks.

- A *public network* is a network to which anyone can connect. The best (and perhaps only pure) example of such a network is the Internet.
- A *private network* is any network to which access is restricted. A corporate network and a network in a school are examples of private networks.

Note

The Internet Assigned Numbers Authority (IANA) is responsible for assigning IP addresses to public networks. However, because of the workload involved in maintaining the systems and processes to do this, IANA has delegated the assignment process to a number of regional authorities. For more information, visit http://www.iana.org/ipaddress/ip-addresses.htm.

The main difference between public and private networks, other than access to a private network is tightly controlled and access to a public network is not, is that the addressing of devices on a public network must be carefully considered. Addressing on a private network has a little more latitude.

As already discussed, for hosts on a network to communicate by using TCP/IP, they must have unique addresses. This number defines the logical network that each host belongs to and the host's address on that network. On a private network with, say, three logical networks and 100 nodes on each network, addressing is not a difficult task. On a network on the scale of the Internet, however, addressing is complex.

If you connect a system to the Internet, you need to get a valid registered IP address. Most commonly, you obtain this address from your ISP. Alternatively, if you wanted a large number of addresses, for example, you could contact the organization responsible for address assignment in your area. You can determine who the regional numbers authority for your area is by visiting the IANA website.

Because of the nature of their business, ISPs have large blocks of IP addresses that they can assign to their clients. If you need a registered IP address, getting one from an ISP is almost certainly a simpler process than going through a regional numbers authority. Some ISPs' plans actually include blocks of registered IP addresses, working on the principle that businesses want some kind of permanent presence on the Internet. Of course, if you discontinue your service with the ISP, you can no longer use the provided IP address.

Private Address Ranges

To provide flexibility in addressing and to prevent an incorrectly configured network from polluting the Internet, certain address ranges are set aside for private use. These address ranges are called *private ranges* because they are designated for use only on private networks. These addresses are special because Internet routers are configured to ignore any packets they see that use these addresses. This means that if a private network "leaks" onto the Internet, it won't get any farther than the first router it encounters. So a private address cannot be on the Internet because it cannot be routed to public networks.

Three ranges are defined in RFC 1918: one each from Classes A, B, and C. You can use whichever range you want; although, the Class A and B address ranges offer more addressing options than Class C. Table 3.4 defines the address ranges for Class A, B, and C addresses.

TABLE 3.4 **Private Address Ranges**

Class	Address Range	Default Subnet Mask
A	10.0.0.0 to 10.255.255.255	255.0.0.0
B	172.16.0.0 to 172.31.255.255	255.255.0.0
C	192.168.0.0 to 192.168.255.255	255.255.255.0

Exam**Alert**

You can expect questions on private IP address ranges and their corresponding default subnet masks.

Classless Interdomain Routing (CIDR)

Classless interdomain routing (CIDR) is a method to assign addresses outside the standard Class A, B, and C structure that is used by IPv6. Specifying the number of bits in the subnet mask offers more flexibility than the three standard class definitions.

Using CIDR, addresses are assigned using a value known as the *slash*. The actual value of the slash depends on how many bits of the subnet mask are used to express the network portion of the address. For example, a subnet mask that uses all 8 bits from the first octet and 4 from the second would be described as /12, or "slash 12." A subnet mask that uses all the bits from the first three octets would be called /24. Why the slash? In actual addressing terms, the CIDR value is expressed after the address, using a slash. So the address 192.168.2.1/24 means that the node's IP address is 192.168.2.1, and the subnet mask is 255.255.255.0.

Note

You can find a great CIDR calculator that can compute values from ranges at http://www.subnet-calculator.com/cidr/php.

ExamAlert

You will likely see IP addresses in their CIDR format on the exam. Be sure that you understand CIDR addressing for the exam.

Default Gateways

Default gateways are the means by which a device can access hosts on other networks for which it does not have a specifically configured route. Most workstation configurations actually default to just using default gateways rather than having any static routes configured. This enables workstations to communicate with other network segments, or with other networks, such as the Internet.

ExamAlert

You will be expected to identify the purpose and function of a default gateway.

When a system wants to communicate with another device, it first determines whether the host is on the local network or a remote network. If the host is on a remote network, the system looks in the routing table to determine whether it has an entry for the network on which the remote host resides. If it does, it uses that route. If it does not, the data is sent to the default gateway.

Note

Although it might seem obvious, it's worth mentioning that the default gateway must be on the same network as the nodes that use it.

In essence, the default gateway is simply the path out of the network for a given device. Figure 3.1 shows how a default gateway fits into a network infrastructure.

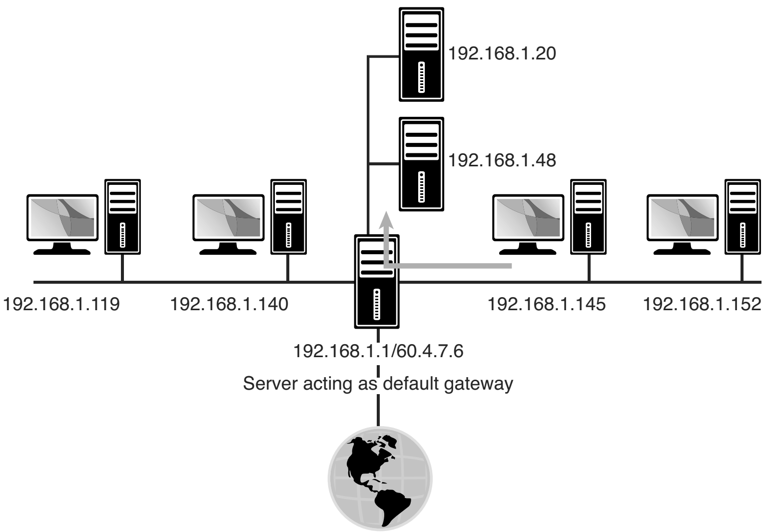


FIGURE 3.1 **The role of a default gateway.**

On the network, a default gateway could be a router or a computer with network interfaces for all segments to which it is connected. These interfaces have local IP addresses for the respective segments. If a system is not configured with any static routes or a default gateway, it is limited to operating on its own network segment.

ExamAlert

If a system is not configured with any static routes or a default gateway, it is limited to operating on its own network segment.

IPv4 Address Types

IPv4 has three primary address types: unicast, broadcast, and multicast. You need to distinguish between these three types of IPv4 addresses.

Unicast Address

With a *unicast address*, a single address is specified. Data sent with unicast addressing is delivered to a specific node identified by the address. It is a point-to-point address link.

Broadcast Address

A broadcast address is at the opposite end of the spectrum from a unicast address. A *broadcast address* is an IP address that you can use to target all systems on a subnet or network instead of single hosts. In other words, a broadcast message goes to everyone on the network.

Multicast

Multicasting is a mechanism by which groups of network devices can send and receive data between the members of the group at one time, instead of separately sending messages to each device in the group. The multicast grouping is established by configuring each device with the same multicast IP address.

IPv6 Addressing

Internet Protocol Version 4 (IPv4) has served as the Internet's protocol for almost 30 years. When IPv4 was in development 30 years ago, it would have been impossible for its creators to imagine or predict the future demand for IP devices and therefore IP addresses.

Note

Does the IETF assign protocol numbers using multiples of 2? Well, no. There was an IPv5. It was an experimental protocol that never went anywhere. But although IPv5 may have fallen into obscurity, because the name had been used, we got IPv6.

Where have all the IPv4 addresses gone?

IPv4 uses a 32-bit addressing scheme. This gives IPv4 a total of 4,294,967,296 possible unique addresses that can be assigned to IP devices. More than 4 billion addresses might sound like a lot, and it is. However, the number of IP-enabled devices increases daily at a staggering rate. Not all these addresses can be used by public networks. Many of these addresses are reserved and are unavailable for public use. This reduces the number of addresses that can be allocated as public Internet addresses.

The IPv6 project started in the mid-1990s, well before the threat of IPv4 limitations. Now network hardware and software are equipped for and ready to deploy IPv6 addressing. IPv6 offers a number of improvements. The most notable is its capability to handle growth in public networks. IPv6 uses a 128-bit addressing scheme, enabling a huge number of possible addresses:

340,282,366,920,938,463,463,374,607,431,768,211,456

Identifying IPv6 Addresses

As previously discussed, IPv4 uses a dotted-decimal format: 8 bits converted to its decimal equivalent and separated by periods. An example of an IPv4 address is 192.168.2.1.

Because of the 128-bit structure of the IPv6 addressing scheme, it looks quite a bit different. An IPv6 address is divided along 16-bit boundaries, and each 16-bit block is converted into a four-digit hexadecimal number and separated by colons. The resulting representation is called colon-hexadecimal. Now look at how it works. Figure 3.2 shows the IPv6 address 2001:0:4137:9e50:2811:34ff:3f57:febc from a Windows 7 system.

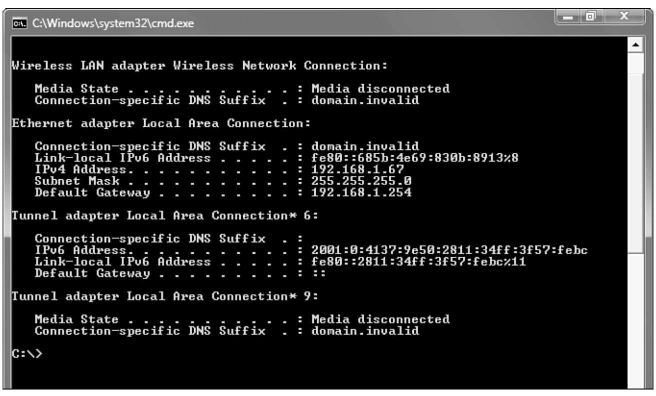


FIGURE 3.2 **An IPv6 address in a Windows 7 dialog screen.**

An IPv6 address can be simplified by removing the leading 0s within each 16-bit block. Not all the 0s can be removed, however, because each address block must have at least a single digit. Removing the 0 suppression, the address representation becomes

```
2001:0000:4137:9e50:2811:34ff:3f57:febc
```

Some of the IPv6 addresses you will work with have sequences of 0s. When this occurs, the number is often abbreviated to make it easier to read. In the preceding example you saw that a single 0 represented a number set in hexadecimal form. To further simplify the representation of IPv6 addresses, a contiguous sequence of 16-bit blocks set to 0 in colon hexadecimal format can be compressed to ::, known as the *double colon*.

For example, the IPv6 address of

```
2001:0000:0000:0000:3cde:37d1:3f57:fe93
```

can be compressed to

```
2001::3cde:37d1:3f57:fe93.
```

Of course, there are limits on how the IPv6 0s can be reduced. 0s within the IPv6 address cannot be eliminated when they are not first in the number sequence. For instance, 2001:4000:0000:0000:0000:0000:0000:0003 cannot be compressed as 2001:4::3. This would actually appear as 2001:4000::3.

When you look at an IPv6 address that uses a double colon, how do you know exactly what numbers are represented? The formula is to subtract the number of blocks from 8 and then multiply that number by 16. For example, the address 2001:4000::3 uses three blocks: 2001, 4000, and 3. So the formula is as follows:

$$(8 - 3) * 16 = 80$$

Therefore, the total number of bits represented by the double colon in this example is 80.

Note

You can remove 0s only once in an IPv6 address. Using a double colon more than once would make it impossible to determine the number of 0 bits represented by each instance of ::.

IPv6 Address Types

Another difference between IPv4 and IPv6 is in the address types. IPv4 addressing was discussed in detail earlier. IPv6 addressing offers several types of addresses, as detailed in this section.

Unicast IPv6 Addresses

As you might deduce from the name, a unicast address specifies a single interface. Data packets sent to a unicast destination travel from the sending host to the destination host. It is a direct line of communication. A few types of addresses fall under the unicast banner:

Global Unicast Addresses

Global unicast addresses are the equivalent of IPv4 public addresses. These addresses are routable and travel throughout the network.

Link-Local Addresses

Link-local addresses are designated for use on a single local network. Link-local addresses are automatically configured on all interfaces. This automatic configuration is comparable to the 169.254.0.0/16 APIPA automatically assigned IPv4 addressing scheme. The prefix used for a link-local address is fe80::/64. On a single-link IPv6 network with no router, link-local addresses are used to communicate between devices on the link.

Site-Local Addresses

Site-local addresses are equivalent to the IPv4 private address space (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16). As with IPv4, in which private address ranges are used in private networks, IPv6 uses site-local addresses that do not interfere with global unicast addresses. In addition, routers do not forward site-local traffic outside the site. Unlike link-local addresses, site-local addresses are not automatically configured and must be assigned through either stateless or stateful address configuration processes. The prefix used for the site-local address is FEC0::/10.

Multicast Addresses

As with IPv4 addresses, multicasting sends and receives data between groups of nodes. It sends IP messages to that group rather than to every node on the LAN (broadcast) or just one other node (unicast).

Anycast Addresses

Anycast addresses represent the middle ground between unicast addresses and multicast addresses. Anycast delivers messages to any one node in the multicast group.

Note

You might encounter the terms *stateful* and *stateless* configuration. *Stateless* refers to IP autoconfiguration, in which administrators need not manually input configuration information. In a *stateful* configuration network, devices obtain address information from a server.

ExamAlert

Earlier you read that IPv4 reserves 127.0.0.1 as the loopback address. IPv6 has the same reservation. IPv6 addresses 0:0:0:0:0:0:0:0 and 0:0:0:0:0:0:0:1 are reserved as the loopback addresses.

ExamAlert

Remember that fe80:: is a private link-local address.

Comparing IPv4 and IPv6 Addressing

Table 3.5 compares IPv4 and IPv6 addressing.

Note

Automatic Private IP Addressing (APIPA) appears in the table and is discussed in detail in the section “Automatic Private IP Addressing (APIPA)” later in this chapter.

TABLE 3.5 **Comparing IPv4 and IPv6 Addressing**

Address Feature	IPv4 Address	IPv6 Address
Loopback address	127.0.0.1	0:0:0:0:0:0:0:1 (::1)
Network-wide addresses	IPv4 public address ranges	Global unicast IPv6 addresses
Private network addresses	10.0.0.0 172.16.0.0 192.168.0.0	Site-local address ranges (FEC0::)
Autoconfigured addresses	IPv4 automatic private IP addressing (169.254.0.0)	Link-local addresses of the FE80:: prefix

ExamAlert

Make sure you know the information provided in Table 3.5.

Assigning IP Addresses

Now that you understand the need for each system on a TCP/IP-based network to have a unique address, the following sections examine how those systems receive their addresses.

Static Addressing

Static addressing refers to the manual assignment of IP addresses to a system. This approach has two main problems:

- Statically configuring one system with the correct address is simple, but in the course of configuring, say, a few hundred systems, mistakes are likely to be made. If the IP addresses are entered incorrectly, the system probably cannot connect to other systems on the network.
- If the IP addressing scheme for the organization changes, each system must again be manually reconfigured. In a large organization with hundreds or thousands of systems, such a reconfiguration could take a considerable amount of time. These drawbacks of static addressing are so significant that nearly all networks use dynamic IP addressing.

Dynamic Addressing

Dynamic addressing refers to the automatic assignment of IP addresses. On modern networks, the mechanism used to do this is Dynamic Host Configuration Protocol (DHCP). DHCP, part of the TCP/IP suite, enables a central system to provide client systems with IP addresses. Automatically assigning addresses with DHCP alleviates the burden of address configuration and reconfiguration that occurs with static IP addressing.

The basic function of the DHCP service is to automatically assign IP addresses to client systems. To do this, ranges of IP addresses, known as *scopes*, are defined on a system running a DHCP server application. When another system configured as a DHCP client is initialized, it asks the server for an address. If all things are as they should be, the server assigns an address to the client for a predetermined amount of time, which is known as the *lease*, from the scope.

A DHCP server typically can be configured to assign more than just IP addresses. It often is used to assign the subnet mask, the default gateway, and Domain Name Service (DNS) information.

Using DHCP means that administrators do not need to manually configure each client system with a TCP/IP address. This removes the common problems associated with statically assigned addresses, such as human error. The potential problem of assigning duplicate IP addresses is also eliminated. DHCP also removes the need to reconfigure systems if they move from one subnet to another, or if you decide to make a wholesale change in the IP addressing structure.

Note

Even when a network is configured to use DHCP, several mission-critical network systems continue to use static addressing: DHCP server, DNS server, web server, and more. They do not have dynamic IP addressing because their IP addresses can never change. If they do, client systems may be unable to access the resources from that server.

Configuring a client for TCP/IP can be relatively complex, or it can be simple. Any complexity involved is related to the possible need to manually configure TCP/IP. The simplicity is because TCP/IP configuration can occur automatically via DHCP or through APIPA. At the least, a system needs an IP address and subnet mask to log on to a network. The default gateway and DNS server IP information is optional, but network functionality is limited without them. The following list briefly explains the IP-related settings used to connect to a TCP/IP network:

- **IP address**: Each system must be assigned a unique IP address so that it can communicate on the network.
- **Subnet mask**: Enables the system to determine what portion of the IP address represents the network address and what portion represents the node address.
- **Default gateway**: Enables the system to communicate on a remote network, without the need for explicit routes to be defined.
- **DNS server addresses**: Enable dynamic hostname resolution to be performed. It is common practice to have two DNS server addresses defined so that if one server becomes unavailable, the other can be used.

ExamAlert

At the very minimum, an IP address and subnet mask are required to connect to a TCP/IP network. With just this minimum configuration, connectivity is limited to the local segment, and DNS resolution is not possible.

BOOT Protocol (BOOTP)

BOOTP was originally created so that diskless workstations could obtain information needed to connect to the network, such as the TCP/IP address, subnet mask, and default gateway. Such a system was necessary because diskless workstations had no way to store the information.

When a system configured to use BOOTP is powered up, it broadcasts for a BOOTP server on the network. If such a server exists, it compares the MAC address of the system issuing the BOOTP request with a database of entries. From this database, it supplies the system with the appropriate information. It can also notify the workstation about a file that it must run on BOOTP.

In the unlikely event that you use BOOTP, you should be aware that, like DHCP, it is a broadcast-based system. Therefore, routers must be configured to forward BOOTP broadcasts.

Automatic Private IP Addressing (APIPA)

Automatic Private IP Addressing (APIPA) was introduced with Windows 98 and has been included in all subsequent Windows versions. The function of APIPA is that a system can give itself an IP address if it is incapable of receiving an address dynamically from a DHCP server. Then APIPA assigns the system an address from the 169.254.0.0 address range and configures an appropriate subnet mask (255.255.0.0). However, it doesn't configure the system with a default gateway address. As a result, communication is limited to the local network.

ExamAlert

If a system that does not support APIPA cannot get an address from a DHCP server, it typically assigns itself an IP address of 0.0.0.0. Keep this in mind when troubleshooting IP addressing problems on non-APIPA platforms.

The idea behind APIPA is that systems on a segment can communicate with each other if DHCP server failure occurs. In reality, the limited usability of APIPA makes it little more than a last resort. For example, imagine that a system is powered on while the DHCP server is operational and receives an IP address of 192.168.100.2. Then the DHCP server fails. Now, if the other systems on the segment are powered on and cannot get an address from the DHCP server because it is down, they would self-assign addresses in the 169.254.0.0 address range via APIPA. The systems with APIPA addresses would talk to each other, but they couldn't talk to a system that received an address from the DHCP server. Likewise, any system that receives an IP address via DHCP cannot talk to systems with APIPA-assigned addresses. This, and the absence of a default gateway, is why APIPA is of limited use in real-world environments.

> Exam**Alert**
>
> Be prepared to answer APIPA questions. Know what it is and how you can tell if you have been assigned an APIPA address and why.

Identifying MAC Addresses

Many times this book refers to MAC addresses and how certain devices use them. However, it has not yet discussed why MAC addresses exist, how they are assigned, and what they consist of.

> Note
>
> A MAC address is sometimes called a *physical address* because it is physically embedded in the interface.

A MAC address is a 6-byte (48-bit) hexadecimal address that enables a NIC to be uniquely identified on the network. The MAC address forms the basis of network communication, regardless of the protocol used to achieve network connection. Because the MAC address is so fundamental to network communication, mechanisms are in place to ensure that duplicate addresses cannot be used.

To combat the possibility of duplicate MAC addresses being assigned, the Institute of Electrical and Electronics Engineers (IEEE) took over the assignment of MAC addresses. But rather than be burdened with assigning individual addresses, the IEEE decided to assign each manufacturer an ID and then let the manufacturer further allocate IDs. The result is that in a MAC address, the first 3 bytes define the manufacturer, and the last 3 are assigned by the manufacturer.

For example, consider the MAC address of the computer on which this book is being written: 00:D0:59:09:07:51. The first 3 bytes (00:D0:59) identify the manufacturer of the card; because only this manufacturer can use this address, it is known as the *Organizational Unique Identifier (OUI)*. The last 3 bytes (09:07:51) are called the *Universal LAN MAC address*: They make this interface unique. You can find a complete listing of organizational MAC address assignments at http://standards.ieee.org/regauth/oui/oui.txt.

ExamAlert

Because MAC addresses are expressed in hexadecimal, only the numbers 0 through 9 and the letters A through F can be used in them. If you get an exam question about identifying a MAC address and some of the answers contain letters and numbers other than 0 through 9 and the letters A through F, you can immediately discount those answers.

You can discover the NIC's MAC address in various ways, depending on what system or platform you work on. Table 3.6 defines various platforms and methods you can use to view an interface's MAC address.

TABLE 3.6 **Methods of Viewing the MAC Addresses of NICs**

Platform	Method
Windows 2003/2008/XP/Vista/7	Enter `ipconfig /all` at a command prompt.
Linux/some Unix	Enter the `ifconfig -a` command.
Novell NetWare	Enter the `config` command.
Cisco router	Enter the `sh int interface name` command.

ExamAlert

Be sure you know the commands used to identify the MAC address in various operating system formats.

Network Address Translation (NAT) and Port Address Translation (PAT)

This chapter has defined many acronyms and continues with two more: NAT and PAT.

NAT

The basic principle of NAT is that many computers can "hide" behind a single IP address. The main reason you need to do this (as pointed out earlier in the section "IP Addressing") is because there simply aren't enough IPv4 addresses to go around. Using NAT means that only one registered IP address is needed on the system's external interface, acting as the gateway between the internal and external networks.

> **Note**
>
> Don't confuse NAT with proxy servers. The proxy service is different from NAT, but many proxy server applications do include NAT functionality.

NAT enables you to use whatever addressing scheme you like on your internal networks; although, it is common practice to use the private address ranges, which were discussed earlier.

When a system is performing NAT, it funnels the requests given to it to the Internet. To the remote host, the request looks like it is originating from a single address. The system performing the NAT function keeps track of who asked for what and makes sure that when the data is returned, it is directed to the correct system. Servers that provide NAT functionality do so in different ways. For example, you can statically map a specific internal IP address to a specific external one (known as the *one-to-one NAT method*) so that outgoing requests are always tagged with the same IP address. Alternatively, if you have a group of public IP addresses, you can have the NAT system assign addresses to devices on a first-come, first-served basis. Either way, the basic function of NAT is the same.

There is a transition technology known as Teredo that gives full IPv6 connectivity for IPv6-capable hosts, which are on the IPv4 Internet but lack direct native connection to an IPv6 network. The distinguishing feature of Teredo is that it can do this from behind network address translation (NAT) devices (such as home routers). You can find more information on this at http://ipv6.com/articles/nat/NAT-In-Depth.htm.

PAT

NAT enables administrators to conserve public IP addresses and, at the same time, secure the internal network. Port Address Translation (PAT) is a variation on NAT. With PAT, all systems on the LAN are translated to the same IP address, but with a different port number assignment. PAT is used when multiple clients want to access the Internet. However, with not enough available public IP addresses, you need to map the inside clients to a single public IP address. When packets come back into the private network, they are routed to their destination with a table within PAT that tracks the public and private port numbers.

When PAT is used, there is a typically only a single IP address exposed to the public network, and multiple network devices access the Internet through this exposed IP address. The sending devices, IP address, and port number are not exposed. For example, an internal computer with the IP address of 192.168.2.2 wants to access a remote Web server at address 204.23.85.49. The request goes to the PAT router where the sender's private IP and port number are modified, and a mapping is added to the PAT table. The remote web server sees the request coming from the IP address of the PAT router and not the computer actually making the request. The web server sends the reply to the address and port number of the router. When received, the router checks its table to see the packet's actual destination and forwards it.

ExamAlert

PAT enables nodes on a LAN to communicate with the Internet without revealing their IP address. All outbound IP communications are translated to the router's external IP address. Replies come back to the router that then translates them back into the private IP address of the original host for final delivery.

Static NAT is a simple form of NAT. Static Network Address Translation (SNAT) directly maps a private IP address to a static unchanging public IP address. This enables an internal system, such as a mail server, to have an unregistered (private) IP address and still be reachable over the Internet. For example, if a network uses a private address of 192.168.2.1 for a mail server, it can be statically linked to a public IP address such as 213.23.213.85.

Cram Quiz

1. What is the IPv6 equivalent of 127.0.0.1? (Choose two.)
   - ❍ **A.** 0:0:0:0:0:0:0:1
   - ❍ **B.** 0:0:0:0:0:0:0:24
   - ❍ **C.** ::1
   - ❍ **D.** ::24

2. Which of the following is a Class B address?
   - ❍ **A.** 129.16.12.200
   - ❍ **B.** 126.15.16.122
   - ❍ **C.** 211.244.212.5
   - ❍ **D.** 193.17.101.27

3. You are the administrator for a network with two Windows Server systems and 65 Windows 7 systems. At 10 a.m., three users call to report that they are experiencing network connectivity problems. Upon investigation, you determine that the DHCP server has failed. How can you tell that the DHCP server failure is the cause of the connectivity problems experienced by the three users?
   - ❍ **A.** When you check their systems, they have an IP address of 0.0.0.0.
   - ❍ **B.** When you check their systems, they have an IP address in the 192.168.x.x address range.
   - ❍ **C.** When you check their systems, they have a default gateway value of 255.255.255.255.
   - ❍ **D.** When you check their systems, they have an IP address from the 169.254.x.x range.

4. Which of the following address types are associated with IPv6? (Choose three.)
   - ❍ **A.** Broadcast
   - ❍ **B.** Multicast
   - ❍ **C.** Unicast
   - ❍ **D.** Anycast

5. Which of the following IP addresses is not from a private address range?
   - ❍ **A.** 192.168.200.117
   - ❍ **B.** 172.16.3.204
   - ❍ **C.** 127.45.112.16
   - ❍ **D.** 10.27.100.143

6. You have been assigned to set up a new network with TCP/IP. For the external interfaces, you decide to obtain registered IP addresses from your ISP, but for the internal network, you choose to configure systems by using one of the private address ranges. Of the following address ranges, which one would you not consider?

❍ **A.** 192.168.0.0 to 192.168.255.255

❍ **B.** 131.16.0.0 to 131.16.255.255

❍ **C.** 10.0.0.0 to 10.255.255.255

❍ **D.** 172.16.0.0 to 172.31.255.255

7. You ask your ISP to assign a public IP address for the external interface of your Windows 2008 server, which is running a proxy server application. In the email message you get that contains the information, the ISP tells you that you have been assigned the IP address 203.15.226.12/24. When you fill out the subnet mask field on the IP configuration dialog box on your system, what subnet mask should you use?

❍ **A.** 255.255.255.255

❍ **B.** 255.255.255.0

❍ **C.** 255.255.240.0

❍ **D.** 255.255.255.240

8. Examine the diagram shown here. What is the most likely reason that user Spencer cannot communicate with user Evan?

❍ **A.** The default gateways should have different values.

❍ **B.** Spencer's IP address is not a loopback address.

❍ **C.** The subnet values should be the same.

❍ **D.** There is no problem identifiable by the values given.

User: Evan
IP address: 192.168.1.121
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1

User: Spencer
IP address: 192.168.1.127
Subnet mask: 255.255.248.0
Default gateway: 192.168.1.1

Cram Quiz Answers

1. **A** and **C.** The IPv4 address 127.0.0.1 is reserved as the loopback address, and IPv6 has the same reservation. IPv6 addresses 0:0:0:0:0:0:0:0 and 0:0:0:0:0:0:0:1 are reserved as the loopback addresses. The address 0:0:0:0:0:0:0:1 can be shown using the :: notation with the 0s removed, resulting in ::1.
2. **A.** Class B addresses fall into the range 128 to 191. Answer A is the only address listed that falls into that range. Answer B is a Class A address, and answers C and D are Class C IP addresses.
3. **D.** When a Windows 7 system that is configured to obtain an IP address via DHCP fails to obtain an address, it uses APIPA to assign itself an address from the 169.254.x.x address range. An address of 0.0.0.0 normally results from a system that does not support APIPA. APIPA does not use the 192.168.x.x address range. The IP address 255.255.255.255 is the broadcast address. A DHCP failure would not lead to a system assigning itself this address.
4. **B, C,** and **D.** A key difference between IPv4 and IPv6 is in the address types. IPv6 addressing has three main types of addresses: unicast, multicast, and anycast. IPv4 uses broadcast addressing, but IPv6 doesn’t.
5. **C.** The 127.x.x.x network range is reserved for the loopback function. It is not one of the recognized private address ranges. The private address ranges as defined in RFC 1918 are 10.x.x.x, 172.16.x.x to 172.31.x.x, and 192.168.x.x.
6. **B.** The 131.16 range is from the Class B range and is not one of the recognized private IP address ranges. All the other address ranges are valid private IP address ranges.
7. **B.** In CIDR terminology, the number of bits to be included in the subnet mask is expressed as a slash value. If the slash value is 24, the first three octets form the subnet mask, so the value is 255.255.255.0.
8. **C.** The most likely problem, given the IP values for each user’s workstation, is that the subnet value is not correct on Spencer’s machine and should be 255.255.255.0.

Understanding TCP/UDP Port Functions

- **Identify common TCP and UDP default ports.**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. What is the default port used by NTP?
2. True or False: Although FTP is a TCP-based protocol, TFTP uses UDP.

Answers

1. By default, NTP uses port 123.
2. True. Although FTP is a TCP-based protocol, TFTP uses UDP.

Each TCP/IP or application has a port associated with it. When a communication is received, the target port number is checked to determine which protocol or service it is destined for. The request is then forwarded to that protocol or service. For example, consider HTTP, whose assigned port number is 80. When a web browser forms a request for a web page, that request is sent to port 80 on the target system. When the target system receives the request, it examines the port number. When it sees that the port is 80, it forwards the request to the web server application.

TCP/IP has 65,535 ports available, with 0 to 1023 labeled as the well-known ports. Although a detailed understanding of the 65,535 ports is not necessary for the Network+ exam, you need to understand the numbers of some well-known ports. Network administration often requires you to specify port assignments when you work with applications and configuring services. Table 3.7 shows some of the most common port assignments.

ExamAlert

You should concentrate on the information provided in Table 3.7 and answer any port-related questions you might receive. The exam may present you with a situation in which you can't access a particular service; you may have to determine whether a port is open or closed on a firewall.

TABLE 3.7 **TCP/IP Port Assignments for Commonly Used Protocols**

Protocol	Port Assignment
TCP Ports	
FTP	20
FTP	21
SSH	22
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110
NNTP	119
NTP	123
IMAP4	143
HTTPS	443
RDP	3389
UDP Ports	
TFTP	69
DNS	53
DHCP (and BOOTP server)	67
DHCP (and BOOTP client)	68
SNMP	161
RDP	3389

ExamAlert

The term *well-known ports* identifies the ports ranging from 0 to 1023. When CompTIA says to "identify the well-known ports," this is what it refers to.

Note

You might have noticed in Table 3.7 that two ports are associated with FTP. Port 20 is considered the data port, whereas port 21 is considered the control port. In practical use, FTP connections use port 21. Port 20 is rarely used in modern implementations.

Cram Quiz

1. As the network administrator, you decide to block port 80. Which of the following services will be unavailable for network users?
   - ❍ **A.** DNS
   - ❍ **B.** POP3
   - ❍ **C.** FTP
   - ❍ **D.** HTTP

2. Which of the following is the most commonly used port for FTP in modern implementations?
   - ❍ **A.** 20
   - ❍ **B.** 21
   - ❍ **C.** 23
   - ❍ **D.** 27

Cram Quiz Answers

1. **D.** The HTTP service uses port 80, so blocking port 80 prevents users from using the HTTP service. Answer A is incorrect because DNS uses port 53. Answer B is incorrect because POP3 uses port 110. Answer C is incorrect because FTP uses port 21.
2. **B.** The most commonly used port for FTP in modern implementations is 21.

Managing TCP/IP Routing

- **Explain the purpose and properties of routing and switching.**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. What are the most common distance-vector routing protocols?
2. What are the most common link-state protocols?
3. What is convergence?

Answers

1. Distance-vector routing protocols include RIP, RIPv2, BGP, and EIGRP.
2. Link-state protocols include OSPF and IS-IS.
3. Convergence represents the time it takes routers to detect change on the network.

Because today's networks branch out between interconnected offices all over the world, networks may have any number of separate physical network segments connected using routers. Routers are devices that direct data between networks. Essentially, when a router receives data, it must determine the destination for the data and send it there. To accomplish this, the network router uses two key pieces of information: the gateway address and the routing tables.

The Default Gateway

A default gateway is the router's IP address, which is the pathway to any and all remote networks. To get a packet of information from one network to another, the packet is sent to the default gateway, which helps forward the packet to its destination network. Computers that live on the other side of routers are said to be on remote networks. Without default gateways, Internet communication is not possible because your computer doesn't have a way to send a packet destined for any other network. On the workstation, it is common for the default gateway option to be configured automatically through DHCP configuration.

Routing Tables

Before a data packet is forwarded, a chart is reviewed to determine the best possible path for the data to reach its destination. This chart is the computer's routing table. Maintaining an accurate routing table is essential for effective data delivery. Every computer on a TCP/IP network has a routing table stored locally. Figure 3.3 shows the routing table on a Windows 7 system.

> **Note**
>
> The `route print` command can be used to view the routing table on a client system.

As shown in Figure 3.3, the information in the routing table includes the following:

- **Destination**: The host IP address.
- **Network mask**: The subnet mask value for the destination parameter.
- **Gateway**: Where the IP address is sent. This may be a gateway server, router, or another system acting as a gateway.
- **Interface**: The address of the interface that's used to send the packet to the destination.
- **Metric**: A measurement of the directness of a route. The lower the metric, the faster the route. If multiple routes exist for data to travel, the one with the lowest metric is chosen.

Routing tables play an important role in the network routing process. They are the means by which the data is directed through the network. For this reason, a routing table needs to be two things. It must be up to date and complete. The router can get the information for the routing table in two ways: through static routing or dynamic routing.

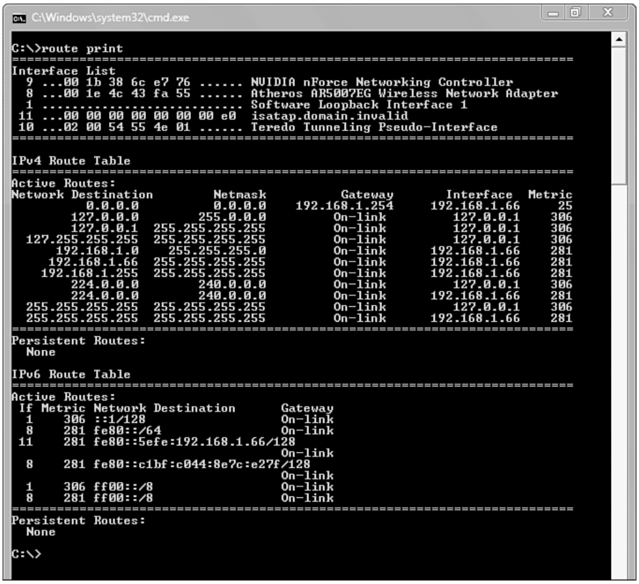


FIGURE 3.3 **The routing table on a Windows 7 system.**

Static Routing

In environments that use *static routing*, routes and route information are manually entered into the routing tables. Not only can this be a time-consuming task, but also errors are more common. In addition, when a change occurs to the network's layout, or topology, statically configured routers must be manually updated with the changes. Again, this is a time-consuming and potentially error-laden task. For these reasons, static routing is suited to only the smallest environments, with perhaps just one or two routers. A far more practical solution, particularly in larger environments, is to use dynamic routing.

You can add a static route to a routing table using the `route add` command. To do this, specify the route, the network mask, and the destination IP address of the network card your router will use to get the packet to its destination network.

The syntax for the `route add` command is as follows:

```
route add 192.168.2.1 mask (255.255.255.0) 192.168.2.4
```

Adding a static address is not permanent; in other words, it will most likely be gone when the system reboots. To make it persistent (the route is still in the routing table on boot), you can use the switch with the command.

ExamAlert

The `route add` command adds a static route to the routing table. The `route add` command with the `-p` switch makes the static route persistent. You may want to try this on your own before taking the Network+ exam.

Dynamic Routing

In a *dynamic routing* environment, routers use special routing protocols to communicate. The purpose of these protocols is simple: They enable routers to pass on information about themselves to other routers so that other routers can build routing tables. Two types of routing protocols are used: the older distance-vector protocols and the newer link-state protocols.

Distance-Vector Routing

With distance-vector router communications, each router on the network communicates all the routes it knows about to the routers to which it is directly attached. In this way, routers communicate only with their router neighbors and are unaware of other routers that may be on the network.

The communication between distance-vector routers is known as *hops*. On the network, each router represents one hop, so a network using six routers has five hops between the first and last router.

The `tracert` command is used in a Windows environment to see how many hops a packet takes to reach a destination. To try this at the command prompt, enter `tracert comptia.org`. Figure 3.4 shows an example of the output on a Windows 7 workstation.

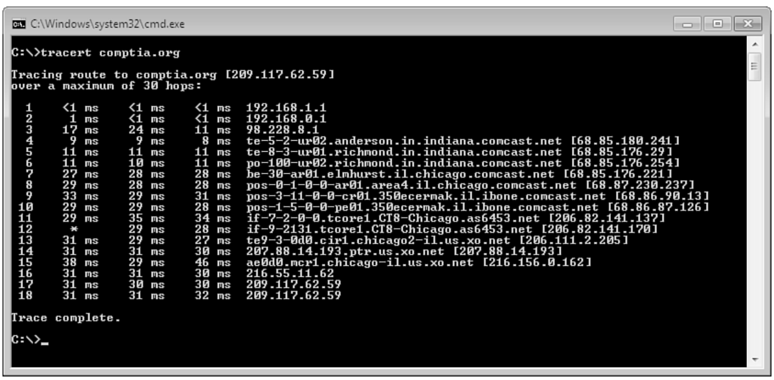


FIGURE 3.4 **The results of running tracert on a Windows 7 system.**

Several distance-vector protocols are in use today, including Routing Information Protocol (RIP and RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP):

- **RIP**: As mentioned, RIP is a distance-vector routing protocol. RIP is limited to a maximum of 15 hops. One of the downsides of the protocol is that the original specification required router updates to be transmitted every 30 seconds. On smaller networks this is acceptable; however, this can result in a huge traffic load on larger networks. The original RIP specification also did not support router authentication, leaving it vulnerable to attacks.
- **RIPv2**: The second version of RIP dealt with the shortcomings of the original design. Authentication was included to enable secure transmissions, also, it changed from a networkwide broadcast discovery method to a multicast method to reduce overall network traffic. However, to maintain compatibility with RIP, RIPv2 still supports a limit of 15 hops.
- **BGP**: A routing protocol often associated with the Internet. BGP can be used between gateway hosts on the Internet. BGP examines the routing table, which contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. BGP communicates between the routers using TCP.
- **EIGRP**: A protocol that enables routers to exchange information more efficiently than earlier network protocols. EIGRP uses its neighbors to help determine routing information. Routers configured to use EIGRP keep copies of their neighbors' routing information and query these tables to help find the best possible route for transmissions to follow. EIGRP uses Diffusing Update Algorithm (DUAL) to determine the best route to a destination.

ExamAlert

Be sure you can identify the differences between the distance-vector protocols discussed here.

Distance-vector routing protocols operate by having each router send updates about all the other routers it knows about to the routers directly connected to it. The routers use these updates to compile their routing tables. The updates are sent automatically every 30 or 60 seconds. The interval depends on the routing protocol used. Apart from the periodic updates, routers can also be configured to send a *triggered update* if a change in the network topology is detected. The process by which routers learn of a change in the network topology is called *convergence*.

Routing loops can occur on networks with slow convergence. Routing loops occur when the routing tables on the routers are slow to update and a redundant communication cycle is created between routers. Two strategies can combat potential routing loops:

- **Split horizon**: Works by preventing the router from advertising a route back to the other router from which it was learned. This prevents two nodes from bouncing packets back and forth between them, creating a loop.
- **Poison reverse (also called split horizon with poison reverse)**: Dictates that the route *is* advertised back on the interface from which it was learned, but it has a hop count of infinity, which tells the node that the route is unreachable.

ExamAlert

If a change in the routing is made, it takes some time for the routers to detect and accommodate this change. This is known as convergence.

Although distance-vector protocols can maintain routing tables, they have three problems:

- The periodic update system can make the update process slow.
- The periodic updates can create large amounts of network traffic—much of the time unnecessarily, because the network's topology should rarely change.
- Perhaps the most significant problem is that because the routers know about only the next hop in the journey, incorrect information can be propagated between routers, creating routing loops.

ExamAlert

Know that "next hop" in routing is the next closest router that a packet can go through.

Link-State Routing

A router that uses a link-state protocol differs from a router that uses a distance-vector protocol because it builds a map of the entire network and then holds that map in memory. On a network that uses a link-state protocol, routers send link-state advertisements (LSAs) that contain information about the networks to which they connect. The LSAs are sent to every router on the network, thus enabling the routers to build their network maps.

When the network maps on each router are complete, the routers update each other at a given time, just like with a distance-vector protocol; however, the updates occur much less frequently with link-state protocols than with distance-vector protocols. The only other circumstance under which updates are sent is if a change in the topology is detected, at which point the routers use LSAs to detect the change and update their routing tables. This mechanism, combined with the fact that routers hold maps of the entire network, makes convergence on a link-state-based network quickly occur.

Although it might seem like link-state protocols are an obvious choice over distance-vector protocols, routers on a link-state-based network require more powerful hardware and more RAM than those on a distance-vector-based network. Not only do the routing tables need to be calculated, but they must also be stored. A router that uses distance-vector protocols need only maintain a small database of the routes accessible by the routers to which it is directly connected. A router that uses link-state protocols must maintain a database of all the routers in the entire network.

Link-state protocols include the following:

- **Open Shortest Path First (OSPF)**: A link-state routing protocol based on the SPF (Shortest Path First) algorithm to find the least-cost path to any destination in the network. In operation, each router using OSPF sends a list of its neighbors to other routers on the network. From this information, routers can determine the network design and the shortest path for data to travel.
- **Intermediate System-to-Intermediate System (IS-IS)**: A link-state protocol that discovers the shortest path for data to travel using the shortest path first (SPF) algorithm. IS-IS routers distribute topology information to other routers, enabling them to make the best path decisions.

So what's the difference between the two? OSPF (a network layer protocol) is more often used in medium to large enterprise networks because of its special tunneling features. IS-IS is more often used in large ISP networks because of its stability features and that it can support more routers.

IGP Versus EGP

Now that routing protocols have been discussed, you need to understand the difference between Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). An IGP identifies the protocols used to exchange routing information between routers within a LAN or interconnected LANs. IGP is not a protocol itself but describes a category of link-state routing protocols that support a single, confined geographic area such as a LAN. IGPs fall into two categories: distance-vector protocols, which include RIP and IGRP, and link-state protocols, which include OSPF and IS-IS.

Whereas IGPs are geographically confined, EGPs are used to route information outside the network, such as on the Internet. On the Internet, an EGP is required. An EGP is a distance-vector protocol commonly used between hosts on the Internet to exchange routing table information. BGP is an example of an EGP.

Exam**Alert**

Be prepared to identify both the link-state and distance-vector routing protocols used on TCP/IP networks.

Routing Metrics

Following are a number of metrics related to routing that you should know for the exam:

- *Hop counts* are the number of hops necessary to reach a node. A hop count of infinity means the route is unreachable.
- The *Maximum Transmission Unit (MTU)* defines the largest data unit that can be passed without fragmentation.
- *Bandwidth* specifies the maximum packet size permitted for Internet transmission.
- *Costs* are the numbers associated with traveling from point A to point B (often hops). The lower the total costs (the less links in the route), the more that route should be favored.
- *Latency* is the amount of time it takes for a packet to travel from one location to another.

Cram Quiz

1. Which of the following best describes the function of the default gateway?
   - ❍ **A.** It provides the route for destinations outside the local network.
   - ❍ **B.** It enables a single Internet connection to be used by several users.
   - ❍ **C.** It identifies the local subnet and formulates a routing table.
   - ❍ **D.** It is used to communicate in a multiple-platform environment.

2. What is the term used for the number of hops necessary to reach a node?
   - ❍ **A.** Jump list
   - ❍ **B.** Link stops
   - ❍ **C.** Connections
   - ❍ **D.** Hop count

Cram Quiz Answers

1. **A.** The default gateway enables systems on one local subnet to access those on another. Answer B does not accurately describe the role of the default gateway. Answers C and D don't describe the main function of a default gateway, which is to provide the route for destinations outside the local network.
2. **D.** The hop count is the number of hops necessary to reach a node.

Configuring Routers and Switches

- **Given a scenario, install and configure routers and switches.**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. Which technology enables electrical power to transmit over twisted-pair Ethernet cable?
2. True or False: With the help of FSL, STP avoids or eliminates loops on Layer 2 bridges.

Answers

1. Power over Ethernet (PoE) is the technology that enables electrical power to transmit over twisted-pair Ethernet cable.
2. False. With the help of Spanning Tree Algorithm (STA), STP avoids or eliminates loops on a Layer 2 bridge.

The next chapter focuses on actual hardware components of a network, but the reason for the hardware is to carry out the operations discussed in this chapter. This section looks at a few of the more advanced features that routers and switches perform.

Power over Ethernet (PoE)

The purpose of Power over Ethernet (PoE) is pretty much described in its name. Essentially, PoE is a technology that enables electrical power to transmit over twisted-pair Ethernet cable. The power transfers, along with data, to provide power to remote devices. These devices may include remote switches, wireless access points, voice over IP (VoIP) equipment, and more.

One of the key advantages of PoE is the centralized management of power. For instance, without PoE, all remote devices need to be independently powered. In the case of a power outage, each of these devices requires an uninterruptible power supply (UPS) to continue operating. A UPS is a battery pack that enables devices to operate for a period of time. With PoE supplying power, a UPS is required only in the main facility. In addition, centralized power management enables administrators to power up or down remote equipment.

> **Note**
>
> VLAN and spanning tree were outlined in the CompTIA objectives for this chapter. Spanning tree is covered next. VLANs are discussed in Chapter 1, "Introduction to Networking."

The Spanning Tree Protocol (STP)

An Ethernet network can have only a single active path between devices on a network. When multiple active paths are available, switching loops can occur. Switching loops are simply the result of having more than one path between two switches in a network. Spanning Tree Protocol (STP) is designed to prevent these loops from occurring.

STP is used with network bridges and switches. With the help of Spanning Tree Algorithm (STA), STP avoids or eliminates loops on a Layer 2 bridge.

> **Note**
>
> As a heads-up, talking about STP refers to Layer 2 of the OSI model. Both bridges and switches work at Layer 2. Routers work at Layer 3.

STA enables a bridge or switch to dynamically work around loops in a network's topology. Both STA and STP were developed to prevent loops in the network and provide a way to route around any failed network bridge or ports. If the network topology changes, or if a switch port or bridge fails, STA creates a new spanning tree, notifies the other bridges of the problem, and routes around it. STP is the protocol, and STA is the algorithm STP uses to correct loops.

If a particular port has a problem, STP can perform a number of actions, including blocking the port, disabling the port, or forwarding data destined for that port to another port. It does this to ensure that no redundant links or paths are found in the spanning tree and that only a single active path exists between any two network nodes.

STP uses bridge protocol data units (BPDUs) to identify the status of ports and bridges across the network. BPDUs are simple data messages exchanged between switches. BPDUs contain information on ports and provide the status of those ports to other switches. If a BPDU message finds a loop in the network, it is managed by shutting down a particular port or bridge interface.

Redundant paths and potential loops can be avoided within ports in several ways:

- **Blocking**: A blocked port accepts BPDU messages but does not forward them.
- **Disabled**: The port is offline and does not accept BPDU messages.
- **Forwarding**: The port is part of the active spanning tree topology and forwards BPDU messages to other switches.
- **Learning**: In a learning state, the port is not part of the active spanning tree topology but can take over if another port fails. Learning ports receive BPDUs and identify changes to the topology when made.
- **Listening**: A listening port receives BPDU messages and monitors for changes to the network topology.

Most of the time, ports are in either a forwarding or blocked state. When a disruption to the topology occurs or a bridge or switch fails for some reason, listening and learning states are used.

Exam**Alert**

STP actively monitors the network, searching for redundant links. When it finds some, it shuts them down to prevent switching loops. STP uses STA to create a topology database to find and then remove the redundant links. With STP operating from the switch, data is forwarded on approved paths, which limits the potential for loops.

Trunking

In computer networking, the term *trunking* refers to the use of multiple network cables or ports in parallel to increase the link speed beyond the limits of any one cable or port. Sound confusing? If you have network experience, you might have heard the term *link aggregation*, which is essentially the same thing. It is just using multiple cables to increase the throughput. The higher-capacity trunking link is used to connect switches to form larger networks.

VLAN trunking—or *VLAN (trunking)*, as CompTIA lists it—is the application of trunking to the virtual LAN—now common with routers, firewalls, VMWare hosts, and wireless access points. VLAN trunking provides a simple and cheap way to offer a nearly unlimited number of virtual network connections. The requirements are only that the switch, the network adapter, and the OS drivers all support VLANs. The *VLAN Trunking Protocol (VTP)* is a proprietary protocol from Cisco for just such a purpose.

Port Mirroring

You need some way to monitor network traffic and monitor how well a switch works. This is the function of port mirroring. To use port mirroring, administrators configure a copy of all inbound and outbound traffic to go to a certain port. A protocol analyzer examines the data sent to the port and therefore does not interrupt the flow of regular traffic.

ExamAlert

Port mirroring enables administrators to monitor the traffic outbound and inbound to the switch.

Port Authentication

Port authentication is what it sounds like—authenticating users on a port-by-port basis. One standard that specifies port authentication is the 802.1X standard, often associated with wireless security. Systems that attempt to connect to a LAN port must be authenticated. Those who are authenticated can access the LAN; those who are not authenticated get no further. Chapter 10 provides more information on the 802.1X standard and port authentication.

Cram Quiz

1. Port mirroring enables administrators to monitor which traffic to the switch?
   - ❍ **A.** Inbound only
   - ❍ **B.** Outbound only
   - ❍ **C.** Inbound and outbound
   - ❍ **D.** Neither inbound nor outbound

2. Which of the following is NOT used to avoid redundant paths and potential loops within ports?
   - ❍ **A.** Blocking
   - ❍ **B.** Learning
   - ❍ **C.** Forwarding
   - ❍ **D.** Jamming

Cram Quiz Answers

1. **C.** Port mirroring enables administrators to monitor the traffic outbound and inbound to the switch.
2. **D.** The common methods to avoid redundant paths and potential loops within ports include blocking, disabled, forwarding, learning, and listening. Jamming is not one of the methods employed.

What Next?

Chapter 4, "Components and Devices," introduces you to commonly used networking devices. All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and are requirements for a Network+ candidate.

Index

Numerics

A

B

E

F

G

H

I

J

K

L

M

N

P

Q

R

S

U

V

W

X