PEARSON IT
CERTIFICATION

Cert Guide

Advance your IT career with hands-on learning

Practice Tests

Video Training

Flash Cards

Review Exercises

Labs

Interactive Study Guide

Study Planner

CompTIA®

Network+

N10-008

ANTHONY SEQUEIRA
CCIE® NO.15626

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

CompTIA® Network+ N10-008 Cert Guide

Anthony Sequeira, CCIE No. 15626

Pearson IT Certification

Pearson

CompTIA® Network+ N10-008 Cert Guide

Anthony Sequeira

ISBN-13: 978-0-13-744994-1

ISBN-10: 0-13-744994-1

Library of Congress Control Number: 2021911389

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Managing Editor
Sandra Schroeder

Development Editor
Christopher Cleveland

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Technical Editor
Chris Crayton

Editorial Assistant
Cindy Teeters

Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Ken Johnson

Proofreader
Charlotte Kughen

Warning and Disclaimer

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Figure	Attribution
Figure 2-1	Courtesy of Cisco Systems, Inc
Figure 2-2	Courtesy of Cisco Systems, Inc
Figure 2-3	Courtesy of Cisco Systems, Inc
Figure 2-4	Courtesy of Cisco Systems, Inc
Figure 2-5	Courtesy of Cisco Systems, Inc
Figure 2-6	Courtesy of Cisco Systems, Inc
Figure 2-7	Courtesy of Cisco Systems, Inc
Figure 2-8	Courtesy of Cisco Systems, Inc
Figure 2-10	Courtesy of Cisco Systems, Inc
Figure 2-11	Courtesy of Cisco Systems, Inc
Figure 2-12	Courtesy of Cisco Systems, Inc
Figure 2-13	Courtesy of Cisco Systems, Inc
Figure 2-14	Courtesy of Cisco Systems, Inc
Figure 2-15	Courtesy of Cisco Systems, Inc
Figure 2-16	Screenshot of Configuring a vNIC © 2021, Oracle and/or its affiliates
Figure 2-17	Courtesy of Cisco Systems, Inc
Figure 2-18	Screenshot of Configuring a Virtual Switch © Microsoft 2021
Figure 2-19	Courtesy of Cisco Systems, Inc
Figure 2-20	Courtesy of Cisco Systems, Inc
Figure 2-21	Courtesy of Cisco Systems, Inc
Figure 2-22	Courtesy of Cisco Systems, Inc
Figure 2-23	Courtesy of Cisco Systems, Inc
Figure 4-4	Courtesy of Cisco Systems, Inc
Figure 4-5	Courtesy of Cisco Systems, Inc
Figure 4-6	Courtesy of Cisco Systems, Inc
Figure 4-7	Screenshot of Windows Control Panel © Microsoft 2021
Figure 4-8	Screenshot of Network and Internet Control Panel © Microsoft 2021
Figure 4-9	Screenshot of Network and Sharing Center © Microsoft 2021
Figure 4-10	Screenshot of Network Connections Window © Microsoft 2021
Figure 4-11	Screenshot of Local Area Connection Status Window © Microsoft 2021
Figure 4-12	Screenshot of Local Area Connection Properties © Microsoft 2021
Figure 4-13	Screenshot of Internet Protocol Version 4 (TCP/IPv4) Properties © Microsoft 2021

Figure 4-14	Screenshot of Advanced TCP/IP Settings: DNS Tab © Microsoft 2021
Figure 4-15	Screenshot of Advanced TCP/IP Settings: WINS Tab © Microsoft 2021
Figure 4-16; Figure 6-2	Screenshot of Configuring Microsoft Windows 10 to Obtain IP Address Information via DHCP © Microsoft 2021
Figure 4-17	Screenshot of APIPA Configuration Enabled by Default © Microsoft 2021
Figure 4-18	Courtesy of Cisco Systems, Inc
Figure 4-19	Screenshot of Free IP Address Manager © 2021 SolarWinds Worldwide, LLC
Figure 4-21	Courtesy of Cisco Systems, Inc
Figure 4-22	Courtesy of Cisco Systems, Inc
Figure 4-23	Courtesy of Cisco Systems, Inc
Figure 4-24	Courtesy of Cisco Systems, Inc
Figure 4-25	Courtesy of Cisco Systems, Inc
Figure 6-1	Courtesy of Cisco Systems, Inc
Figure 6-3	Courtesy of Cisco Systems, Inc
Figure 9-1	Courtesy of Cisco Systems, Inc
Figure 9-2	Courtesy of Cisco Systems, Inc
Figure 9-3	Courtesy of Cisco Systems, Inc
Figure 9-4	Courtesy of Cisco Systems, Inc
Figure 9-5	Courtesy of Cisco Systems, Inc
Figure 9-6	Courtesy of Cisco Systems, Inc
Figure 9-7	Courtesy of Cisco Systems, Inc
Figure 9-8	Courtesy of Cisco Systems, Inc
Figure 9-9	Courtesy of Cisco Systems, Inc
Figure 9-10	Courtesy of Cisco Systems, Inc
Figure 9-11	Courtesy of Cisco Systems, Inc
Figure 9-12	Courtesy of Cisco Systems, Inc
Figure 9-13	Courtesy of Cisco Systems, Inc
Figure 9-14	Courtesy of Cisco Systems, Inc
Figure 9-15	Courtesy of Cisco Systems, Inc
Figure 9-16	Courtesy of Cisco Systems, Inc
Figure 9-17	Norman Chan/Shutterstock
Figure 9-18	Courtesy of Cisco Systems, Inc
Figure 9-19	Courtesy of Cisco Systems, Inc
Figure 9-20	Courtesy of Cisco Systems, Inc
Figure 9-21	Courtesy of Cisco Systems, Inc
Figure 9-22	Courtesy of Cisco Systems, Inc
Figure 10-1	Courtesy of Cisco Systems, Inc
Figure 10-2	Courtesy of Cisco Systems, Inc

Figure 10-3	Courtesy of Cisco Systems, Inc
Figure 10-4	Courtesy of Cisco Systems, Inc
Figure 10-5	Courtesy of Cisco Systems, Inc
Figure 10-6	Courtesy of Cisco Systems, Inc
Figure 10-7	Courtesy of Cisco Systems, Inc
Figure 10-8	Courtesy of Cisco Systems, Inc
Figure 10-9	Courtesy of Cisco Systems, Inc
Figure 10-10	Courtesy of Cisco Systems, Inc
Figure 10-11	Courtesy of Cisco Systems, Inc
Figure 10-12	Courtesy of Cisco Systems, Inc
Figure 10-13	Courtesy of Cisco Systems, Inc
Figure 11-4	Courtesy of Cisco Systems, Inc
Figure 11-7	Courtesy of Cisco Systems, Inc
Figure 11-8	Courtesy of Cisco Systems, Inc
Figure 11-9	Courtesy of Cisco Systems, Inc
Figure 11-10	Courtesy of Cisco Systems, Inc
Figure 11-11	Courtesy of Cisco Systems, Inc
Figure 11-13	Courtesy of Cisco Systems, Inc
Figure 11-14	Courtesy of Cisco Systems, Inc
Figure 11-15	Courtesy of Cisco Systems, Inc
Figure 11-16	Courtesy of Cisco Systems, Inc
Figure 11-17	Courtesy of Cisco Systems, Inc
Figure 11-18	Courtesy of Cisco Systems, Inc
Figure 11-19	Courtesy of Cisco Systems, Inc
Figure 11-20	Courtesy of Cisco Systems, Inc
Figure 11-21	Screenshot of Example: Wireshark Packet-Capture Software © Wireshark Foundation
Figure 11-22	Courtesy of Cisco Systems, Inc
Figure 11-23	Courtesy of Cisco Systems, Inc
Figure 11-24	Courtesy of Cisco Systems, Inc
Figure 11-25	Courtesy of Cisco Systems, Inc
Figure 12-1	Courtesy of Cisco Systems, Inc
Figure 12-2	Courtesy of Cisco Systems, Inc
Figure 12-3	Courtesy of Cisco Systems, Inc
Figure 12-4	Courtesy of Cisco Systems, Inc
Figure 12-6	Courtesy of Cisco Systems, Inc
Figure 12-7	Courtesy of Cisco Systems, Inc
Figure 12-8	Courtesy of Cisco Systems, Inc
Figure 12-12	Courtesy of Cisco Systems, Inc
Figure 13-1	Courtesy of Cisco Systems, Inc
Figure 13-2	Courtesy of Cisco Systems, Inc
Figure 13-3	Courtesy of Cisco Systems, Inc

Figure 13-4	Screenshot of Structure of a Syslog Message © 2021 SolarWinds Worldwide, LLC
Figure 13-5	Screenshot of Application Log © Microsoft 2021
Figure 13-6	Screenshot of Security Log © Microsoft 2021
Figure 13-7	Screenshot of System Log © Microsoft 2021
Figure 15-1	Courtesy of Cisco Systems, Inc
Figure 15-2	Courtesy of Cisco Systems, Inc
Figure 15-3	Courtesy of Cisco Systems, Inc
Figure 15-4	Courtesy of Cisco Systems, Inc
Figure 15-5	Courtesy of Cisco Systems, Inc
Figure 15-6	Courtesy of Cisco Systems, Inc
Figure 15-8	Courtesy of Cisco Systems, Inc
Figure 16-1	Courtesy of Cisco Systems, Inc
Figure 16-2	Courtesy of Cisco Systems, Inc
Figure 17-1	Courtesy of Cisco Systems, Inc
Figure 19-1	Courtesy of Cisco Systems, Inc
Figure 19-2	Courtesy of Cisco Systems, Inc
Figure 19-4	Courtesy of Cisco Systems, Inc
Figure 23-1	Screenshot of Wireshark Protocol Analyzer Software © Wireshark Foundation
Figure 24-1	Courtesy of Cisco Systems, Inc
UNPHCov-1	leo_photo/Shutterstock
Cover Credit	TippaPatt/Shutterstock

Contents at a Glance

Table of Contents

About the Author

Anthony Sequeira (CCIE No. 15626) began his IT career in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion: teaching and writing about networking technologies. Anthony lectured to massive audiences around the world while working for Mastering Computers. Anthony has never been happier in his career than he is now, as a senior technical instructor for Splunk. He is an avid tennis player, a private pilot, and a semi-professional poker player, and he loves anything at all to do with technology.

Dedication

This book is dedicated to my wife, Joette Sequeira, who made this book, and all the rest of them, possible.

Acknowledgments

I cannot thank Brett Bartow and Chris Cleveland enough for their patience as I created this latest edition of the text.

About the Technical Reviewer

Chris Crayton (MCSE) is an author, technical consultant, and trainer. In the past, he has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several leading publishing companies. Chris holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.

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.

We welcome your comments. You can email or write to let us 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 we cannot help you with technical problems related to the topic of this book.

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

Email: community@informit.com

Introduction

The CompTIA Network+ certification is a popular certification for those entering the computer networking field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA Network+ certification is unique in that it is vendor neutral. The CompTIA Network+ certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by Cisco Systems.

On the CompTIA Network+ exam, the topics are mostly generic in that they can apply to networking equipment regardless of vendor. Although the CompTIA Network+ certification is vendor neutral, network software and systems are implemented by multiple independent vendors. Therefore, several of the exercises, examples, and simulations in this book include using particular vendors' configurations and technologies, such as Microsoft Windows operating systems or Cisco Systems routers and switches. More detailed training for a specific vendor's software and hardware can be found in books and training specific to that vendor.

Who Should Read This Book?

This book was written with two audiences in mind: those who want to learn all they can about networking technology and those who want to pass the CompTIA Network+ exam. I think that both groups are going to be very impressed with the breadth of technologies this book details. Although it would be impossible to cover every topic in networking today, this book manages to cover all the massive areas that make networking an exciting field that many people want to learn.

Readers will range from people who are attempting to attain a position in the IT field to people who want to keep their skills sharp or perhaps retain their job when facing a company policy that mandates they take the new exams. This book is also for those who want to acquire additional certifications beyond the Network+ certification (for example, the Cisco Certified Network Associate [CCNA] certification and beyond). The book is designed to enable an easy transition to future certification studies.

Resources

This book comes with a wealth of digital resources to help you review, practice, and assess your knowledge. The end of each chapter contains a review section that references several of these tools, and you should be sure to use them as you complete each chapter to help reinforce what you are learning. You can use them again after you finish the book to help review and make sure you are fully prepared for the exam.

Here's a list of resources available on the companion website:

- Interactive glossary flash card application
- Interactive exam essentials appendix
- Performance-based exercises
- CompTIA Network+ Hands-on Lab Simulator Lite Software for exam N10-008
- The Pearson Test Prep practice test software
- Video training on key exam topics
- Memory table review exercises and answer keys
- A study planner tool
- Instructions to redeem your Network+ certification exam voucher, which provides a 10% discount on the exam

To access the companion website, follow these steps:

Step 1. Go to **http://www.pearsonitcertification.com/register.**

Step 2. Either log in to your account if you have an existing account already or create a new account.

Step 3. Enter the ISBN of your book and click **Submit**.

Step 4. Answer the challenge questions to validate your purchase.

Step 5. In your account page, click the **Registered Products** tab and then click the **Access Bonus Content** link.

Pearson Test Prep Practice Test Software

The companion website that accompanies this book includes the Pearson Test Prep practice test engine, which is software that displays and grades a set of exam-realistic practice test questions. Using the Pearson Test Prep practice test engine, you can either study by going through the questions in study mode or take a simulated CompTIA Network+ exam that mimics real exam conditions. The software also has a flash card mode that allows you to challenge yourself to answer the questions without seeing the multiple-choice answers.

The Pearson Test Prep software is available both online and as a Windows desktop application that you can run offline. The online version can be accessed at www.pearsontestprep.com. This version can be used on any device that has an Internet connection, including desktop computers, laptop computers, tablets, and smartphones. It is optimized for viewing on screens as small as a standard iPhone screen. The desktop application can be downloaded and installed from the companion website.

NOTE The desktop Pearson Test Prep application is a Windows-based application, so it is only designed to run on Windows. Although it can be run on other operating systems using a Windows emulator, other operating systems are not officially supported for the desktop version. If you are using an OS other than Windows, you might want to consider using the online version of Pearson Test Prep instead.

Accessing the test engine is a two-step process. The first step is to either install the software on your desktop or access the online version website. However, the practice exam (that is, the database of CompTIA Network+ exam questions) is not available to you until you take the second step: Register the unique access code that accompanies your book.

NOTE The cardboard sleeve in the back of the physical book includes a piece of paper. The paper lists the *access code* for the practice exam associated with this book. Make sure you keep the access code even after you have registered your practice exam because you may need to refer to it later. Also, on the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the *CompTIA Network+ Cert Guide*, *Premium Edition eBook and Practice Test* product—a $40 value!

Installing the Pearson Test Prep Software

If you choose to use the Windows desktop version of the practice test software, you will need to download the installers from the companion website.

The software installation process is similar to other wizard-based installation processes. If you have already installed the Pearson Test Prep practice test software from another Pearson product, you do not need to reinstall the software. Just launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in sleeve in the back of the book. The following steps outline the installation process:

Step 1. Download the software to your computer from the companion website.

Step 2. Extract all files from the .zip file you downloaded.

Step 3. Launch the installer from the extracted files folder.

Step 4. Respond to the wizard-based prompts.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the back of book sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please register when prompted. If you already have a Pearson website login, you do not need to register again; just use your existing login.

Activating and Downloading the Practice Exam

The second step to accessing your practice exam product is to activate the product using the unique access code found in the back of book sleeve. You must follow this step regardless of which version of the product you are using—the online version or the Windows desktop version. The following steps walk you through how to activate your exam on each platform.

Windows Desktop Version:

1. Start the Pearson Test Prep Practice Test software from the Windows Start menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, on the My Products or Tools tab, click the **Activate** button.
3. At the next screen, enter the *access code* from the paper inside the cardboard sleeve in the back of the book and then click the **Activate** button. The activation process downloads the practice exam to your machine.
4. Click **Next** and then click **Finish**.

Online Version:

1. On a device with an active Internet connection, open your browser of choice and go to the website **www.pearsontestprep.com**.
2. Select **Pearson IT Certification** as the product group.
3. Enter the email address and password associated with your account and click **Login**.
4. In the middle of the screen, click the **Activate New Product** button.
5. Enter the access code from the paper inside the cardboard sleeve in the back of the book and click the **Activate** button.

After the activation process is complete, the My Products tab should list your new exam. If you do not see the exam, make sure that you selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Exams** button.

To update an exam that you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Updating your exams ensures that you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, simply select the **Tools** tab and click the **Update Application** button to ensure that you are running the latest version of the exam engine.

NOTE The online version always contains the latest updates to the exam questions, so there is never a need to update when you're using that version.

Activating Other Exams

The exam software installation process and the registration process both occur only once. Then, for each new exam, only a few steps are required. For example, if you buy another new Pearson IT Certification Cert Guide, you can extract the activation code from the sleeve in the back of that book, start the exam engine (if it's not still up and running), and perform the activation steps from the previous list.

Premium Edition

In addition to the free practice exam provided with the book, you can purchase additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional two full practice exams and an eBook (in PDF, EPUB, and Kindle formats). Also, the Premium Edition title provides remediation for each question that links to the specific part of the eBook that relates to that question.

If you purchased the print version of this title, you can purchase the Premium Edition at a deep discount. You'll find a coupon code in the back of book sleeve that contains a one-time-use code and instructions for where you can purchase the Premium Edition.

To view the Premium Edition product page, go to http://www.pearsonitcertification.com.

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the Network+ N10-008 blueprint from CompTIA. This book also helps you prepare for the N10-008 version of the CompTIA Network+ exam.

To aid you in mastering and understanding the Network+ certification objectives, this book uses the following methods:

- **Opening topics list:** This list spells out the Network+ objectives and topics that are covered in the chapter.
- **Foundation topics:** At the heart of a chapter, the sections under "Foundation Topics" explain the topics from hands-on and theory-based standpoints. These sections include in-depth descriptions, tables, and figures that build your knowledge so that you can pass the N10-008 exam. Each chapter is broken into multiple sections.
- **Key topics:** The "Review All Key Topics" section indicates important figures, tables, and lists of information that you need to review for the exam. Key Topic icons are sprinkled throughout each chapter, and a table at the end of each chapter lists the important parts of the text called out by these icons.
- **Memory tables:** You can find memory tables on the book's companion website in Appendixes C and D. Use them to help memorize important information.
- **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the definitions in the Glossary. On the companion website, you will find a flash card application with all the glossary terms separated by chapter, and you can use it to study key terms as well.
- **Exercises:** This book comes with 40 performance-based practice exercises that are designed to help you prepare for the hands-on portion of the Network+ exam. These exercises are available on the companion website. Make sure you do the exercises as you complete each chapter and again when you have completed the book and are doing your final preparation.
- **Hands-on labs:** These hands-on exercises, which are an important part of this book, include matching, drag and drop, and simulations. In addition to reading this book, you should go through all the exercises included with the book. These interactive hands-on exercises provide examples, additional information, and insight about a vendor's implementation of the technologies. To perform the labs, simply install the CompTIA Network+ N10-008 Hands-on Lab Simulator Lite software. This software is a Windows and Mac desktop application. You should be sure to install the software prior to reading the book because each chapter will indicate what labs you should perform. To install the software, follow these steps:

  Step 1. Go to the companion website for the book. (Refer to the "Resources" section for how to access the companion website.)

Step 2. Click the link to download the CompTIA Network+ N10-008 Hands-on Lab Simulator Lite software.

Step 3. Once you have downloaded the software to your computer, extract all the files from the .zip file.

Step 4. Launch the installer from the extracted files.

Step 5. Respond to the wizard-based prompts.

- **Practice exams:** This book comes complete with several full-length practice exams available to you in the Pearson Test Prep practice test software, which you can download and install from the companion website. The Pearson Test Prep software is also available to you online, at www.PearsonTestPrep.com. You can access both the online and desktop versions using the access code printed on the card in the sleeve in the back of this book. Be sure to run through the questions in Exam Bank 1 as you complete each chapter in study mode. When you have completed the book, take a full practice test using Exam Bank 2 questions in practice exam mode to test your exam readiness.
- **Exam essentials:** This book includes an exam essentials appendix that summaries the key points from every chapter. This review tool is available in print and as an interactive PDF on the companion website. Review these essential exam facts after each chapter and again when you have completed the book. This makes a great review summary that you can mark up as you review and master each concept.

For current information about the CompTIA Network+ certification exam, visit https://certification.comptia.org/certifications/network.

Strategies for Exam Preparation

This book comes with a study planner tool on the companion website. It is a spreadsheet that helps you keep track of the activities you need to perform in each chapter and helps you organize your exam preparation tasks. As you read the chapters in this book, jot down notes with key concepts or configurations in the study planner. Each chapter ends with a summary and series of exam preparation tasks to help you reinforce what you have learned. These tasks include review exercises such as reviewing key topics, completing memory tables, defining key terms, answering review questions, and performing hands-on labs and exercises. Make sure you perform these tasks as you complete each chapter to improve your retention of the material and record your progress in the study planner.

The book concludes with Chapter 26, "Final Preparation," which offers you guidance on your final exam preparation and provides you with some helpful exam advice. Make sure you read over that chapter to help assess your exam readiness and identify areas where you need to focus your review.

Make sure you complete all the performance-based question exercises and hands-on labs associated with this book. The exercises and labs are organized by chapter, making it easy to perform them after you complete each section. These exercises help you reinforce what you have learned, offer examples of some popular vendors' methods for implementing networking technologies, and provide additional information to assist you in building real-world skills and preparing you for the certification exam.

Download the current exam objectives by submitting a form on the following web page: https://www.comptia.org/certifications/network.

Use the practice exam, which is included on this book's companion website. As you work through the practice exam, use the practice test software reporting features to note the areas where you lack confidence and then review the related concepts. After you review those areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions become, and the less accurately the practice exam judges your skills.

After you work through the practice exam a second time and feel confident with your skills, schedule the real CompTIA Network+ exam (N10-008).

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (*objectives*) and specific topics under each general topic (*subobjectives*) for the CompTIA Network+ N10-008 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives and subobjectives are interrelated and are addressed in multiple chapters in the book.

Table I-1 CompTIA Network+ Exam Topics

Chapter	N10-008 Exam Objective	N10-008 Exam Subobjective
1 The OSI Model and Encapsulation	1.0 Networking Fundamentals	1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
2 Network Topologies and Types	1.0 Networking Fundamentals	1.2 Explain the characteristics of network topologies and network types.

Chapter	N10-008 Exam Objective	N10-008 Exam Subobjective
3 Network Media Types	1.0 Networking Fundamentals	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
4 IP Addressing	1.0 Networking Fundamentals	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
5 Common Ports and Protocols	1.0 Networking Fundamentals	1.5 Explain common ports and protocols, their application, and encrypted alternatives.
6 Network Services	1.0 Networking Fundamentals	1.6 Explain the use and purpose of network services.
7 Corporate and Datacenter Architectures	1.0 Networking Fundamentals	1.7 Explain basic corporate and datacenter network architecture.
8 Cloud Concepts	1.0 Networking Fundamentals	1.8 Summarize cloud concepts and connectivity options.
9 Various Network Devices	2.0 Network Implementations	2.1 Compare and contrast various devices, their features and their appropriate placement on the network.
10 Routing Technologies and Bandwidth Management	2.0 Network Implementations	2.2 Compare and contrast routing technologies and bandwidth management concepts.
11 Ethernet Switching	2.0 Network Implementations	2.3 Given a scenario, configure and deploy common Ethernet switching features.
12 Wireless Standards	2.0 Network Implementations	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.
13 Ensure Network Availability	3.0 Network Operations	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
14 Organizational Documents and Policies	3.0 Network Operations	3.2 Explain the purpose of organizational documents and policies.
15 High Availability and Disaster Recovery	3.0 Network Operations	3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

Chapter	N10-008 Exam Objective	N10-008 Exam Subobjective
16 Common Security Concepts	4.0 Network Security	4.1 Explain common security topics.
17 Common Types of Attacks	4.0 Network Security	4.2 Compare and contrast common types of attacks.
18 Network Hardening Techniques	4.0 Network Security	4.3 Given a scenario, apply network hardening techniques.
19 Remote Access Methods	4.0 Network Security	4.4 Compare and contrast remote access methods and security implications.
20 Physical Security	4.0 Network Security	4.5 Explain the importance of physical security.
21 A Network Troubleshooting Methodology	5.0 Network Troubleshooting	5.1 Explain the network troubleshooting methodology.
22 Troubleshoot Common Cabling Problems	5.0 Network Troubleshooting	5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.
23 Network Software Tools and Commands	5.0 Network Troubleshooting	5.3 Given a scenario, use the appropriate network software tools and commands.
24 Troubleshoot Common Wireless Issues	5.0 Network Troubleshooting	5.4 Given a scenario, troubleshoot common wireless connectivity issues.
25 Troubleshoot General Network Issues	5.0 Network Troubleshooting	5.5 Given a scenario, troubleshoot general networking issues.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. However, if you do intend to read all the chapters, the order in the book is an excellent sequence to use:

- **Chapter 1: The OSI Model and Encapsulation**—The OSI model is an extremely powerful guide you can use as you design, implement, and troubleshoot networks.
- **Chapter 2: Network Topologies and Types**—This chapter explores the many types of networks and topologies used in enterprises today.
- **Chapter 3: Network Media Types**—This chapter drills deep into the media that connects networks today.
- **Chapter 4: IP Addressing**—Addressing of systems is critical in networks, and this chapter covers the addressing used with IPv4 and IPv6.
- **Chapter 5: Common Ports and Protocols**—This chapter introduces many of the common ports and protocols in use today.
- **Chapter 6: Network Services**—The network is the plumbing that carries the data and services you require. This chapter examines some of the many services that you will encounter in networks today.
- **Chapter 7: Corporate and Datacenter Architectures—**Today's corporate enterprise networks and the datacenters that are common in networks today are the subject of this chapter.
- **Chapter 8: Cloud Concepts**—This chapter explores key principles of the cloud, which has become common in networks today.
- **Chapter 9: Various Network Devices**—This chapter explores some of the various devices found in networks today.
- **Chapter 10: Routing Technologies and Bandwidth Management**—Moving packets from one network to another is the job of a router. This chapter ensures that you are well versed in the many technologies that operate in this category.
- **Chapter 11: Ethernet Switching**—Wireless is great, but Ethernet still rules the access layer. This chapter explores Ethernet in depth.
- **Chapter 12: Wireless Standards**—Wireless networking is here to stay. This chapter provides you with details on important topics such as security and emerging technologies.

- **Chapter 13: Ensure Network Availability**—There are many tools available today to help you ensure that a network is running smoothly. This chapter details many of them.
- **Chapter 14: Organizational Documents and Policies**—This chapter discusses many of the documents and policies that are found in enterprises today. Those that could impact the IT department are the focus of this chapter.
- **Chapter 15: High Availability and Disaster Recovery**—Making sure the network is always available is the subject of this chapter.
- **Chapter 16: Common Security Concepts**—This chapter explores the fundamentals of network security.
- **Chapter 17: Common Types of Attacks**—This chapter covers the most common types of attacks in the cybersecurity landscape today.
- **Chapter 18: Network Hardening Techniques**—This chapter explores the methods of hardening the network and its devices against the most common attacks.
- **Chapter 19: Remote Access Methods**—This chapter explores the many types of remote access that are possible today.
- **Chapter 20: Physical Security**—This chapter explores the important topic of physical security for a network.
- **Chapter 21: A Network Troubleshooting Methodology**—Whereas other chapters just touch on network troubleshooting, this chapter makes it the focus.
- **Chapter 22: Troubleshoot Common Cabling Problems**—This chapter examines the most common issues with network media and what you can do to detect and resolve these issues.
- **Chapter 23: Network Software Tools and Commands**—This chapter explores many of the common tools and commands you can use to troubleshoot a network.
- **Chapter 24: Troubleshoot Common Wireless Issues**—This chapter explores the most common issues with wireless networks.
- **Chapter 25: Troubleshoot General Network Issues**—This chapter explores common general network issues and how you can quickly detect and resolve them.

CHAPTER 10

Routing Technologies and Bandwidth Management

In Chapter 4, "IP Addressing," you learned how Internet Protocol (IP) networks can be divided into subnets. Each subnet is its own broadcast domain, and the device that separates broadcast domains is a router (which this text considers synonymous with a multilayer switch). A multilayer switch is a network device that can perform the Layer 2 switching of frames as well as the Layer 3 routing of IP packets. Multilayer switches generally use dedicated chips to perform these functions and, as a result, may be faster than traditional routers in forwarding packets.

For traffic to flow between subnets, the traffic has to be routed; this routing is a router's primary job. This chapter discusses how routing occurs and introduces a variety of approaches for performing routing, including dynamic routing, static routing, and default routing. The chapter also breaks down the various categories of routing protocols and provides specific examples of each.

The chapter concludes with a discussion of various bandwidth management topics, including a discussion of QoS concepts, such as traffic shaping.

Foundation Topics

Routing

To understand basic routing processes, consider Figure 10-1. In this topology, PC1 needs to send traffic to Server1. Notice that these devices are on different networks. In this topology, how does a packet from the source IP address 192.168.1.2 get routed to the destination IP address 192.168.3.2?

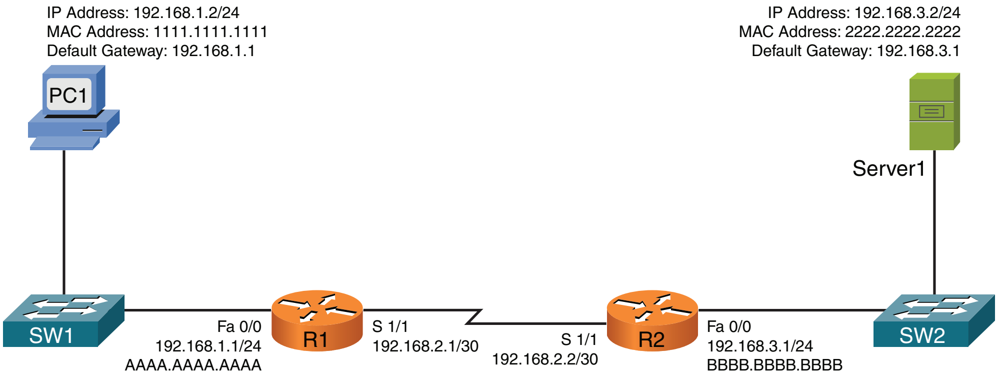


FIGURE 10-1 Basic Routing Topology

It might help to walk through this process systematically:

Key Topic

Step 1. PC1 compares its IP address and subnet mask 192.168.1.2/24 with the destination IP address and subnet mask 192.168.3.2/24. PC1 concludes that the destination IP address resides on a remote subnet. Therefore, PC1 needs to send the packet to its default gateway, which could have been manually configured on PC1 or dynamically learned via Dynamic Host Configuration Protocol (DHCP). In this example, PC1 has the default gateway 192.168.1.1 (router R1). However, to construct a Layer 2 frame, PC1 also needs the MAC address of its default gateway. PC1 sends an ***Address Resolution Protocol (ARP)*** request for router R1's MAC address. After PC1 receives an ARP reply from router R1, PC1 adds router R1's MAC address to its ARP cache. PC1 now sends its data in a frame destined for Server1, as shown in Figure 10-2.

NOTE ARP is a broadcast-based protocol and, therefore, does not travel beyond the local subnet of the sender.

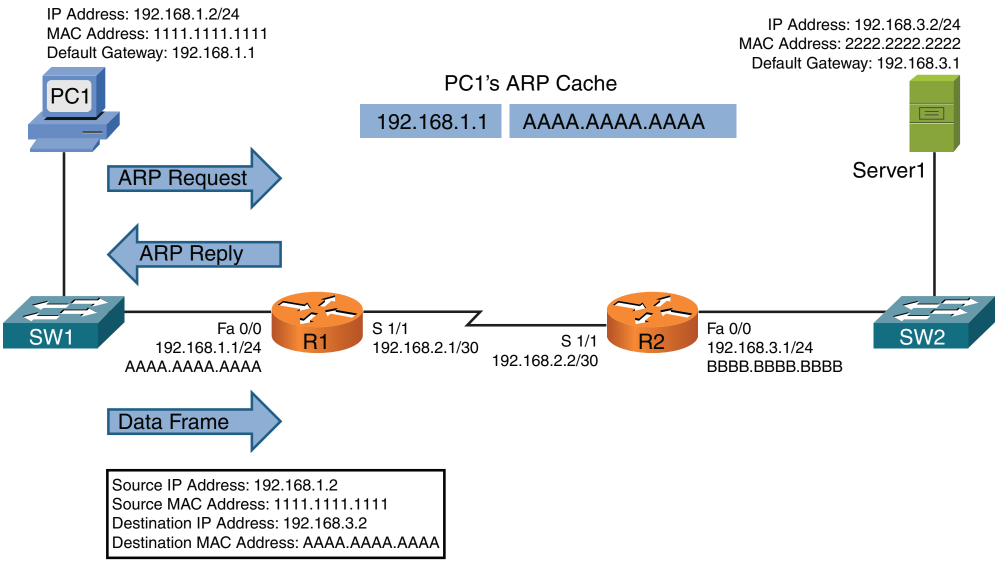


FIGURE 10-2 Basic Routing: Step 1

Step 2. Router R1 receives the frame sent from PC1 and interrogates the IP header. An IP header contains a ***Time-to-Live (TTL)*** field, which is decremented once for each router hop. Therefore, router R1 decrements the packet's TTL field. If the value in the TTL field is reduced to 0, the router discards the frame and sends a "time exceeded" Internet Control Message Protocol (ICMP) message back to the source. As long as the TTL has not been decremented to 0, router R1 checks its routing table to determine the best path to reach network 192.168.3.0/24. In this example, router R1's routing table has an entry stating that network 192.168.3.0/24 is accessible via interface Serial 1/1. Note that ARP is not required for serial interfaces because these interface types do not have MAC addresses. Router R1, therefore, forwards the frame out its Serial 1/1 interface, as shown in Figure 10-3.

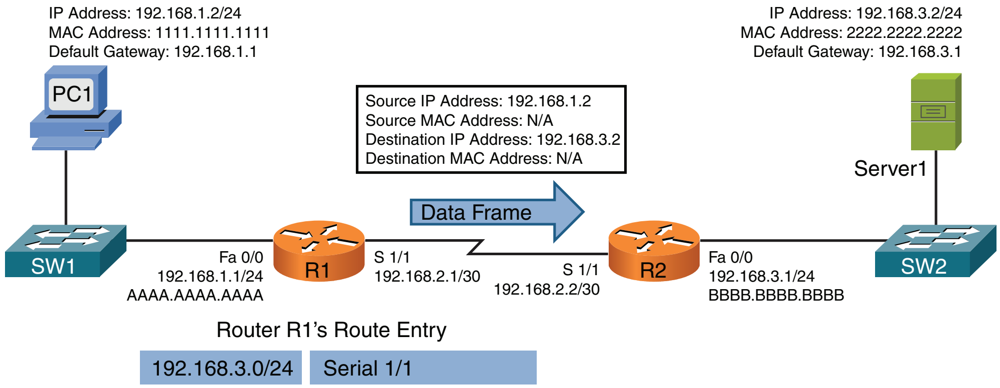


FIGURE 10-3 Basic Routing: Step 2

Step 3. When router R2 receives the frame, it decrements the TTL in the IP header, just as router R1 did. Again, as long as the TTL has not been decremented to 0, router R2 interrogates the IP header to determine the destination network. In this case, the destination network 192.168.3.0/24 is directly attached to router R2's Fast Ethernet 0/0 interface. Similar to the way PC1 sent out an ARP request to determine the MAC address of its default gateway, router R2 sends an ARP request to determine the MAC address of Server1. After an ARP reply is received from Server1, router R2 forwards the frame out its Fast Ethernet 0/0 interface to Server1, as illustrated in Figure 10-4.

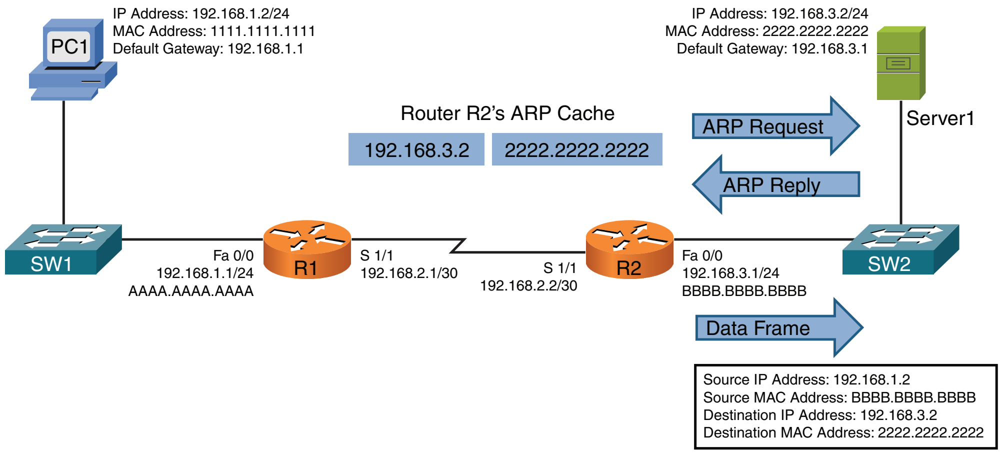


FIGURE 10-4 Basic Routing: Step 3

The previous steps identified two router data structures:

- **IP routing table:** When a router needed to route an IP packet, it consulted its IP routing table to find the best match. The best match is the route that has the longest prefix. Specifically, a route entry with the longest prefix is the most specific network. For example, imagine that a router has an entry for network 10.0.0.0/8 and for network 10.1.1.0/24. Also, imagine that the router is seeking the best match for destination address 10.1.1.1/24. The router would select the 10.1.1.0/24 route entry as the best entry because that route entry has the longest prefix (/24 is longer than /8, which is a more specific entry).
- **Layer 3 to Layer 2 mapping:** In the previous example, router R2's ARP cache contained Layer 3 to Layer 2 mapping information. Specifically, the ARP cache had a mapping that said MAC address 2222.2222.2222 corresponded to IP address 192.168.3.2.

As shown in the preceding example, routers rely on their internal routing table to make packet-forwarding decisions. So how does a router's routing table become populated with entries? That is the focus of the next section.

Sources of Routing Information

A router's routing table can be populated from various sources. As an administrator, you could statically configure a route entry. A route could be learned via a ***dynamic routing*** protocol (for example, OSPF or EIGRP), or a router could know how to get to a specific network because the router is physically attached to that network.

Directly Connected Routes

A router that has an interface directly participating in a network knows how to reach that specific destination network. For example, consider Figure 10-5.

In Figure 10-5, router R1's routing table knows how to reach the 192.168.1.0/24 and 192.168.2.0/30 networks because router R1 has an interface physically attached to each network. Similarly, router R2 has interfaces participating in the 10.1.1.0/30 and 192.168.2.0/30 networks and therefore knows how to reach those networks. The entries currently shown to be in the routing tables of routers R1 and R2 are called *directly connected routes*.

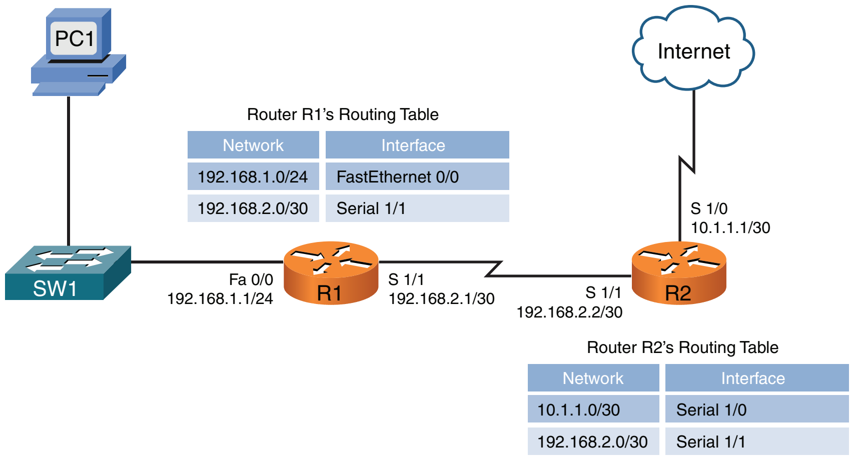


FIGURE 10-5 Directly Connected Routes

Static Routes

It is also possible to statically configure routes in a router's routing table. Continuing to expand on the previous example, consider router R1. As shown in Figure 10-6, router R1 does not need knowledge of each route on the Internet. Specifically, router R1 already knows how to reach devices on its locally attached networks. All router R1 really needs to know at this point is how to get out to the rest of the world. As you can see from Figure 10-6, any traffic destined for a nonlocal network (for example, any of the networks available on the public Internet) can simply be sent to router R2. Because R2 is the next router hop along the path to reach all those other networks, router R1 could be configured with a ***default static route***, which says, "If traffic is destined for a network not currently in the routing table, send that traffic out interface Serial 1/1."

NOTE A static route does not always reference a local interface. Instead, a static route might point to a ***next-hop IP address*** (that is, an interface's IP address on the next router to which traffic should be forwarded). The network address of a default route is 0.0.0.0/0.

Similarly, router R2 can reach the Internet by sending traffic out its Serial 1/0 interface. However, router R2 does need information about how to reach the 192.168.1.0/24 network available off router R1. To educate router R2 about how this network can be reached, a network administrator can add a static route pointing to 192.168.1.0/24 to router R2's routing table.

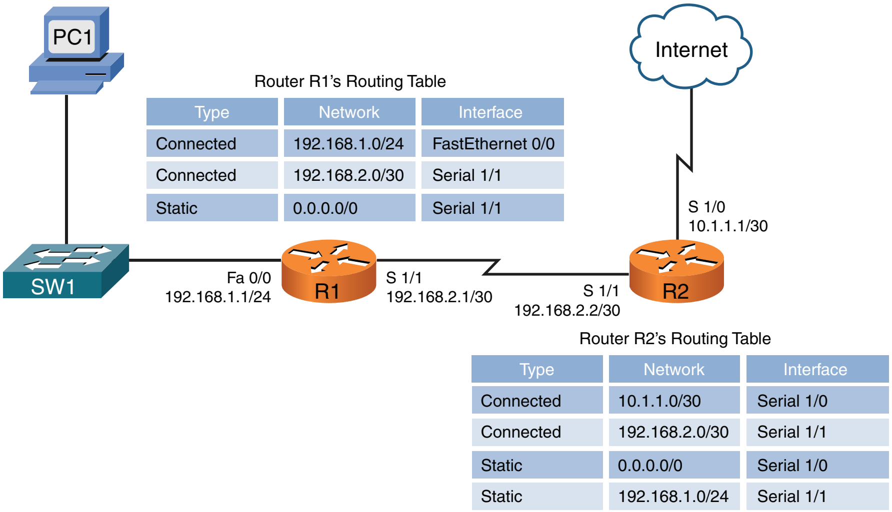


FIGURE 10-6 Static Routes

Dynamic Routing Protocols

In complex networks, such as the topology shown in Figure 10-7, static routing does not scale well. Fortunately, a variety of dynamic routing protocols are available that allow a router's routing table to be updated as network conditions change.

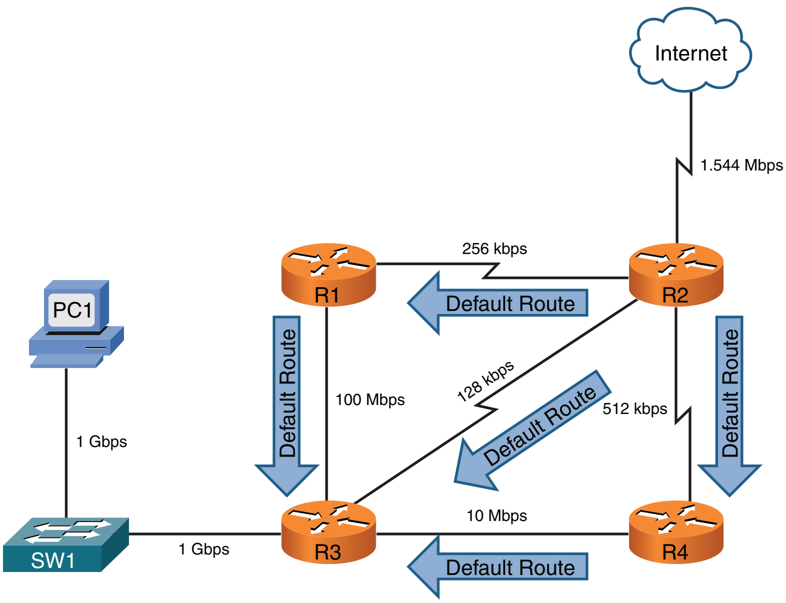


FIGURE 10-7 Dynamic Routes

In Figure 10-7, router R2 is advertising a default route to its neighbors (routers R1, R3, and R4). What happens if PC1 wants to send traffic to the Internet? PC1's default gateway is router R3, and router R3 has received three default routes. Which one does it use?

Router R3's path selection depends on the dynamic routing protocol being used. As you will see later in this chapter, a routing protocol such as Routing Information Protocol (RIP) would make the path selection based on the number of routers that must be used to reach the Internet (that is, *hop count*). Based on the topology presented, router R3 would select the 128Kbps link (where Kbps stands for kilobits per second, meaning thousands of bits per second) connecting to router R2 because the Internet would be only one hop away. If router R3 instead selected a path pointing to either router R1 or R4, the Internet would be two hops away.

However, based on the link bandwidths, you can see that the path from router R3 to router R2 is suboptimal. Unfortunately, RIP does not consider available bandwidth when making its route selection. Some other protocols, such as Open Shortest Path First (OSPF), can consider available bandwidth when making their routing decisions.

Dynamic routes also allow a router to reroute around a failed link. For example, in Figure 10-8, router R3 prefers to reach the Internet via router R4. However, the link between routers R3 and R4 goes down. Thanks to a dynamic routing protocol, router R3 knows of two other paths to reach the Internet, and it selects the next-best path, which is via router R1 in this example. This process of failing over from one route to a backup route is called *convergence*.

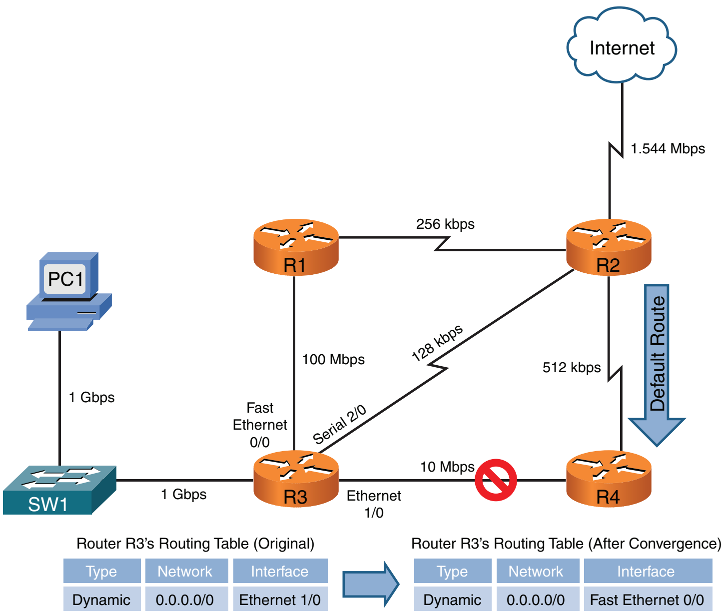


FIGURE 10-8 Route Redundancy

Routing Protocol Characteristics

Before examining the characteristics of routing protocols, we need to look at the important distinction between a *routing protocol* and a *routed protocol*:

- A ***routing protocol*** (for example, RIP, OSPF, or EIGRP) is a protocol that advertises route information between routers.
- A ***routed protocol*** is a protocol with an addressing scheme (for example, IP) that defines different network addresses. Traffic can then be routed between defined networks, perhaps with the assistance of a routing protocol.

This section looks at routing protocol characteristics, such as how believable a routing protocol is compared to other routing protocols. In addition, in the presence of multiple routes, different routing protocols use different ***metrics*** to determine the best path. A distinction is made between ***interior gateway protocols (IGPs)*** and ***exterior gateway protocols (EGPs)***. Finally, this section discusses different approaches to making route advertisements.

Believability of a Route

If a network is running more than one routing protocol (maybe as a result of a corporate merger), and a router receives two route advertisements from different routing protocols for the same network, which route advertisement does the router believe? Interestingly, some routing protocols are considered to be more believable that others. For example, a Cisco router would consider EIGRP to be more believable than RIP.

The index of believability is called ***administrative distance (AD)***. Table 10-1 shows the AD values for various sources of routing information. Note that lower AD values are more believable than higher AD values.

Key Topic

Table 10-1 Administrative Distance

Routing Information Source	AD Value
Directly connected network	0
Statically configured network	1
EIGRP	90
OSPF	110
RIP	120
External EIGRP	170
Unknown or unbelievable	255 (considered to be unreachable)

Metrics

Some networks might be reachable via more than one path. If a routing protocol knows of multiple paths to reach such a network, which route (or routes) does the routing protocol select? Actually, it varies depending on the routing protocol and what that routing protocol uses as a *metric* (that is, a value assigned to a route). Lower metrics are preferred over higher metrics.

Some routing protocols support load balancing across equal-cost paths; this is useful when a routing protocol knows of more than one route to reach a destination network and those routes have equal metrics. EIGRP can even be configured to do load balancing across unequal-cost paths.

Different routing protocols can use different parameters in their calculation of a metric. The specific parameters used for a variety of routing protocols are presented later in this chapter.

Interior Versus Exterior Gateway Protocols

Routing protocols can also be categorized based on the scope of their operation. Interior gateway protocols (IGPs) operate within an autonomous system, where an autonomous system is a network under a single administrative control. Conversely, exterior gateway protocols (EGPs) operate between autonomous systems.

Consider Figure 10-9. Routers R1 and R2 are in one autonomous system (AS 65002), and routers R3 and R4 are in another autonomous system (AS 65003). Within those autonomous systems, an IGP is used to exchange routing information. However, router ISP1 is a router in a separate autonomous system (AS 65001) that is run by a service provider. An EGP (typically, Border Gateway Protocol) is used to exchange routing information between the service provider's autonomous system and each of the other autonomous systems.

Route Advertisement Method

Another characteristic of a routing protocol is how it receives, advertises, and stores routing information. The two fundamental approaches are *distance vector* and *link state*.

Key Topic

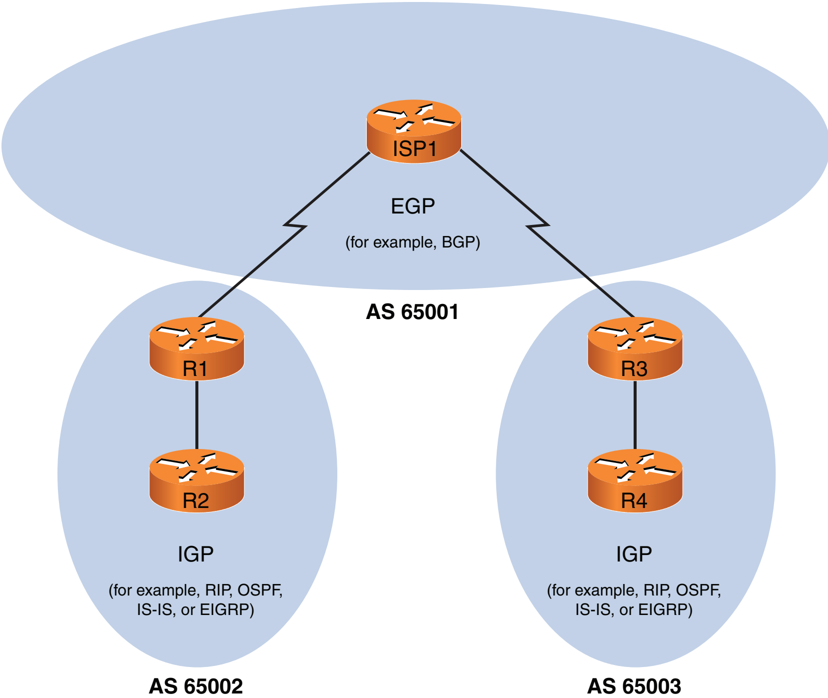


FIGURE 10-9 IGPs Versus EGPs

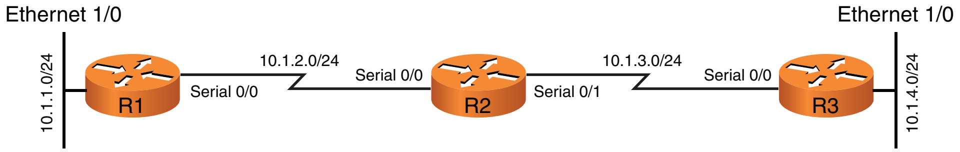
Distance Vector

A ***distance-vector routing protocol*** sends a full copy of its routing table to its directly attached neighbors. This is a periodic advertisement, meaning that even if there have been no topological changes, a distance-vector routing protocol will, at regular intervals, advertise again its full routing table to its neighbors.

Obviously, this periodic advertisement of redundant information is inefficient. Ideally, you want a full exchange of route information to occur only once and subsequent updates to be triggered by topological changes.

Another drawback to distance-vector routing protocols is the time they take to converge, which is the time required for all routers to update their routing tables in response to a topological change in a network. ***Hold-down timers*** can speed the convergence process. After a router makes a change to a route entry, a hold-down timer prevents any subsequent updates for a specified period of time. This approach helps stop flapping routes (which are routes that oscillate between being available and unavailable) from preventing convergence.

Yet another issue with distance-vector routing protocols is the potential of a routing loop. To illustrate, consider Figure 10-10. In this topology, the metric being used is *hop count*, which is the number of routers that must be crossed to reach a network. As one example, router R3's routing table has a route entry for network 10.1.1.0/24 available off router R1. For router R3 to reach that network, two routers must be transited (routers R2 and R1). As a result, network 10.1.1.0/24 appears in router R3's routing table with a metric (hop count) of 2.



Router R2's Routing Table

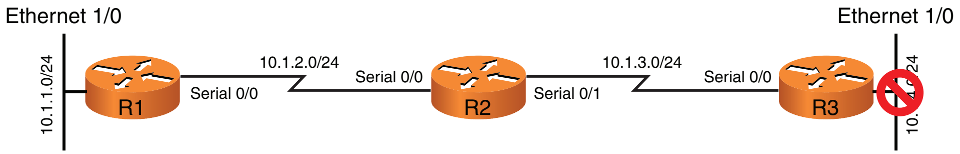
Network	Interface	Metric
10.1.1.0/24	S 0/0	1
10.1.2.0/24	S 0/0	0
10.1.3.0/24	S 0/1	0
10.1.4.0/24	S 0/1	1

Router R3's Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	2
10.1.2.0/24	S 0/0	1
10.1.3.0/24	S 0/0	0
10.1.4.0/24	E 1/0	0

FIGURE 10-10 Routing Loop: Before Link Failure

Continuing with the example, imagine that interface Ethernet 1/0 on router R3 goes down. As shown in Figure 10-11, router R3 loses its directly connected route (with a metric of 0) to network 10.1.4.0/24. However, router R2 had a route to 10.1.4.0/24 in its routing table (with a metric of 1), and this route was advertised to router R3. Router R3 adds this entry for 10.1.4.0 to its routing table and increments the metric by 1.



Router R2's Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	1
10.1.2.0/24	S 0/0	0
10.1.3.0/24	S 0/1	0
10.1.4.0/24	S 0/1	1

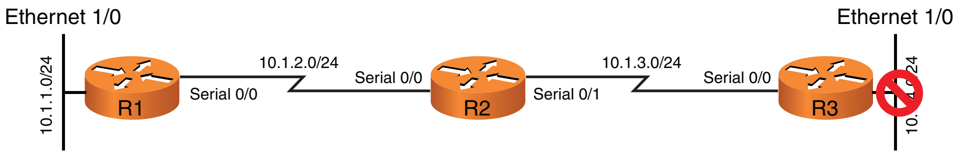
10.1.4.0/24
Hop Count 1

Router R3's Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	2
10.1.2.0/24	S 0/0	1
10.1.3.0/24	S 0/0	0
~~10.1.4.0/24~~	~~E 1/0~~	~~0~~
10.1.4.0/24	S 0/0	2

FIGURE 10-11 Routing Loop: After Link Failure

The problem with this scenario is that the 10.1.4.0/24 entry in router R2's routing table was due to an advertisement router R2 received from router R3. Now, router R3 is relying on that route, which is no longer valid. The routing loop continues as router R3 advertises its newly learned route 10.1.4.0/24 with a metric of 2 to its neighbor, router R2. Because router R2 originally learned the 10.1.4.0/24 network from router R3, when it sees router R2 advertising that same route with a metric of 2, the network gets updated in router R2's routing table to have a metric of 3, as shown in Figure 10-12.



Router R2's Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	1
10.1.2.0/24	S 0/0	0
10.1.3.0/24	S 0/1	0
~~10.1.4.0/24~~	~~S 0/1~~	~~1~~
10.1.4.0/24	S 0/1	3

10.1.4.0/24
Hop Count 2

Router R3's Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	2
10.1.2.0/24	S 0/0	1
10.1.3.0/24	S 0/0	0
~~10.1.4.0/24~~	~~E 1/0~~	~~0~~
10.1.4.0/24	S 0/0	2

FIGURE 10-12 Routing Loop: Routers R2 and R3 Incrementing the Metric for 10.1.4.0/24

The metric for the 10.1.4.0/24 network continues to increment in the routing tables for both routers R2 and R3 until the metric reaches a value considered to be an unreachable value (for example, 16 in the case of RIP). This process is referred to as a *routing loop*.

Key Topic

Distance-vector routing protocols typically use one of two approaches for preventing routing loops:

- ***Split horizon***: The split-horizon feature prevents a route learned on one interface from being advertised back out that same interface.
- ***Poison reverse***: The poison-reverse feature causes a route received on one interface to be advertised back out that same interface with a metric that is considered to be infinite.

In the previous example, either approach would have prevented router R3 from adding the 10.1.4.0/24 network to its routing table based on an advertisement from router R2.

Link State

Rather than having neighboring routers exchange their full routing tables with one another, a *link-state* routing protocol allows routers to build a topological map of the network. Then, much like a Global Positioning System (GPS) device in a car, a router can execute an algorithm to calculate an optimal path (or paths) to a destination network.

Routers send ***link-state advertisements (LSAs)*** to advertise the networks they know how to reach. Routers then use those LSAs to construct the topological map of a network. The algorithm that runs against this topological map is *Dijkstra's shortest path first* algorithm.

Unlike distance-vector routing protocols, ***link-state routing protocols*** exchange full routing information only when two routers initially form their adjacency. Then routing updates are sent in response to changes in the network, as opposed to being sent periodically. Also, link-state routing protocols benefit from shorter convergence times compared to distance-vector routing protocols.

Routing Protocol Examples

Key Topic

Now that you understand some of the characteristics that distinguish one routing protocol from another, this section contrasts some of the most popular routing protocols used in modern networks:

- ***Routing Information Protocol (RIP)*:** RIP is a distance-vector routing protocol that uses the metric *hop count*. The maximum number of hops between two routers in an RIP-based network is 15. Therefore, a hop count of 16 is considered to be infinite. Also, RIP is an IGP.
- ***Open Shortest Path First (OSPF)*:** OSPF is a link-state routing protocol that uses the metric *cost*, which is based on the link speed between two routers. OSPF is a popular IGP because of its scalability, fast convergence, and vendor interoperability.
- **Intermediate System-to-Intermediate System (IS-IS):** This link-state routing protocol is similar in operation to OSPF. It uses a configurable, yet dimensionless, metric associated with an interface and runs Dijkstra's shortest path first algorithm. Although IS-IS is an IGP that offers the scalability, fast convergence, and vendor-interoperability benefits of OSPF, it has not been as widely deployed as OSPF.

- ***Enhanced Interior Gateway Routing Protocol (EIGRP)*:** EIGRP is a Cisco-proprietary protocol that is popular in Cisco-only networks but less popular in mixed-vendor environments. Like OSPF, EIGRP is an IGP that offers fast convergence and scalability. EIGRP is more challenging to classify as a distance-vector or a link-state routing protocol.

By default, EIGRP uses bandwidth and delay in its metric calculation; however, other parameters can be considered, including reliability, load, and maximum transmission unit (MTU) size. Using delay as part of the metric, EIGRP can take into consideration the latency caused by the slowest links in the path.

Some literature calls EIGRP an *advanced distance-vector* routing protocol, and some literature calls it a ***hybrid routing protocol*** (mixing characteristics of both distance-vector and link-state routing protocols). EIGRP uses information from its neighbors to help select an optimal route (like distance-vector routing protocols). However, EIGRP also maintains a database of topological information (like a link-state routing protocol). The algorithm EIGRP uses for its route selection is not Dijkstra's shortest path first algorithm. Instead, EIGRP uses Diffusing Update Algorithm (DUAL).

- ***Border Gateway Protocol (BGP)*:** BGP is the only EGP in widespread use today. In fact, BGP is considered to be the routing protocol that runs the Internet, which is an interconnection of multiple autonomous systems. Although some literature classifies BGP as a distance-vector routing protocol, it can more accurately be described as a *path-vector* routing protocol, meaning that it can use as its metric the number of autonomous system hops that must be transited to reach a destination network, as opposed to a number of required router hops. BGP's path selection is not solely based on autonomous system hops, however. BGP can consider a variety of other parameters. Interestingly, none of those parameters are based on link speed. In addition, although BGP is incredibly scalable, it does not quickly converge in the event of a topological change.

NOTE When studying for the Network+ exam, be sure to focus on RIP, OSPF, EIGRP, and BGP as these are the dynamic routing protocols that the exam is sure to cover.

Table 10-2 compares the key characteristics of dynamic routing protocols.

Table 10-2 Comparing Dynamic Routing Protocols

Routing Protocol	IGP or EGP	Type	Metric
RIP	IGP	Distance vector	Hop count
OSPF	IGP	Link state	Cost (based on bandwidth)
EIGRP	IGP	Hybrid	Composite (bandwidth and delay by default)
BGP	EGP	Path vector	Path attributes

A network can simultaneously support more than one routing protocol through the process of ***route redistribution***. For example, a router could have one of its interfaces participating in an OSPF area of the network and have another interface participating in an EIGRP area of the network. This router could then take routes learned via OSPF and inject those routes into the EIGRP routing process. Similarly, EIGRP-learned routes could be redistributed into the OSPF routing process.

Bandwidth Management

While the main concern with routing is ensuring that data packets (as well as control plane packets) reach their rightful destinations, it is the job of ***quality of service*** (QoS) to ensure that packets do not suffer from long delays (latency) or, worse, dropped packets.

QoS is actually a suite of technologies that allows you to strategically optimize network performance for select traffic types. For example, in today's converged networks (that is, networks simultaneously transporting voice, video, and data), some applications (for example, voice) might be more intolerant of delay (or *latency*) than other applications; for example, an FTP file transfer is less latency sensitive than a VoIP call. Fortunately, through the use of QoS technologies, you can identify which traffic types need to be sent first, how much bandwidth to allocate to various traffic types, which traffic types should be dropped first in the event of congestion, and how to make the most efficient use of the relatively limited bandwidth of an IP WAN. This section introduces QoS and a collection of QoS mechanisms.

NOTE Do not get confused by the many uses we have for the word converged in networking. It all depends on the context. For example, when speaking about the network in general and what data it can carry, a converged network is one that includes multiple forms of traffic—for example VoIP and data traffic. When we are speaking of a single routing protocol—converged means the device has learned of all the updates that have been in the routing protocol's information.

Introduction to QoS

A lack of bandwidth is the overshadowing issue for most network quality problems. Specifically, when there is a lack of bandwidth, packets might suffer from one or more of the symptoms listed in Table 10-3.

Key Topic

Table 10-3 Three Categories of Quality Issues

Issue	Description
Delay	Delay is the time required for a packet to travel from source to destination. You might have witnessed delay on the evening news when the news anchor is talking via satellite to a foreign news correspondent. Because of the satellite delay, the conversation begins to feel unnatural.
Jitter	Jitter is the uneven arrival of packets. For example, imagine a VoIP conversation where packet 1 arrives at a destination router. Then, 20 ms later, packet 2 arrives. After another 70 ms, packet 3 arrives, and then packet 4 arrives 20 ms behind packet 3. This variation in arrival times (that is, *variable delay*) is not due to dropped packets, but the jitter might be interpreted by the listener as dropped packets.
Drops	Packet drops occur when a link is congested and a router's interface queue overflows. Some types of traffic, such as UDP traffic carrying voice packets, are not retransmitted if packets are dropped.

Fortunately, QoS features available on many routers and switches can recognize important traffic and then treat that traffic in a special way. For example, you might want to allocate 128Kbps of bandwidth for your VoIP traffic and give that traffic priority treatment.

Consider water flowing through a series of pipes with varying diameters. The water's flow rate through those pipes is limited to the water's flow rate through the pipe with the smallest diameter. Similarly, as a packet travels from source to destination, its effective bandwidth is the bandwidth of the slowest link along that path. For example, in Figure 10-13, notice that the slowest link speed is 256Kbps. This weakest link becomes the effective bandwidth between client and server.

Because the primary challenge of QoS is a lack of bandwidth, the logical question is, "How do we increase available bandwidth?" A knee-jerk response to that question is often "Add more bandwidth." However, more bandwidth often comes at a relatively high cost.

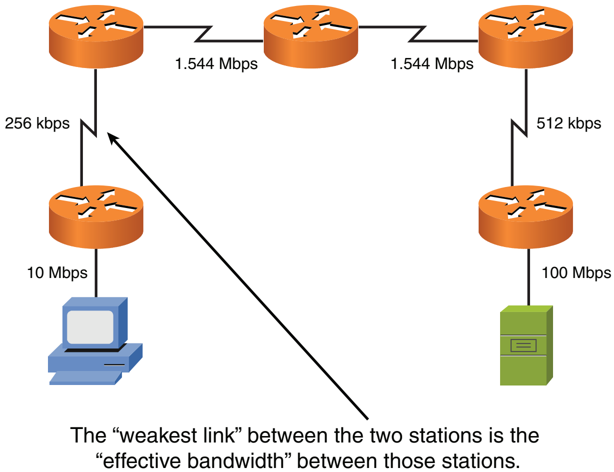


FIGURE 10-13 Effective Bandwidth of 256Kbps

Think of your network as a highway system in a large city. During rush hour, the lanes of the highway are congested; during other periods of the day, the lanes might be underutilized. Instead of just building more lanes to accommodate peak traffic rates, the highway engineers might add a carpool lane to give higher priority to cars with two or more occupants. Similarly, you can use QoS features to give your mission-critical applications higher-priority treatment in times of network congestion.

QoS Configuration Steps

The mission statement of QoS could read something like this: "To categorize traffic and apply a policy to those traffic categories, in accordance with a QoS policy." Understanding this underlying purpose of QoS can help you better understand the three basic steps involved in QoS configuration:

Key Topic

Step 1. Determine network performance requirements for various traffic types. For example, consider these design recommendations for voice, video, and data traffic:

- **Voice:** No more than 150 ms of one-way delay; no more than 30 ms of jitter; and no more than 1% packet loss.
- **Video:** No more than 150 ms of one-way delay for interactive voice applications (for example, video conferencing); no more than 30 ms of jitter; and no more than 1% of packet loss.
- **Data:** Applications have varying delay and loss requirements. Therefore, data applications should be categorized into predefined *classes*

of traffic, where each class is configured with specific delay and loss characteristics.

Step 2. Categorize traffic into specific categories. For example, you might have a category named *Low Delay* for voice and video packets in that category. You might also have a *Low Priority* class for traffic such as music downloads from the Internet.

Step 3. Document your QoS policy and make it available to your users. Then, for example, if users complain that their network gaming applications are running slowly, you can point them to your corporate QoS policy, which describes how applications such as network gaming have *best-effort* treatment, while VoIP traffic receives *priority* treatment.

The actual implementation of these steps varies based on the specific device you are configuring. In some cases, you might be using the command-line interface (CLI) of a router or switch. In other cases, you might have some sort of graphical user interface (GUI) through which you configure QoS on your routers and switches.

QoS Components

QoS features are categorized into one of the three categories shown in Table 10-4.

Key Topic

Table 10-4 Three Categories of QoS Mechanisms

Issue	Description
Best effort	Best-effort treatment of traffic does not truly provide QoS to that traffic because there is no reordering of packets. Best effort uses a first-in, first-out (FIFO) queuing strategy, where packets are emptied from a queue in the same order in which they entered the queue.
Integrated Services (IntServ)	IntServ is often referred to as *hard QoS* because it can make strict bandwidth reservations. IntServ uses signaling among network devices to provide bandwidth reservations. Resource Reservation Protocol (RSVP) is an example of an IntServ approach to QoS. Because IntServ must be configured on every router along a packet's path, the main drawback of IntServ is its lack of scalability.
Differentiated Services (DiffServ)	DiffServ, as its name suggests, differentiates between multiple traffic flows. Specifically, packets are marked, and routers and switches can then make decisions (for example, dropping or forwarding decisions) based on those markings. Because DiffServ does not make an explicit reservation, it is often called *soft QoS*. Most modern QoS configurations are based on the DiffServ approach.

Figure 10-14 summarizes these three QoS categories.

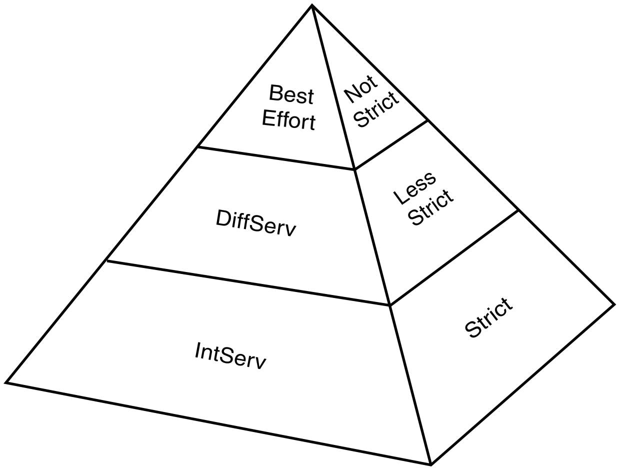


FIGURE 10-14 QoS Categories

QoS Mechanisms

As previously mentioned, a DiffServ approach to QoS marks traffic. However, for markings to impact the behavior of traffic, a QoS tool must reference those markings and alter the packets' treatment based on them. The following is a collection of commonly used QoS mechanisms:

- Classification
- Marking
- Congestion management
- Congestion avoidance
- Policing and shaping
- Link efficiency

While all of these mechanisms can be considered important, this chapter focuses on the main bandwidth management tools policing and traffic shaping.

Policing and Traffic Shaping

Key Topic

Instead of making a minimum amount of bandwidth available for specific traffic types, you might want to limit available bandwidth. Both ***traffic policing*** and ***traffic shaping*** tools can accomplish this objective. Collectively, these tools are called *traffic conditioners*.

Policing can be used in either the inbound or the outbound direction, and it typically discards packets that exceed the configured rate limit, which you can think of as a *speed limit* for specific traffic types. Because policing drops packets, resulting in retransmissions, it is recommended for higher-speed interfaces.

Shaping buffers (and therefore delays) traffic exceeding a configured rate. Therefore, shaping is recommended for slower-speed interfaces.

Because traffic shaping (and policing) can limit the speed of packets exiting a router, a question arises: "How do you send traffic out of an interface at a rate that is less than the physical clock rate of the interface?" For this to be possible, shaping and policing tools do not transmit all the time. Specifically, they send a certain number of bits or bytes at line rate, and then they stop sending until a specific timing interval (for example, one-eighth of a second) is reached. After the timing interval is reached, the interface again sends a specific amount of traffic at the line rate. It stops and waits for the next timing interval to occur. This process continually repeats, allowing an interface to send an average bandwidth that might be below the physical speed of the interface. This average bandwidth is called the *committed information rate* (*CIR*). The number of bits (the unit of measure used with shaping tools) or bytes (the unit of measure used with policing tools) that is sent during a timing interval is called the *committed burst* (*Bc*). The timing interval is written as *Tc*.

For example, imagine that you have a physical line rate of 128Kbps, but the CIR is only 64Kbps. Also, assume that there are eight timing intervals in a second (that is, Tc = 1/8 second = 125 ms), and during each of those timing intervals, 8000 bits (the committed burst parameter) are sent at the line rate. Therefore, over the period of a second, 8000 bits are sent (at the line rate) eight times, for a grand total of 64,000 bits per second, which is the CIR. Figure 10-15 illustrates this shaping of traffic to 64Kbps on a line with a rate of 128Kbps.

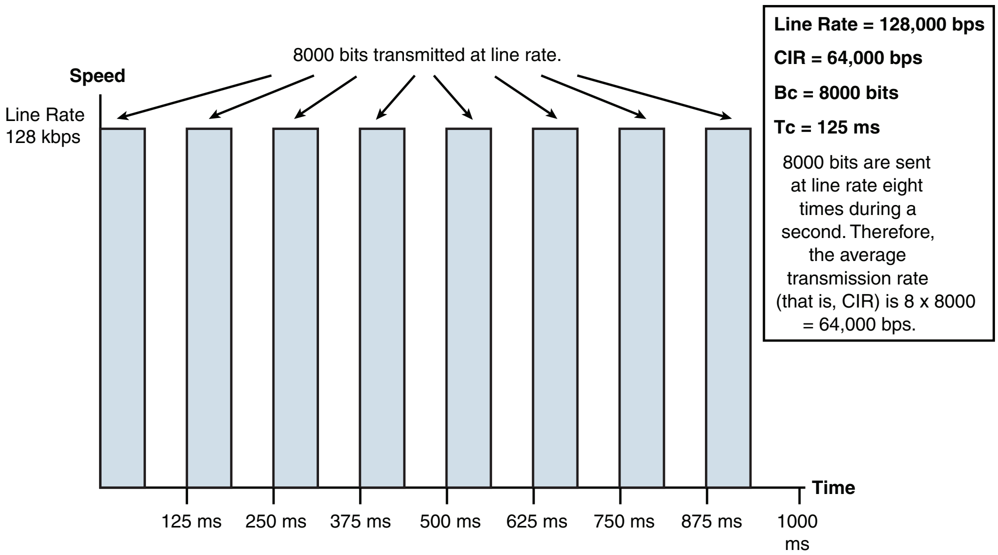


FIGURE 10-15 Traffic Shaping

If all the Bc bits (or bytes) are not sent during a timing interval, there is an option to *bank* those bits and use them during a future timing interval. The parameter that allows this storing of unused potential bandwidth is called the *excess burst* (*Be*) parameter. The Be parameter in a shaping configuration specifies the maximum number of bits or bytes that can be sent in excess of the Bc during a timing interval, if those bits are indeed available. For those bits or bytes to be available, they must have gone unused during previous timing intervals. Policing tools, however, use the Be parameter to specify the maximum number of bytes that can be sent during a timing interval. Therefore, in a policing configuration, if the Bc equals the Be, no excess bursting occurs. If excess bursting occurs, policing tools consider this excess traffic to be *exceeding traffic*. Policing tools consider traffic that conforms to (that is, does not exceed) a specified CIR to be *conforming traffic*.

The relationship between the Tc, Bc, and CIR is given with this formula: *CIR = Bc / Tc*. Alternatively, the formula can be written as *Tc = Bc / CIR*. Therefore, if you want a smaller timing interval, you can configure a smaller Bc.

Real-World Case Study

Acme, Inc. has decided to use a link-state routing protocol for dynamic routing between its LANs and the remote offices, which are connected over the WANs. The link-state protocol the company has chosen is OSPF. Each of the routers that has connections to the LAN and WAN subnets will learn about and advertise OSPF routes with its OSPF neighbors.

The branch offices will have a default route that points toward the headquarters' routers, and at the headquarters' site, they will use a default route that points toward the service provider. Acme, Inc. itself will not be using BGP, but its WAN and Internet service provider, which is interacting with other service providers, will use BGP.

The WAN connection to one of the remote offices is very low bandwidth and is prone to becoming congested with traffic. It also occasionally drops all connection to the remote office's router. Acme, Inc., has decided to use traffic shaping as part of the QoS configuration to attempt to ensure that the link is used more sparingly and is not overwhelmed with traffic during key business hours.

Summary

Here are the main topics covered in this chapter:

- This chapter discusses how routers forward traffic through a network based on source and destination IP addresses.
- This chapter also covers the sources of route information used to populate a router's routing table. These sources include directly connected routes, statically configured routes, and dynamically learned routes.
- This chapter distinguishes between routed protocols (for example, IP) and routing protocols (such as OSPF or EIGRP).
- Some routing sources are more trustworthy than other routing sources, based on their administrative distances.
- Different routing protocols use different metrics to select the best route in the presence of multiple routes.
- This chapter distinguishes between IGPs (which run within an autonomous system) and EGPs (which run between autonomous systems).
- This chapter contrasts the behavior of distance-vector and link-state routing protocols and shows how split horizon and poison reverse can prevent routing loops in a distance-vector routing protocol environment.
- This chapter describes today's most popular routing protocols (including RIP, OSPF, IS-IS, EIGRP, and BGP), along with their characteristics.
- This chapter reviews various QoS technologies, with an emphasis on traffic shaping, which can limit the rate of data transmission on a WAN link to the CIR.

Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, noted with the Key Topic icon in the outer margin of the page. Table 10-5 lists these key topics and the page number where each is found.

Key Topic

Table 10-5 Key Topics for Chapter 10

Key Topic Element	Description	Page Number
Step list	Basic routing process	256
Table 10-1	Administrative distance	263
Figure 10-9	IGPs versus EGPs	265
List	Preventing routing loops	267
List	Routing protocol examples	268
Step list	QoS configuration	272
Table 10-4	Three categories of QoS mechanisms	273
Section	Limiting available bandwidth through traffic policing and traffic-shaping tools	275

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables," or at least the section for this chapter and complete as many of the tables as possible from memory. Appendix D, "Memory Tables Answer Key," includes the completed tables and lists so you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Address Resolution Protocol (ARP), Time-to-Live (TTL), default static route, next-hop IP address, routed protocol, routing protocol, administrative distance (AD), metric, interior gateway protocol (IGP), exterior gateway protocol (EGP), distance-vector routing protocol, link-state routing protocol, hold-down timer, split horizon, poison reverse, link-state advertisement (LSA), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior

Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), route redistribution, quality of service (QoS), traffic shaping, traffic policing, dynamic routing, hybrid routing protocol

Additional Resources

An OSPF Review: https://www.ajsnetworking.com/an-ospf-review/

EIGRP's Composite Metric: https://www.ajsnetworking.com/eigrp-metric

Review Questions

The answers to these review questions appear in Appendix A, "Answers to Review Questions."

1. If a PC on an Ethernet network attempts to communicate with a host on a different subnet, what destination IP address and destination MAC address will be placed in the packet/frame header sent by the PC?
    a. **Destination IP: IP address of the default gateway. Destination MAC: MAC address of the default gateway.**
    b. **Destination IP: IP address of the remote host. Destination MAC: MAC address of the default gateway.**
    c. **Destination IP: IP address of the remote host. Destination MAC: MAC address of the remote host.**

   d. **Destination IP: IP address of the remote host. Destination MAC: MAC address of the local PC.**

2. What protocol is used to request a MAC address that corresponds to a known IPv4 address on the local network?
   a. IGMP
   b. TTL
   c. ICMP
   d. ARP

3. What is the network address and subnet mask of a default route?
   a. 255.255.255.255/32
   b. 0.0.0.0/32
   c. 255.255.255.255/0
   d. 0.0.0.0/0

4. What routing protocol characteristic indicates the believability of the routing protocol (compared to other routing protocols)?
   a. Weight
   b. Metric
   c. Administrative distance
   d. SPF algorithm

5. Which of the following are distance-vector routing protocol features that can prevent routing loops? (Choose two.)
   a. Reverse path forwarding (RPF) check
   b. Split horizon
   c. Poison reverse
   d. Rendezvous point

6. Which of the following is a distance-vector routing protocol with a maximum usable hop count of 15?
   a. BGP
   b. EIGRP
   c. RIP
   d. OSPF

7. Which of the following routing protocols is an EGP?
   a. BGP
   b. EIGRP
   c. RIP
   d. OSPF

8. What is the term for unpredictable variation in delay in a modern network?
   a. Congestion
   b. Contention
   c. Jitter
   d. Serialization delay

9. The RSVP protocol is associated with which overall approach to QoS in a modern network?
   a. DiffServ
   b. IntServ
   c. FIFO
   d. Best effort

10. What QoS tool seeks to smooth out bandwidth utilization by buffering excess packets?
    a. Traffic policing
    b. Traffic shaping
    c. Weighted Random Early Detection (WRED)
    d. Integrated Services (IntServ)

Index

Numbers

A

B

C

E

F

G

H

I

J

K

L

M

N

O

P

S

U

V

W

X

Y - Z