EXAM PREP™

CCNA

David Minutella
Jeremy Cioara
Heather Stevenson

CCNA Exam Prep

International Standard Book Number: 0-7897-3519-9

Library of Congress Catalog Card Number: 20055933178

Printed in the United States of America

First Printing: December 2005

08 07 06 05 4 3 2 1

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Que Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

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 the U.S., please contact

International Sales
international@pearsoned.com

PUBLISHER
Paul Boger

EXECUTIVE EDITOR
Jeff Riley

ACQUISITIONS EDITOR
Carol Ackerman

DEVELOPMENT EDITOR
Michael Watson

MANAGING EDITOR
Charlotte Clapp

PROJECT EDITOR
Andrew Beaster

COPY EDITORS
Margo Catts
Rhonda Tinch-Mize

INDEXER
Aaron Black

PROOFREADER
Kathy Bidwell

TECHNICAL EDITORS
Chris Ward
David Camardella

PUBLISHING COORDINATOR
Cindy Teeters

MULTIMEDIA DEVELOPER
Dan Scherf

INTERIOR DESIGNER
Gary Adair

COVER DESIGNER
Anne Jones

PAGE LAYOUT
Michelle Mitchell

Contents at a Glance

Table of Contents

About the Authors

Dave Minutella (CCNP, CCDP, CCSP, INFOSEC, CISSP, MCSA, MCDST, Security+, Network +, A+) has been working in the IT and telecom industry for more than 12 years. He currently serves as Vice President of Educational Services for TechTrain/The Training Camp. Before that, he was the lead Cisco instructor, primarily teaching CCNA, CCDA, and CCNP courses. Dave is also the technical author of *CSVPN Exam Cram 2*, from Que Publishing, and is the present Cisco certifications expert for SearchNetworking.com's Ask The Networking Expert panel.

Jeremy D. Cioara (CCIE, MCSE, CNE) is the owner of AdTEC Networks and works as a network consultant, instructor, and author. He has been working in network technologies for more than a decade and has deployed networks worldwide. His current consulting work focuses on network and Voice over IP (VoIP) implementations. Jeremy has written many books on Cisco network technology, but has a true passion for educating individuals both in the classroom and through e-learning environments.

Heather Stevenson (CCNA) has been working in the IT industry for more than 5 years. She first started her networking career in a rapidly growing telecommunications company where part of her job responsibilities included writing network procedures and training guides. In addition to technical training and consulting, Heather has also worked as a network engineer supporting networks worldwide. In her personal time, Heather enjoys spending quality time with her friends and family. She loves visiting the beach in the summer and hitting the slopes in the winter.

About the Technical Editors

David Camardella holds a CCNP, CCDA, MCSE:Messaging/Security, MCDST, Security+, A+, Network+, and Linux+ certifications. He has worked with Cisco products for 6 years providing technical support and services such as; designing and maintaining Cisco Internetworks, Active Directory, Messaging Infrastructures, and desktop deployment systems. While perusing a Bachelor of Science in Business Management, David has performed technical editing on numerous books as well as co-authored an A+ certification textbook.

Chris Ward is a senior technical instructor for a Web-based ILT company and is a CCSI, CCNP, CCDP, and MCSE. He has worked for companies such as IntegrationWorks, Salem Communications, and his own company, NightFall Productions, over the past ten years. He has written for several publications as well as co-authored a book on Windows Server 2003 and *CCNA Practice Questions Exam Cram*.

Dedications

From Dave:

I would like to dedicate this book to my grandfather, Albert Zambino. I will never forget you.

To my wife, Marsha: I never imagined I could feel so vulnerable daring to love someone so much. Your unwavering patience, support, and assistance in writing my dedication made this book possible.

To my family and friends at home: Thank you for your encouragement and standing by me despite not having the slightest clue what I am writing about.

To my friends at work: Thank you for your encouragement and standing by me despite knowing exactly what I am writing about.

From Jeremy:

To my darling wife, Susan: Thank you for your support through all these projects that keep me glued to a computer screen through all hours of the day and night. You are a more wonderful companion than I could have ever hoped for. I love you!

From Heather:

I would like to dedicate this book to my village, my people.

To Dustin: Thank you for every little thing you do. You mean everything to me. My sanity also wants to thank you, by the way the forest walrus says "hello."

To my mommy and daddy: Thank you for being the absolute best parents in the world. I couldn't ask for a better support system than my family.

Finally, I must also thank Shilo and DYB Bear, without them this book would just not be possible.

Acknowledgments

From Dave:

I would like to thank everybody at Que Publishing, especially Carol Ackerman who willingly and voluntarily put up with me for another book. To my technical editors David Camardella and Chris Ward, thank you for your incredible input and insight. Your contributions were invaluable in the formation of this book. Thank you to Margo Catts for combing through the endless mistakes I made in these chapters to make my grammar and speling much gooder. Also thank you to Michael Watson for keeping our content focused and…oh look, a shiny object.

From Jeremy:

First and foremost, I'd like to thank Jesus Christ, who continues to bless me in every way and keeps me from killing myself by doing something stupid. You will always be at the core of everything I do. To Carol, the Que super-project-manager-extraordinaire, thank you for always sounding happy on the phone. To the cricket chirping in the room right now, I hate you. If I ever find you, I'm going to feed you to my fish and dance merrily around the room as they eat you slowly.

From Heather:

I would like to send out a big thank you to Carol Ackerman and the editorial staff at Que, you have all been a pleasure to work with. Also, the support I received from my co-authors has been immeasurable. To Dave Minutella, thank you for thinking of me. I'm sure there are a boat load of sea monkeys out there waiting to be loved.

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 executive editor for Que Publishing, 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@quepublishing.com

Mail: Jeff Riley
Executive Editor
Que Publishing
800 East 96th Street
Indianapolis, IN 46240 USA

For more information about this book or another Que Certification title, visit our website at www.examcram.com. Type the ISBN (excluding hyphens) or the title of a book in the Search field to find the page you're looking for.

Cisco INTRO/ICND/CCNA Exam Objectives

INTRO

Introduction to Cisco Networking Technologies Exam

Exam Number: 640-821

Associated Certifications: CCNA

Duration: 75 minutes (45–55 questions)

Exam Description

The Introduction to Cisco Networking Technologies (INTRO) exam is one of the two qualifying exams available to candidates pursuing a two-exam option for CCNA. This exam tests content covered in the INTRO course, including topics on Network Types, Network Media, Switching Fundamentals, TCP/IP, IP Addressing and Routing, WAN Technologies, Operating and Configuring IOS Devices, and Managing Network Environments. The exam will certify that the successful candidate has important knowledge and skills necessary to describe and identify major LAN and WAN components, along with their function and purpose.

Exam Topics

The following information provides general guidelines for the content likely to be included on the INTRO exam. However, other related topics might also appear on any specific delivery of the exam.

Design and Support

- Use a subset of Cisco IOS commands to analyze and report network problems
- Use embedded Layer 3 through Layer 7 protocols to establish, test, suspend, or disconnect connectivity to remote devices from the router console
- Determine IP addresses

Implementation and Operation

- Establish communication between a terminal device and the router IOS, and use IOS for system analysis
- Manipulate system image and device configuration files
- Perform an initial configuration on a router and save the resultant configuration file
- Use commands incorporated within IOS to analyze and report network problems
- Assign IP addresses
- Describe and install the hardware and software required to be able to communicate via a network
- Use embedded Data Link layer functionality to perform network neighbor discovery and analysis from the router
- Use embedded Layer 3 through Layer 7 protocols to establish, test, suspend, or disconnect connectivity to remote devices from the router console

Technology

- Demonstrate the mathematical skills required to work seamlessly with integer decimal, binary, and hexadecimal numbers and simple binary logic
- Define and describe the structure and technologies of computer networks
- Describe the hardware and software required to be able to communicate via a network
- Describe the physical, electrical, and mechanical properties and standards associated with optical, wireless, and copper media used in networks
- Describe the topologies and physical issues associated with cabling common LANs
- Identify the key characteristics of common Wide Area Networking (WAN) configurations and technologies, and differentiate between these and common LAN technologies
- Describe the purpose and fundamental operation of the internetwork operating system (IOS)
- Describe the role of a router in a WAN
- Identify the major internal and external components of a router, and describe the associated functionality
- Identify and describe the stages of the router bootup sequence
- Describe how the configuration register and boot system commands modify the router bootup sequence

- Describe the concepts associated with routing, as well as the different methods and protocols used to achieve it
- Describe how an IP address is associated with a device interface, as well as the association between physical and employ IP addressing techniques
- Employ IP addressing techniques
- Compare and contrast collision and broadcast domains, and describe the process of network segmentation
- Describe the principles and practice of switching in an ethernet network
- Explain how collisions are detected and handled in an ethernet system
- Explain the fundamental concepts associated with the ethernet media access technique
- Describe how the protocols associated with TCP/IP enable host communication to occur
- Describe the operation of the Internet Control Message Protocol (ICMP) and identify the reasons, types, and format of associated error and control messages
- Describe the principles and practice of packet switching using the Internet Protocol (IP)

ICND

Interconnecting Cisco Networking Devices Exam

Exam Number: 640-811
Associated Certifications: CCNA
Duration: 60 minutes (40–50 questions)

Exam Description

The Interconnecting Cisco Network Devices (ICND) exam is one of the two qualifying exams available to candidates pursuing a two-exam option for the CCNA certification. The ICND (640-811) exam will test materials from the new ICND course. The exam will certify that the successful candidate has important knowledge and skills necessary to select, connect, configure, and troubleshoot the various Cisco networking devices. The exam covers topics on Extending Switched Networks with VLANS, Determining IP Routes, Managing IP Traffic with Access Lists, Establishing Point-to-Point Connections, and Establishing Frame Relay Connections.

Exam Topics

The following information provides general guidelines for the content likely to be included on the ICND exam. However, other related topics might also appear on any specific delivery of the exam.

Planning and Designing

- Design or modify a simple LAN using Cisco products
- Design an IP addressing scheme to support classful, classless, and private addressing to meet design requirements
- Select an appropriate routing protocol based on user requirements
- Design a simple internetwork using Cisco products
- Develop an access list to meet user specifications
- Choose WAN protocols to meet design requirements

Implementation and Operations

- Perform an initial configuration on a switch
- Configure routing protocols given user requirements
- Configure IP addresses, subnet masks, and gateway addresses on routers and hosts
- Configure a router for additional administrative functionality
- Configure a switch with VLANS and interswitch communication
- Implement a LAN
- Customize a switch configuration to meet specified network requirements
- Implement access lists
- Implement simple WAN protocols

Troubleshooting

- Use the OSI model as a guide for systematic network troubleshooting
- Perform LAN and VLAN troubleshooting
- Troubleshoot routing protocols
- Troubleshoot IP addressing and host configuration
- Troubleshoot a device as part of a working network

- Troubleshoot an access list
- Perform simple WAN troubleshooting

Technology

- Describe the Spanning Tree process
- Evaluate the characteristics of LAN environments
- Evaluate the characteristics of routing protocols
- Evaluate rules for packet control
- Evaluate key characteristics of HDLC, PPP, Frame Relay, DDR, and ISDN technologies

CCNA

Cisco Certified Network Associate Exam

Exam Number: 640-801
Associated Certifications: CCNA
Duration: 90 minutes (55–65 questions)

Exam Description

The Cisco Certified Network Associate (CCNA) exam is the qualifying exam available to candidates pursuing a single-exam option for the CCNA certification. The CCNA (640-801) exam will test materials from the new ICND course as well as the new INTRO course. The exam will certify that the successful candidate has important knowledge and skills necessary to select, connect, configure, and troubleshoot the various Cisco networking devices. The exam covers topics on Extending Switched Networks with VLANS, Determining IP Routes, Managing IP Traffic with Access Lists, Establishing Point-to-Point Connections, and Establishing Frame Relay Connections.

Exam Topics

The following information provides general guidelines for the content likely to be included on the ICND exam. However, other related topics might also appear on any specific delivery of the exam.

Planning and Designing

- Design a simple LAN using Cisco technology
- Design an IP addressing scheme to meet design requirements
- Select an appropriate routing protocol based on user requirements
- Design a simple internetwork using Cisco technology
- Develop an access list to meet user specifications
- Choose WAN services to meet customer requirements

Implementation and Operation

- Configure routing protocols given user requirements
- Configure IP addresses, subnet masks, and gateway addresses on routers and hosts
- Configure a router for additional administrative functionality
- Configure a switch with VLANS and interswitch communication
- Implement a LAN
- Customize a switch configuration to meet specified network requirements
- Manage system image and device configuration files
- Perform an initial configuration on a router
- Perform an initial configuration on a switch
- Implement access lists
- Implement simple WAN protocols

Troubleshooting

- Use the OSI model as a guide for systematic network troubleshooting
- Perform LAN and VLAN troubleshooting
- Troubleshoot routing protocols
- Troubleshoot IP addressing and host configuration
- Troubleshoot a device as part of a working network
- Troubleshoot an access list
- Perform simple WAN troubleshooting

Technology

- Describe network communications using layered models
- Describe the Spanning Tree process
- Compare and contrast key characteristics of LAN environments
- Evaluate the characteristics of routing protocols
- Evaluate the TCP/IP communication process and its associated protocols
- Describe the components of network devices
- Evaluate rules for packet control
- Evaluate key characteristics of WANs

Introduction

The Cisco Certified Network Associate (CCNA) accreditation has become the leading introductory-level network certification available today. The CCNA certification is recognized by employers as providing candidates with a solid foundation of Cisco networking concepts, terminology, and skills. The CCNA exam covers a broad range of networking concepts, to prepare candidates for the technologies they are likely to be working with in today's network environments.

This book is your one-stop shop. Everything you need to know to pass the exam is in here. You do not have to take a class in addition to buying this book to pass the exam. However, depending on your personal study habits or learning style, you might benefit from buying this book *and* taking a class. Taking a CCNA certification class gives you dedicated study time and precious hands-on experience with live Cisco equipment.

Exam Preps are meticulously crafted to give you the best possible learning experience for the particular characteristics of the technology covered and the actual certification exam. The instructional design implemented in the *Exam Preps* reflects the task- and experience-based nature of Cisco certification exams. The *Exam Preps* provide the factual knowledge base you need for the exams, but then take it to the next level, with exercises and exam questions that are required in the CCNA exam.

Cisco has divided the CCNA from a single test into two separate exams, INTRO and ICND. Although the single CCNA exam still remains, Cisco recommends only those who are recertifying an existing CCNA certification take this exam. This CCNA Exam Prep title prepares you for both the INTRO exam, which covers the foundation Cisco network concepts and configurations, and the ICND exam, which covers the more advanced network concepts and configurations. Personally, we would recommend that you follow Cisco's advice on taking the two-exam path rather than the single CCNA exam. Although it may be tempting to go after the one-test "fast-track," this single exam is extremely difficult and has discouraged many potential CCNA candidates from continuing on in their Cisco certification journey.

How This Book Helps You

This book takes you on a self-guided tour of all the areas covered by the CCNA exam and teaches you the specific skills you need to achieve your certification. The book also contains helpful hints, tips, real-world examples, and exercises, as well as references to additional study materials. Specifically, this book is set up to help you in the following ways:

- *Organization*—This book is organized by individual exam objectives. Every objective you need to know for the CCNA exam is covered in this book. It presents the objectives in an order as close as possible to that listed by Cisco. However, we do not hesitate to reorganize them where needed to make the material as easy as possible for you to learn. We also make the information accessible in the following ways:
  - The full list of exam units and objectives is included in this introduction.
  - Each chapter begins with an outline that provides an overview of the material and the page numbers where particular topics can be found.
  - The objectives are repeated where the material most directly relevant to it is covered.
- *Instructional features*—This book provides multiple ways to learn and reinforce the exam material. Following are some of the helpful methods:
  - *Study and Exam Tips*—Read this section early on to help you develop study strategies. This section also provides valuable exam-day tips and information on exam and question formats, such as adaptive tests and case study-based questions.
  - *Exam Alerts*—These provide specific exam-related advice. Such tips might address what material is covered (or not covered) on the exam, how it is covered, mnemonic devices, or particular quirks of that exam.
  - *Review breaks and summaries*—Crucial information is summarized at various points in the book in lists or tables. Each chapter ends with a summary as well.
  - *Key terms*—A list of key terms appears at the end of each chapter.
  - *Notes*—Notes contain various kinds of useful or practical information, such as tips on technology or administrative practices, historical background on terms and technologies, or side commentary on industry issues.
  - *Warnings*—When using sophisticated information technology, there is always the potential for mistakes or even catastrophes to occur because of improper application of the technology. Warnings alert you to such potential problems.
  - *In the Field sidebars*—These relatively extensive discussions cover material that might not be directly relevant to the exam but that is useful as reference material or in everyday practice. In the Field sidebars also provide useful background or contextual information necessary for understanding the larger topic under consideration.
  - *Exercises*—Found at the end of the chapters in the "Apply Your Knowledge" section and in the "Challenge Exercises" found throughout chapters, exercises are performance-based opportunities for you to learn and assess your knowledge.

- *Extensive practice test options*—The book provides numerous opportunities for you to assess your knowledge and practice for the exam. The practice options include the following:
  - *Exam questions*—These questions appear in the "Apply Your Knowledge" section. You can use them to help determine what you know and what you need to review or study further. Answers and explanations for these questions are provided in a separate section, titled "Answers to Exam Questions."
  - *Practice exam*—A practice exam is included in the "Final Review" section of the book. The "Final Review" section and the practice exam are discussed later in this Introduction.
- *Final Review*—This part of the book provides two valuable tools for preparing for the exam:
  - *Fast Facts*—This condensed version of the information contained in the book is useful for last-minute review.
  - *Practice Exam*—A practice test is included. Questions on this practice exam are written in styles similar to those used on the actual exam. Use the practice exam to assess your readiness for the real thing. Use the extensive answer explanations to improve your retention and understanding of the material.

The book includes several other features, such as a "Suggested Readings and Resources" section at the end of each chapter that directs you to additional information that can aid you in your exam preparation and your real-life work. Valuable appendixes are provided as well, including a glossary and a description of what is on the CD-ROM (Appendix B).

For more information about the exam or the certification process, refer to the Cisco website, at www.cisco.com/certification.

Network Hardware and Software Requirements

As a self-paced study guide, *CCNA Exam Prep* is meant to help you understand concepts that must be refined through hands-on experience. To make the most of your studying, you need to have as much background on and experience with both common operating systems and network environments as possible. The best way to do this is to combine studying with work on actual networks. These networks need not be complex; the concepts involved in configuring a network with only a couple of routers and a switch follow the same principles as those involved in configuring a network that has hundreds of connected systems. This section describes the recommended equipment for a solid practice environment.

To fully practice some of the exam objectives, you need to create a network with two (or more) routers networked together with one (or more) Cisco switches. We recognize that finances may be limited, and suggest purchasing routers from the Cisco 2500 series (primarily the 2501 or 2514 routers). These can commonly be found for between $50.00–$150.00 through a used equipment vendor or online auction. Likewise, a Catalyst 1912 or 1924 switch can typically be found for under $50.00. Some of the syntax on the 1900 series switches may be slightly different than Cisco's mainline switches, but most of the commands will be similar. Do realize that Cisco has strict restrictions about using used or remanufactured equipment in production networks. Although Cisco hardware can be resold, the software that runs them (Cisco's IOS) cannot. Before used or remanufactured equipment can be used in a production environment, the IOS software must be re-licensed through Cisco or an authorized reseller. Be sure to verify these regulations before using your lab equipment in a production network.

If you are looking to build a lab environment, the following is a more detailed list of the minimum equipment you need. Do keep in mind that this is the minimum equipment that we suggest for the CCNA. If you plan on moving into the CCNP, CCVP, or CCSP programs, you may want to look into the more advanced (and expensive) Cisco equipment such as the 2600 or 3600 routers.

- At least one Cisco 2514 router, which has two 10Mbps AUI ethernet ports to test configurations such as NAT and two serial ports to simulate WAN connectivity.
- One additional Cisco router, such as the 2501, with one ethernet port and two serial ports to create and test WAN connectivity.
- A DB-60 DTE to DB-60 DCE cross-over serial cable.
- At least one Cisco switch, ideally a 2900XL or 2950; however, a 1900 series switch will also suffice. If you decide to use a 1900 series switch, be sure it is equipped with the Enterprise IOS version, which includes the command-line interface. The Standard IOS for the 1900 allows only a menu-driven configuration.
- At least one rollover console cable.
- Multiple straight-through and cross-over network cables.
- Optionally, adding one or more PCs to the network can add realism and troubleshooting advantages. These PCs can be connected to the switch and act as network clients in your scenarios.

It's easy to get access to the necessary computer hardware and software in a corporate business environment. It can be difficult, however, to allocate enough time within the busy workday to complete a self-study program. Most of your study time will occur after normal working hours, away from the everyday interruptions and pressures of your regular job.

Advice on Taking the Exam

More extensive tips are found in the "Study and Exam Prep Tips" section, but keep this advice in mind as you study:

- *Read all the material*—Cisco has been known to include material that is not expressly specified in the objectives. This book includes additional information that is not reflected in the objectives, in an effort to give you the best possible preparation for the examination—and for your real-world experiences to come.
- *Complete the exercises in each chapter*—They will help you gain experience in using the specified methodology or approach. Cisco exams require task- and experienced-based knowledge and require you to have an understanding of how certain network procedures are accomplished.
- *Use the exam 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 know. If you are struggling, study some more, review, and then assess your knowledge again.
- *Review the objectives*—Develop your own questions and examples for each objective listed. If you can develop and answer several questions for each objective, you should not find it difficult to pass the exam.

NOTE

Exam-Taking Advice Although this book is designed to prepare you to take and pass the Cisco certification exam, there are no guarantees. Read this book, work through the questions and exercises, and when you feel confident, take the practice exam. Your results should tell you whether you are ready for the real thing. Keep in mind that lots of capable, intelligent people fail these exams one or more times. Cisco exams are some of the most difficult in the industry; if you do fail the exam, use it as a tool to help you focus your studies in the areas where you felt weak. As overused as this guidance is, we still need to say it: Don't give up. Every author writing this book has hit their own low points in the certification journey. Trust us—after you pass the CCNA exam, the benefits will far outweigh the cost.

When taking the actual certification exam, make sure that you answer all the questions before your time limit expires. Do not spend too much time on any one question. If you are unsure about the answer to a question, answer it as best as you can and move on. This especially applies to simulation-based questions. Partial credit is given on these questions if you have completed the majority of the steps, so don't get hung up on any one simulation objective for an extended time.

Remember that the primary objective is not to pass the exam but to understand the material. When you understand the material, passing the exam should be simple. Knowledge is a pyramid; to build upward, you need a solid foundation. This book and the CCNA certification are designed to ensure that you have that solid foundation.

Good luck!

PART I

Exam Preparation

CHAPTER ONE

Standard Internetworking Models

Objectives

This chapter covers the following Cisco-specified objectives for the "Technology" section of the Cisco Certified Network Associate (CCNA) exam:

Describe network communications using layered models

Evaluate rules for packet control

Evaluate TCP/IP communication process and its associated protocols

- The OSI model and the TCP/IP model are both layered models that provide architecture and standards to help you understand the foundation of internetworking. The Cisco 3-Layer Hierarchical Model was created by Cisco to help design a network using Cisco products.
- Layered models provide an overview of data transmission and the associated rules for controlling that data to ensure delivery over a network.
- The TCP/IP suite is widely used in internetworking. The communication process and the TCP/IP protocols are integral to understanding how these networks work today.

Outline

Study Strategies

- Read through the exam objectives at the beginning of the chapter.
- Review the characteristics of each internetwork and keep in mind which network would be appropriate based on a given company and its individual requirements.
- Identify the names and primary functions of each OSI model layer. Create a mnemonic device to help you remember the seven layers.
- Identify the protocols and standards that are used at each layer of the OSI model. Pay close attention to the application protocols used at the Application layer.
- Review and memorize associated UDP and TCP port assignments for several well-known protocols.

Introduction

Whether you already work in the computer technology industry, or you are trying to enter the field as a newcomer, it is important in this day and age to back up your resume with a vendor-specific certification. If you search job postings on the Internet, it is commonplace for hiring companies today to require or recommend that an applicant have at least one vendor certification. Other companies ask that their current employees obtain certifications as a way to meet goals for advancement. Regardless of the underlying reason, studying for the CCNA is a smart move.

The CCNA certification was developed by Cisco to test your knowledge of networking at a beginner's level. Cisco wants to identify individuals capable of installing, configuring, and maintaining small-scale networks, which include Local Area Networks (LANs) and Wide Area Networks (WANs).

The purpose of this first chapter is to provide a general overview of the concepts that will ultimately be the foundation for the rest of this book. To start this chapter, the first step is to define the term *internetwork*. It then reviews the general concepts that pertain to LAN and WAN internetworks, as well as the Metropolitan Area Network (MAN), Storage Area Network (SAN), and Virtual Private Network (VPN). Later chapters go into more detail regarding the technologies that are related to both LAN and WAN.

This chapter also gives an in-depth look at the three networking reference models that are likely to be tested on the CCNA exam. These are the Open Systems Interconnection (OSI), Transmission Control Protocol/Internet Protocol (TCP/IP), and Cisco 3-Layer Hierarchical models. Being familiar with these models is fundamental to understanding how networks operate, as well as how various devices and protocols fit into their structure. By using these models, you can design an infrastructure based on a given organization's specific requirements.

What Is an Internetwork?

Simply put, an internetwork is the connection of more than one network. These networks are linked together by an internetworking device to provide communication between the networks. Internetworks may also be referred to as an *internet*. Notice the lower case *i* at the beginning of the word *internet*—this differentiates it from the Internet. The Internet is considered to be the largest internet in the world. I know the phrase sounds odd, but it is a great example of how thousands of smaller networks are joined together to form one large global internetwork. Another example of an internet would be the connection of individual LANs to form a WAN.

The term *internetworking* signifies the industry, products, and processes that are required to handle the challenges of network interoperability. Such issues can be quite complex because of the existence of multiple vendors and protocols.

Types of Internetworks

There are various types of internetworks discussed in greater detail. I already mentioned LAN and WANs, which are the most common types of internetworks. Other important internetworks include MANs, SANs, and VPNs, which are also reviewed in this section.

Local Area Network (LAN)

Like the name suggests, LANs are limited to a local or small geographical area. An example of a LAN would be a network of individual computers or workstations that are connected in a single department. These users have shared access to resources such as data and network devices. Users on a LAN segment can share a network printer and communicate with one another via email. Also, they are governed by one authoritative administrator.

NOTE

LAN is the smallest network in geographical size.

Given the size constraints, downsides of a LAN network are limited distance that data can travel and a limited number of computers that can be connected. An upside of a LAN is fast data transfer with data speed that can reach up to 10Gbps.

Xerox Corporation worked in collaboration with DEC and Intel to create ethernet, which is the most pervasive LAN architecture used today. Ethernet has evolved and has seen significant improvements in regard to speed and efficiency.

Other significant LAN technologies are Fiber Distributed Data Interface (FDDI) and token ring.

EXAM ALERT

An understanding of LAN technology is required for the CCNA exam. Each ethernet version is discussed in detail in Chapter 3, "Data Link Networking Concepts."

Local area networking uses switches, bridges and/or repeaters, and hubs to interconnect LANs and increase overall size. Routers are used to connect a LAN to a WAN or MAN. Both of these scenarios form an internetwork.

Figure 1.1 provides an example of a LAN. A single switch connects to all the peripheral network devices in this example.

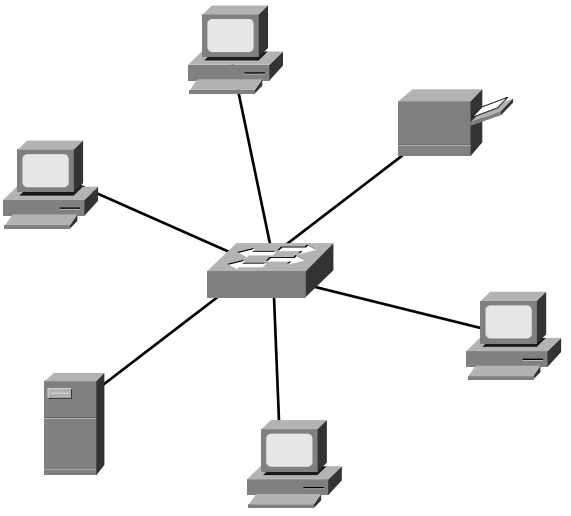


FIGURE 1.1 Example of a LAN.

EXAM ALERT

Multiple LANs are interconnected with switches, bridges, or repeaters.
LANs are connected to a MAN or a WAN with a router.

Metropolitan Area Network (MAN)

A MAN is larger than a LAN but smaller than or equal in size to a WAN. Think of it as the size of a city or college campus network, which can range anywhere from 5 to 50km in diameter. MANs are typically owned and managed by a single entity. This could be an ISP or telecommunications company that sells its services to end-users in that metropolitan area. For all intents and purposes, a MAN has the same characteristics as a WAN with distance constraints.

Wide Area Network (WAN)

WANs cover more than one geographical area. This is ideal for a company that has offices in different cities around the country or even the world. Each office can connect to the other sites in the WAN via a router. Connectivity from router to router is a circuit leased from a telephone or communications company, such as AT&T to name one. The larger the circuit a company needs to transmit data, the more it costs to lease. The company also needs to pay close attention to the performance of its WAN connection because that cost can directly impact its ability to do business. It is important to keep an eye on the amount of traffic that is

going over each circuit to ensure that you have sufficient throughput. *Throughput* refers to the amount of data transferred in a specified timeframe.

NOTE

Earlier I mentioned that the Internet is the perfect example of an internetwork. It is also an excellent example of a WAN network where thousands of small networks are joined together to form one large global network.

The following are WAN encapsulations that are reviewed in Chapter 15, "Wide Area Networks":

- Frame Relay
- PPP
- ISDN
- HDLC—Cisco standard

EXAM ALERT

WAN characteristics, protocols, services, and troubleshooting techniques are all possible exam topics. Therefore, WAN technologies are discussed in length in Chapter 15.

Figure 1.2 provides an example of a WAN. In this example, a central router connects two LANs to create the WAN. Each LAN has a switch connected to its local end-user devices.

Storage Area Network (SAN)

SAN may be referred to as a subnetwork or special purpose network. Its special purpose is to allow users on a larger network to connect various data storage devices with clusters of data servers. Cisco offers this service with its Cisco MDS 9000 Series Multilayer SAN Switches. These switches provide scalable storage solutions for the end user.

Virtual Private Network (VPN)

VPN is a private network that can access public networks remotely. VPN uses encryption and security protocols to retain privacy while it accesses outside resources. When employed on a network, VPN enables an end user to create a virtual tunnel to a remote location. Typically, telecommuters use VPN to log in to their company networks from home.

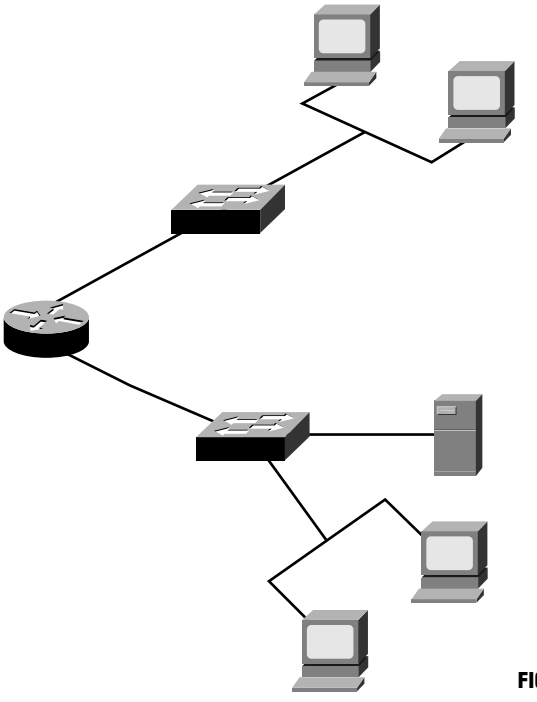


FIGURE 1.2 Example of a WAN.

Open Systems Interconnection (OSI) Model

Objective:

Describe network communications using layered models

By now you understand the concept of an internetwork. Now the OSI model will help you see just how an internetwork operates by using a *layered architecture*.

The International Organization for Standardization (ISO) created the OSI model as the first major attempt to internetwork various vendor-specific networks, the ultimate goal being that these different vendor networks could work together in harmony. This model consists of seven layers. Although it is not widely used today, the terminology is prevalent in the networking community. The OSI model may also be helpful when troubleshooting a network issue.

First of all, it is important to know the name of each layer and its corresponding layer number. This will help you remember where the layers reside in the OSI model. You may also hear the layers referred to by number, so knowing them will also help in that respect. Table 1.1 provides a list of all seven layers.

TABLE 1.1 The Seven Layers of the OSI Model

Layer Number	Layer Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

In general, each layer communicates with the adjacent layers on the OSI model and the corresponding layer on another system. For example, the Presentation layer communicates with the Application layer, the Session layer, and also with the Presentation layer of another connected system.

EXAM ALERT

It is crucial that you learn the layers of the OSI model and their respective functions. Also know that the OSI model helps with multi-vendor integration. The functions are reviewed in this chapter. For now, to help you remember the names of the layers and their order, it may be helpful to come up with a mnemonic device. The most commonly used phrase is "All People Seem To Need Data Processing." There are many other phrases out there, some of which are quite crass, but it is ultimately up to you to decide whether this will help.

Upper Layers

Now that you know the layers in order, it is also important to know that the layers may also be referred to as the *upper* and *lower* layers. Primarily, the upper layers of the OSI model define communications between applications that reside on end-user stations. This is generally related to software communication. Table 1.2 provides a list of the layers considered as the upper layers.

TABLE 1.2 The Upper Layers of the OSI Model = Applications

Layer Number	Layer Name
7	Application
6	Presentation
5	Session

Application Layer

Layer 7 provides an interface between a host's communication software and any necessary external applications (such as email, file transfers, and terminal emulation). This layer can also evaluate what resources are necessary to communicate between two devices and determine their availability.

Layer 7 also provides the following functionality:

- Synchronization of client/server applications
- Error control and data integrity between applications
- System-independent processes to a host

Table 1.3 provides a list of the protocols supported by the Application layer.

TABLE 1.3 Application Protocols Supported by the Application Layer

Application Protocols	Function
Telnet	A TCP/IP protocol that provides terminal emulation to a remote host by creating a virtual terminal. Secure CRT is one program that can be installed on a user computer to create telnet sessions. This protocol requires authentication via a username and password.
Hypertext Transfer Protocol (HTTP)	Enables web browsing with the transmission of Hypertext Markup Language (HTML) documents on the Internet.
Secure Hypertext Transfer Protocol (HTTPS)	Enables secure web browsing. A secure connection is indicated when the URL begins with https:// or when there is a lock symbol at the lower-right corner of the web page that is being viewed.
File Transfer Protocol (FTP)	Enables a user to transfer files. Provides access to files and directories. Securely implemented with telnet, which allows remote authentication to an FTP server.
Trivial File Transfer Protocol (TFTP)	A bare-bones version of FTP that does not provide access to directories. With TFTP you can just send and receive files. Unlike FTP, TFTP is not secure and sends smaller blocks of data.
Domain Name System (DNS)	Resolves hostnames such as www.cisco.com into IP addresses.
Simple Mail Transfer Protocol (SMTP)	Sends electronic mail across the network.
Post Office Protocol 3 (POP3)	Receives electronic mail by accessing an Internet server.

TABLE 1.3 *Continued*

Application Protocols	Function
Network File System (NFS)	Enables users with different operating systems (for example, NT and Unix workstations) to share files.
Network News Transfer Protocol (NNTP)	Offers access to Usenet newsgroup postings.
Simple Network Management Protocol (SNMP)	Monitors the network and manages configurations. Collects statistics to analyze network performance and ensure network security.
Network Time Protocol (NTP)	Synchronizes clocks on the Internet to provide accurate local time on the user system.
Dynamic Host Configuration Protocol (DHCP)	Works dynamically to provide an IP address, subnet mask, domain name, and a default gateway for routers. Works with DNS and WINS (used for NetBIOS addressing).

EXAM ALERT

Know the Protocols Be prepared to identify which protocols are used at the Application layer of the OSI model. Also familiarize yourself with the general functions of these protocols.

Presentation Layer

Layer 6 presents data to the Application layer and acts as a data format translator. Format translation is necessary to ensure that the data can be read by applications. Layer 6 also handles the structuring of data and negotiating data transfer syntax to Layer 7. Processes involved include data encryption, decryption, compression, and decompression.

NOTE

The Presentation layer is the only layer that can actually change data.

Layer 6 protocols include the following:

- Joint Photographic Experts Group (JPEG)
- American Standard Code for Information Interchange (ASCII)
- Extended Binary Coded Decimal Interchange Code (EBCDIC)
- Tagged Image File Format (TIFF)
- Graphic Image File (GIF)

- Picture (PICT)
- Moving Picture Experts Group (MPEG)
- Musical Instrument Digital Interface (MIDI)
- QuickTime
- Rich Text Format (RTF)

NOTE

Graphic and visual images use PICT, TIFF, and JPEG. Audio and video formatting uses MIDI, MPEG, QuickTime, and RTF.

Session Layer

Layer 5 is primarily concerned with dialog control among devices. This layer determines the beginning, middle, and end of a session or conversation that occurs between applications. In this way, the Session layer acts as an intermediary for those applications. Table 1.4 lists the Session layer protocols and their functionality.

TABLE 1.4 Session Layer Protocols and Their General Functionality

Session Layer Protocol	Function
Network File System (NFS)	Accesses remote resources transparently and represents files and directories as if local to the user system. Developed by SUN and used on Unix workstations.
Structured Query Language (SQL)	Functions as a query language that requests, updates, and manages databases. Developed by IBM and compatible with XML and HTML.
Remote Procedure Call (RPC)	Basis for client/server communications. Calls are created on the client and then carried out on the server.
AppleTalk Session Protocol (ASP)	Also client/server–based communications, but specific to AppleTalk client and server devices.
X Window	Communicates with remote Unix machines and enables the user to operate the device as if attached locally.
Digital Network Architecture Session Control Protocol (DNA SCP)	A proprietary Digital Equipment Corporation Networking (DECnet) protocol, also referred to as a DECnet session.

Lower Layers

The lower layers of the OSI model focus on data transport, which can be achieved via a router, switch, or a physical wire. They are listed in Table 1.5.

TABLE 1.5 The Lower Layers of the OSI Model—Responsible for Data Transport

Layer Number	Layer Name
4	Transport
3	Network
2	Data Link
1	Physical

Transport Layer

Layer 4 is responsible for end-to-end connections and data delivery between two hosts. The ability to segment and reassemble data is a key functionality of this layer. For example, when one system is sending data to another system, that data can be segmented into smaller data blocks and transmitted across the network. The receiving system can then reassemble the segmented data blocks at the Transport layer. Transmissions occur via logical connectivity between the sender and destination. Layer 4 provides transparent data transfer by hiding details of the transmission from the upper layers.

EXAM ALERT

Segmenting occurs at the Transport layer.

Layer 4 also provides the following functionality:

- Fault detection
- Error recovery
- Establishing, maintaining, and tearing down virtual circuits

The Transport layer can provide reliable networking via acknowledgments, sequencing, and flow control.

- **Acknowledgments**—Delivered segments are acknowledged to the sender. If they are not acknowledged, the sender will retransmit.

- **Sequencing**—Data segments are sequenced into their original order when they arrive at the destination.
- **Flow Control**—Provides buffer controls that prevent packet flooding to the destination host. Buffers store bursts of data for processing when the transmission is complete.

Layer 4 protocols include the following:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Sequenced Packet Exchange (SPX)—A reliable communications protocol created by Novell NetWare

NOTE

TCP and UDP protocols are important to know for the exam. These are discussed later in this chapter, under the "Transport Layer" section of the TCP/IP model.

Network Layer

Layer 3 is where the best path determination is made for packet delivery across the network. Routed protocols such as IP are used to determine logical addressing, which can identify the destination of a packet or datagram. The most common network device found at the Network layer is a router; however, Layer 3 switches may also be implemented.

A router at the Network layer follows these general steps to ensure proper data transport:

1. The router checks the destination IP address of the incoming packet on the router interface.
2. Packets destined for that router are processed, whereas packets destined for another router must be looked up in the routing table.
3. The router determines an exit interface based on the routing table and sends the packet to the interface for framing and forwarding. If there is no route in the routing table, the packet is dropped by the router.

A routing table on a router contains the following information:

- Network Address
- Interface—Exit interface used to forward packets
- Metric—Distance to reach a remote network

There are two packet types utilized at Layer 3:

- **Data Packets**—Transport data across the internetwork and are supported by IP and IPX protocols.
- **Route Update Packets**—Send updates to neighbor routers about all networks connected to that internetwork and are supported by routing protocols such as RIP, EIGRP, and OSPF.

Layer 3 routed protocols include the following:

- Internet Protocol (IP)
- Internet Packet Exchange (IPX)—Part of the IPX/SPX protocol suite created by Novell NetWare
- AppleTalk DDP—Datagram delivery protocol used by Apple

EXAM ALERT

For the exam, this book focuses on IP, which is reviewed in Chapter 4, "IP at the Network Layer."

NOTE

Routers and logical addressing (that is, IP addresses) are used at Layer 3. Data at Layer 3 is in the form of packets or a datagram.

Data Link Layer

Layer 2 ensures reliable data transfer from the Network layer to the Physical layer for transmission across the network.

Two domains determine data transport reliability:

- **Broadcast Domain**—A group of nodes that can receive each other's broadcast messages and are segmented by routers.
- **Collision Domain**—A group of nodes that share the same media and are segmented by switches. A collision occurs if two nodes attempt a simultaneous transmission. *Carrier Sense Multiple Access Collision Detection (CSMA/CD)* is an access method that sends a jam signal to notify the devices that there has been a collision. The devices then halt transmission for a random back-off time.

EXAM ALERT

Routers segment broadcast domains, whereas switches segment collision domains.

Data received from the Network layer is formatted into frames to be transmitted to the Physical layer. Physical addressing or hardware addressing (rather than logical addressing) ensures that data is delivered to the appropriate node on the LAN. This layer is also responsible for error notification (not correction), network topology, and flow control.

This is the only layer of the OSI model that has sublayers. The two sublayers in question define the IEEE Ethernet 802.3 frame, which in turn provides physical addressing and flow control. Also, routed protocol information (IP, IPX, AppleTalk, and so on) is provided to the upper layers.

The IEEE Ethernet 802.3 sublayers are Media Access Control (MAC) and Logical Link Control (LLC), and are described in the following sections.

Media Access Control (MAC)

The MAC address is the hard-coded address on the network interface controller (NIC) of the Physical layer node attached to the network. Although the source address will always be a unicast or single destination address, the destination address can be a unicast, multicast (a determined subset of nodes), or broadcast (all nodes in a broadcast domain) address.

Each MAC address must be unique and follow this format:

- It must consist of 48 bits.
- It must be displayed by 12 hexadecimal digits (0-9, A-F).
- The first 6 hexadecimal digits in the address are a vendor code or organizationally unique identifier (OUI) assigned by the NIC manufacturer.

This is an example of a MAC address: 00:00:07:A9:B2:EB

EXAM ALERT

Know the structure of a MAC address and that the broadcast address value is FFFF FFFF FFFF.

Logical Link Control (LLC)

The LLC sublayer complements the MAC sublayer in the ethernet model; the LLC is responsible for framing, error, and flow control. LLC provides a service access point (SAP) identifier in the frame. The SAP field of the frame consists of one byte that identifies an

upper layer protocol (for example, 06 = IP, whereas E0 = IPX). The LLC inserts a destination SAP (DSAP) and a Source SAP (SSAP) in the frame. Figure 1.3 provides an example of an ethernet frame.

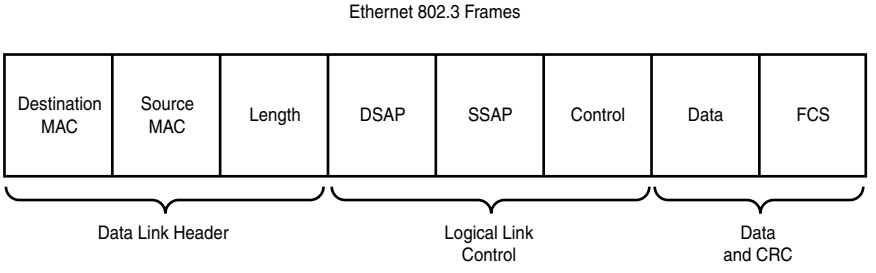


FIGURE 1.3
Example of an ethernet frame.

Two devices are used at the Data Link layer:

- **Bridges**—Bridges connect two segments in a single network or two networks together. They simply forward data between those segments/networks without performing an analysis or redirection of the data.
- **Switches**—At Layer 2, switches are multi-port bridges that utilize Application Specific Integrated Circuit (ASIC) to forward frames. Each port of the switch has a dedicated bandwidth.

EXAM ALERT

Dedicated bandwidth enables the switch port to guarantee the speed assigned to that port. For example, 100Mbps port connections get 100Mbps transmission rates.

Although both devices create a separate collision domain for each connected device, all the devices connected to either are a part of the same broadcast domain. Remember that broadcast domains are segmented at the Network layer by routers.

Switches and bridges identify MAC addresses by scanning for the source MAC address of each frame received.

NOTE

Bridging and switching are discussed in more detail in Chapter 3.

Physical Layer

Layer 1 moves bits between nodes. Electrical, mechanical, procedural, and functional requirements are defined at the Physical layer to assist with the activation, maintenance, and deactivation of physical connectivity between devices.

Other attributes of Layer 1 include the following:

- Specification of voltage, wire speed, and pin-out cables
- Capability to receive and transmit a data signal
- Identification of the interface that is set up between the data terminal equipment (DTE) and the data communication equipment (DCE)

NOTE

Although DTE is the locally attached device, DCE is typically found at the service provider. DTE services can be accessed with either a model or a channel service unit/data service unit (CSU/DSU). For additional information on associated Layer 1 technologies, continue on to Chapter 2, "Physical Layer Networking Concepts."

Devices at the Physical layer include hubs and repeaters. Hubs and repeaters *extend* a network, whereas Layer 2 and Layer 3 devices *segment* a network.

OSI Layered Communications

Objective:

Evaluate rules for packet control

Now that you have reviewed all seven layers of the OSI model, it is a good time to see how those layers communicate with each other. Each layer passes information to adjacent layers by using Protocol Data Units (PDUs). The PDU includes both the message and the protocol/control information from the forwarding layer. That control information can be in the form of a header or trailer. The process of adding a header or trailer to the PDU at each layer of the OSI is called *encapsulation*.

Each layer has an associated control information name, which is listed in Table 1.6.

TABLE 1.6 OSI Model Layers and Their Control Information Names

OSI Layer	Control Information Name
Application	Data
Presentation	
Session	
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit

Based on this chart, you can see how information is encapsulated as it travels down through the various layers. The correct order for data encapsulation is data, segment, packet, frame, and bit.

EXAM ALERT

It is important to know the control information name for the OSI layers and the correct order for data encapsulation.

REVIEW BREAK

Let's take a few minutes to go over the OSI model. Table 1.7 lists the seven layers and significant aspects of each layer.

TABLE 1.7 OSI Model Layers and Their Respective Functionalities

OSI Layer	Important Functions
Application	Provides an interface between a host's communication software and any necessary external applications.
	Evaluates what resources are necessary and the available resources for communication between two devices.
	Synchronizes client/server applications.
	Provides error control and data integrity between applications.
	Provides system-independent processes to a host.

(continues)

TABLE 1.7 *Continued*

OSI Layer	Important Functions
Presentation	Presents data to the Application layer.
	Acts as a data format translator.
	Handles the structuring of data and negotiating data transfer syntax to Layer 7.
	Processes involved include data encryption, decryption, compression, and decompression.
Session	Handles dialog control among devices.
	Determines the beginning, middle, and end of a session or conversation that occurs between applications (intermediary).
Transport	Manages end-to-end connections and data delivery between two hosts.
	Segments and reassembles data.
	Provides transparent data transfer by hiding details of the transmission from the upper layers.
Network	Determines best path for packet delivery across the network.
	Determines logical addressing, which can identify the destination of a packet or datagram.
	Uses data packets (IP, IPX) and route update packets (RIP, EIGRP, and so on).
	Uses routed protocols IP, IPX, and AppleTalk DDP.
	Devices include routers and Layer 3 switches.
Data Link	Ensures reliable data transfer from the Network layer to the Physical layer.
	Oversees physical or hardware addressing.
	Formats packets into a frame.
	Provides error notification.
	Devices include bridges and Layer 2 switches.
Physical	Moves bits between nodes.
	Assists with the activation, maintenance, and deactivation of physical connectivity between devices.
	Devices include hubs and repeaters.

TCP/IP Model

Objective:

Evaluate TCP/IP communication process and its associated protocols

The TCP/IP model, also known as the Department of Defense (DoD) model, was created by the DoD when they developed the TCP/IP protocol suite. Their goal was to provide reliable networking and data integrity in the event of a disaster. This model is prevalent in the current

networking community. Although the OSI model is rarely used (except for the terminology), TCP/IP communications are ingrained in today's networking fabric and are a focal point on the CCNA exam.

NOTE

So far, the Internet has been a great example of an internetwork and a WAN. It's also a great example of the TCP/IP protocol suite at work.

Essentially the TCP/IP model has many similarities to the OSI model. Table 1.8 lists the layers of the OSI model in the left column and the related layers of the TCP/IP model in the right.

TABLE 1.8 Layers of the OSI and TCP/IP Models

OSI Layer	TCP/IP Layer
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data Link	Network Access
Physical	

Application Layer

This layer combines functionalities of the three top layers of the OSI model and may also be called the Process/Application layer. Some of the most popular applications (email, file transport, and so on) interface with this layer to communicate with other applications on the network.

If you'll remember, the description of the Application layer of the OSI model included a list of application protocols and their primary functions. (Refer to Table 1.3.) These applications are also relative to the Application layer of the TCP/IP model.

Table 1.9 provides a quick list of the protocols at their respective layers of the TCP/IP model.

TABLE 1.9 Protocols for Each Layer of the TCP/IP Model

TCP/IP Layer	Protocols			
Application	Telnet	HTTP/HTTPS	FTP	TFTP
	DNS	SMTP	POP3	NFS
	NNTP	SNMP	NTP	DHCP
Transport	TCP		UDP	
Internet	ICMP	ARP	RARP	IP
Network Interface	Ethernet	Fast Ethernet	Token Ring	FDDI

Transport Layer

The Transport layer corresponds with the Transport layer of the OSI model and is also known as the Host-to-Host layer. Not only is this layer responsible for reliable data delivery, but it can also make certain that data arrives in the proper order. You will see two transport layer protocols on the CCNA exam. These protocols are TCP and UDP. The following sections cover each protocol and its related applications.

TCP

TCP is a reliable connection-oriented protocol. TCP uses acknowledgments, sequencing, and flow control to ensure reliability (please refer back to the "Transport Layer" section of the OSI model for definitions of these terms). A TCP segment contains fields for the Sequence, Acknowledgment, and Windowing numbers. These fields help make sure that datagrams arrive undamaged. This is considered to be reliable delivery.

TCP uses Positive Acknowledgment and Retransmission (PAR):

- The source device begins a timer when a segment is sent and retransmits if the timer runs out before an acknowledgment is received.
- The source device keeps track of segments that are sent and requires an acknowledgment for each segment.
- The destination device acknowledges when a segment is received by sending a packet to the source that iterates the next sequence number it is looking for from the source.

Figure 1.4 shows the TCP segment header format.

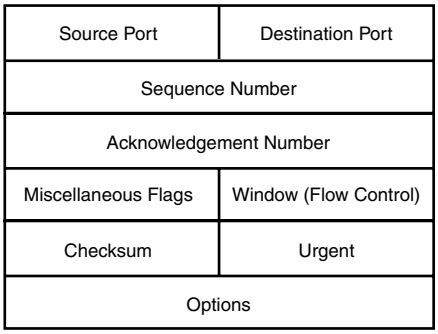


FIGURE 1.4 TCP segment header format.

Flow control via TCP includes *windowing*. Windowing is a method for traffic congestion control where a window is determined by the receiving system to limit the number of data segments (bytes) that can be sent by the source device without an acknowledgment from the recipient. The size of a window determines the number of unacknowledged data segments allowed by the receiving system. Window sizes vary and can change throughout the duration of a connection. Increasing a window size enables more data segments to be transmitted to the recipient before acknowledgment, whereas decreasing the window size allows for fewer data segments to be transmitted before an acknowledgment is sent.

As mentioned at the beginning of this section, TCP is a connection-oriented protocol. When a source device is ready to transmit data, it sets up a Connection-Oriented Communication session with the intended recipient. This is a *call setup* or a *three-way handshake*. When the data is successfully transmitted, a call termination occurs to disconnect the virtual circuit.

The three-way handshake includes the following steps:

1. A "connection agreement" segment is sent to the recipient asking to synchronize systems. This step is associated with the term *SYN packet*.
2. The second and third segments acknowledge the request to connect and determine the rules of engagement. Sequencing synchronization is requested of the receiving device. A two-way connection is established. This step is associated with the term *SYN-ACK packet*.
3. A final segment is sent as an acknowledgement that the rules have been accepted and a connection has been formed. This step is associated with the term *ACK packet*.

For the exam you may also be asked to identify the applications that use TCP and their respective port numbers. Both TCP and UDP use port numbers. Public applications are assigned port numbers below 256. Numbers 256-1023 are allocated to companies. Numbers above 1023 are dynamically assigned by an application. Access lists can use port numbers to filter traffic. Table 1.10 lists applications that use TCP.

TABLE 1.10 Applications Using TCP

Application	Port Number(s)
FTP	20,21
Telnet	23
SMTP	25
DNS (zone transfers)	53
HTTP	80
POP3	110
NNTP	119
HTTPS	443

EXAM ALERT

The application and port identifiers used by TCP and UDP should be memorized for the exam.

UDP is the other protocol that is used at the Transport layer of the TCP/IP model.

UDP

UDP is much simpler than TCP because it is a connectionless protocol. UDP headers contain only the source and destination ports, a length field, and a checksum. Because of the lack of a sequence, acknowledgment, and windowing field, UDP cannot guarantee delivery. Because there are no delivery guarantees, UDP is considered unreliable. With this protocol, it is up to the application to provide reliability. Figure 1.5 shows a UDP segment header.

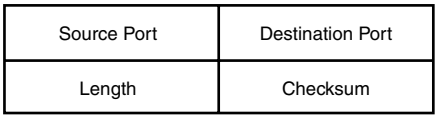


FIGURE 1.5 The UDP header.

On the plus side, UDP is considerably cheaper to implement and has faster transfer rates. Table 1.11 lists the applications that use UDP.

TABLE 1.11 Applications Using UDP

Application	Port Number(s)
DHCP	67,68
DNS (name resolution)	53
TFTP	69

TABLE 1.11 *Continued*

Application	Port Number(s)
NTP	123
SNMP	161

NOTE

Note that DNS is listed for both TCP and UDP because it can be used with both protocols. With TCP, DNS is used for zone transfers and with UDP, it is used for name resolution.

Challenge

As mentioned in the TCP section of this chapter, knowing the applications that use TCP and UDP is important for the CCNA exam. It is also important that you know which port number is assigned to each application. Fill in the blanks that are given in each of the following tables. You may reference Tables 1.10 and 1.11, but I strongly suggest that you keep using these charts until you have this information memorized.

Applications Using TCP

Application	Port Number(s)

Applications Using UDP

Application	Port Number(s)

Internet Layer

The Internet layer corresponds with the Network layer of the OSI model.

The following protocols relate to the logical transmission of packets:

- IP
- ICMP
- ARP, RARP, and Proxy ARP

IP

IP uses logical or virtual addressing to get a packet from a source to its destination. IP addresses are used by routers to make forwarding decisions.

Some key characteristics of IP addresses include the following:

- Addresses are allocated by the Internet Assigned Numbers Authority (IANA).
- IPv4 IP addresses are 32 bits, divided into four octets (8 bits each). An example of an IP address in dotted decimal format would be 172.16.122.204.
- The minimum value (per octet) is 0 and the maximum value is 255.
- IPv6, which is the future of IP addresses, is 128 bits.

Figure 1.6 shows the data fields that make up an IP datagram.

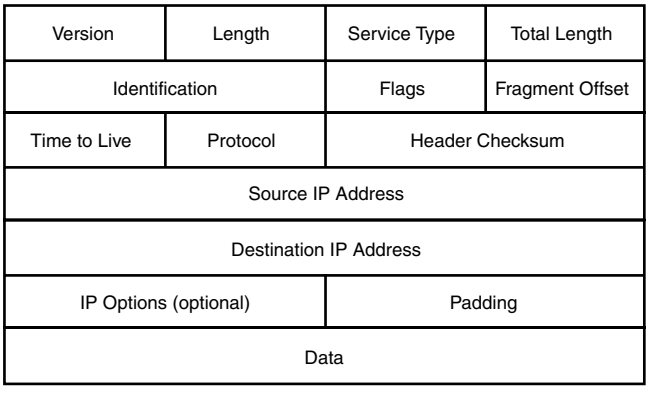


FIGURE 1.6 IP datagram.

NOTE

IP addressing is a topic discussed with additional detail in Chapter 4.

ICMP

Internet Control Messaging Protocol is used by ping and traceroute utilities.

Ping (Packet Internet Groper) enables you to validate that an IP address exists and can accept requests. The following transmissions are used by the Ping utility:

- Ping sends an echo request packet to receive the echo response.
- Routers send Destination Unreachable messages when they can't reach the destination network and they are forced to drop the packet. The router that drops the packet sends the ICMP DU message.

Traceroute traces the route or path taken from a client to a remote host. Traceroute also reports the IP addresses of the routers at each next hop on the way to the destination. This is especially useful when you suspect that a router on the route to an unreachable network is responsible for dropping the packet.

NOTE

Extended ping enables you to select a datagram size and a timeout.

ARP, RARP, and Proxy ARP

The Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), and Proxy Address Resolution Protocol (Proxy ARP) are all protocols used at the TCP/IP model's Internet layer.

ARP maps a known IP address to a MAC address by sending a broadcast ARP. When the destination IP address is on another subnet, the sender broadcasts ARP for the router's ethernet port or default gateway, so the MAC address sent back is that of the router's ethernet port.

RARP maps a known MAC address to an IP address.

Proxy ARP enables a router to respond to an ARP request that has been sent to a remote host. Some Unix machines (especially Solaris) rely on Proxy ARP versus default gateways.

Network Interface Layer

This layer corresponds with the Data Link and Physical layers of the OSI model. As mentioned earlier in the chapter, this layer manages hardware addressing and physical data transfer.

Cisco 3-Layer Hierarchical Model

When I think of the word *hierarchy* outside the realm of networking, I think of the military. Each branch of the military has a list of ranks that is assigned to each soldier. In the Army for

example, the ranks range from an enlisted private all the way up to the General of the Army. Each soldier reports to a higher-ranking soldier, and each rank has its own group of functions and responsibilities, much like the layers of the Cisco hierarchical model.

The term *hierarchy* as it pertains to this model is the classification of a group of functions or responsibilities into a logical layer where each layer is subordinate to the layer above it in the hierarchy. This model is most effective when you plan to implement a small- to moderate-sized network.

EXAM ALERT

Remember that logical rather than physical layers also comprise the OSI and TCP/IP models. A single device may operate at more than one layer of the model, or more than one device may operate at a single layer.

The following sections start from the bottom and work up through the ranks to the top of the hierarchy. First though, take a look Figure 1.7 for an example of the Cisco hierarchical model in its entirety.

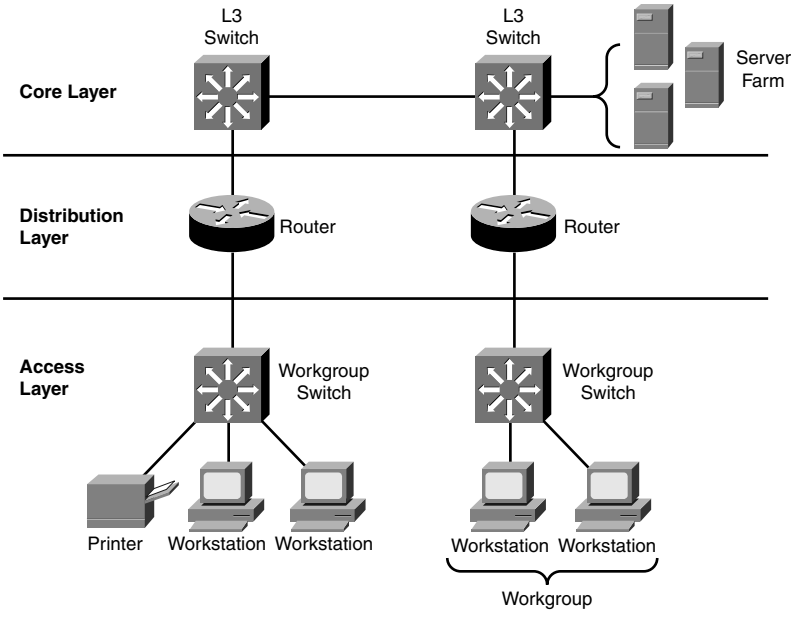


FIGURE 1.7 Cisco hierarchical model.

Access Layer

End users are connected at the Access layer; therefore, this layer may also be referred to as the *desktop* layer. These end users may also be combined to form a workgroup. Virtual LAN (VLAN) workgroups are defined by virtual access lists or filter lists at the Access layer to allow

for a continuation of the policies implemented at the Distribution layer. This functionality further controls internetwork resource access granted to each end user or workgroup. Users may access locally available resources at this level or they may be directed to the Distribution layer to access remotely available resources.

EXAM ALERT

Chapter 9, "Virtual LANs," discusses Virtual LANs in depth. Configuring and troubleshooting VLANs are both CCNA exam topics.

Distribution Layer

In the hierarchy, the Distribution layer is the middle man between the access and core layers. You may also hear this layer called the *workgroup* layer. Although the Distribution layer acts as a gathering point for the Access layer devices, it also uses a router or Layer 3 switch whenever necessary to determine how to traverse packets to the core layer.

You achieve traffic control at this layer by using various policies that ultimately provide network management and security.

Primary functions of the Distribution layer include the following:

- Routing (best path determination)
- Routing between VLANs
- Filtering—Access lists provide packet filtering, Quality of Service (QoS), network address translation (NAT), and route filtering
- Accessing WAN
- Defining broadcast and multicast domains
- Translating between different types of media (for example, ethernet and token ring)

EXAM ALERT

Design and implementation of access lists are CCNA exam topics. Given their importance, Chapter 13, "Access Lists," is devoted to access lists. Also, Chapter 5, "Introduction to Cisco Routers and Switches," reviews Cisco routers and switches that may be used at the Distribution layer. The 2600 series Cisco routers and 4000 series Cisco switches are included in that chapter.

Core Layer

The Core layer is the foundation or backbone of the network. Much like a building would falter without its foundation, a network would fall apart without the structure provided by the

core layer. As mentioned before, the Distribution layer manages access to the core. This enables the core to focus on speed and reliability. The goal is to provide high-speed switching as quickly and efficiently as possible. Any latency or delay can affect everyone on that network. Because speed is of the essence, the policies implemented at the Distribution layer (for example, filtering, access lists, and so on) should not occur at the Core layer.

Redundancy and fault tolerance are also important to the successful design of a core. If a network is set up with full redundancy, any failures should be transparent to the end user, which is the definition of a fault tolerant network.

NOTE

You might see Enterprise servers (server farms) connected to the core. Devices used at the core layer may include the Catalyst 6500 series switch or the 7000 series routers. These devices also are reviewed in Chapter 5.

If you were tasked with the design of a new network, would you select a Layer 2 core or a Layer 3 core? Although the Layer 2 core consists of a switched hierarchical setup, a Layer 3 core consists of a routed hierarchical setup.

The answer depends upon the individual requirements of the company in question. If the primary requirement is speed, perhaps a Layer 2 core is appropriate. If a stated desire is the additional network control that is available with a routed solution, then a Layer 3 core would fit the bill.

EXAM ALERT

Remember that routers segment broadcast domains (Layer 3 core) while switches segment collision domains (Layer 2 core).

Challenge

This chapter discusses three different layered models, including the Cisco 3-Layer Hierarchical model. To enhance your understanding of network communications with a layered architecture, please list each layer of the hierarchical model in the correct order and also list its primary responsibilities.

Layer Name	Layer Responsibilities

Although the hierarchical model is typically mentioned in published reviews for the CCNA examination, Cisco also created the Enterprise Composite Network Model (ECNM) for larger-scale network implementations. The ECNM is often mentioned in reviews for the Cisco Certified Design Associate (CCDA) exam and is covered in Appendix A, "Future Exam Topics," of this book.

The hierarchical model can assist in the implementation of a small- to moderate-sized network. The composite model goes a step further and provides a guide for creating a larger network. Because Cisco has a group of topics listed as "Planning and Designing," it is important to have a general knowledge of their models for network design.

Chapter Summary

The term *internetworking* signifies the industry, products, and processes that are required to handle the challenges of interconnecting networks. Various internetworks can be used, depending on the user's specific needs. For example, a LAN is a small network that is confined to a local geographical area. A LAN can connect to another LAN via a switch, bridge, or repeater. If a LAN attempts to connect to a MAN or WAN, it needs to interconnect via a router. WANs are much larger in scope. WANs are good for a company that has offices in multiple cities around the country. LAN and WAN technology are discussed in greater detail in later chapters of this book.

This chapter also discusses the importance of layered reference models such as the OSI model, TCP/IP model, and the Cisco 3-Layer Hierarchical model. The OSI model is important to discussions of internetworking because the terminology related to each layer has endured the test of time. Seven layers essentially map out the transmission of data from one end-user system to another. Multiple protocols relate to the interoperation of each layer. Special focus is placed on the Application layer protocols and their primary functions.

The TCP/IP model is implemented in a large portion of the networks that are set up today. The model is a condensed version of the OSI model with four related layers. The two most important protocols discussed in the TCP/IP suite for this first chapter are TCP and UDP. TCP is a connection-oriented protocol that provides for reliable data transport. UDP is a connectionless protocol that is considered unreliable. There are advantages and disadvantages to each protocol. Although TCP is reliable, it also costs more to implement on a network.

Overall, this chapter was designed to provide a general overview of standard internetworks and the layered architecture that was designed to represent network interactions. Now that you have gone over all of the internetworking models that are relevant to the exam, you are ready to move on to Chapter 2 and review the concepts related to networking at the Physical layer.

Key Terms

- internetwork
- LAN
- MAN
- WAN
- SAN
- VPN
- OSI model
- Application layer
- Telnet
- HTTP
- HTTPS
- FTP
- TFTP
- DNS
- SMTP
- POP3
- NFS
- NNTP
- SNMP
- NTP
- DHCP
- Presentation layer
- Session layer
- NFS

- SQL
- RPC
- ASP
- X Window
- DNA SCP
- Transport layer
- segment
- acknowledgment
- sequencing
- flow control
- buffers
- Network layer
- packet
- datagram
- data packets
- route update packets
- Data Link layer
- broadcast domain
- collision domain
- CSMA/CD
- grame
- MAC
- MAC address
- LLC
- ridge
- dwitch
- Physical layer
- hub
- repeater
- bit
- DCE
- DTE
- CSU/DSU
- encapsulation
- PDU
- TCP/IP model
- TCP/IP
- TCP
- PAR
- windowing
- UDP
- IP
- ICMP
- ARP
- RARP
- proxy ARP
- Cisco 3-Layer Hierarchical model
- VLAN
- routing
- filtering
- packet filtering
- route filtering
- QoS
- NAT

Apply Your Knowledge

Exercises

1.1 OSI Layered Model Identification

This has been mentioned throughout the chapter, but it is extremely important for the CCNA exam to know the seven layers of the OSI model and their general functions. If you have not decided on a mnemonic device that you like, you may want to take another look because most people find them to be very helpful with this type of exercise.

Estimated Time: 10 minutes

List the name of the appropriate layer next to the number listed and then identify two primary functions of that layer. Refer to Table 1.7 to check your responses.

1. _____Layer

   Functions: _____

2. _____Layer

   Functions: _____

3. _____Layer

   Functions: _____

4. _____Layer

   Functions: _____

5. _____Layer

   Functions: _____

6. _____Layer

   Functions: _____

7. _____Layer

   Functions: _____

Review Questions

1. Briefly list the communication application protocols that are used at the Application layer of the OSI model and what service they provide.
2. Describe how information is passed through the layers of the OSI model.
3. Define Positive Acknowledgments and Retransmission (PAR).
4. Describe the steps involved in a three-way handshake.
5. List the differences between TCP and UDP.
6. List the key functionalities of the Access layer of the Cisco hierarchical model.
7. List the key functionalities of the Distribution layer of the Cisco hierarchical model.
8. List the key functionalities of the Core layer of the Cisco hierarchical model.

Exam Questions

1. What information can DHCP provide to clients? (Choose the 3 best answers.)

- ❍ **A.** Clock information
- ❍ **B.** IP information
- ❍ **C.** DNS information
- ❍ **D.** Gateway information

2. Which of the protocols are used by email? (Choose the 2 best answers.)

- ❍ **A.** POP3
- ❍ **B.** SMTP
- ❍ **C.** SNMP
- ❍ **D.** DHCP

3. What takes place when a collision occurs on an ethernet network? (Choose the 3 best answers.)

- ❍ **A.** Every device stops transmitting for a short time.
- ❍ **B.** A jam signal is sent to notify devices of a collision.
- ❍ **C.** A collision signal is sent to notify devices of a collision.
- ❍ **D.** A random back-off algorithm starts.

4. What is the OUI of the MAC address 01:AB:4D:F2:89:10?

- ❍ **A.** 01
- ❍ **B.** F2:89:10
- ❍ **C.** 01:AB
- ❍ **D.** 01:AB:4D

5. A MAC address is… (Choose the 2 best answers.)

- ❍ **A.** A unique hardware address in a broadcast domain
- ❍ **B.** A unique IP address in a broadcast domain
- ❍ **C.** Provided by the manufacturer of the NIC
- ❍ **D.** Configured manually by the network administrator

6. At what layer of the OSI model do you find MAC addresses?

- ❍ **A.** Transport
- ❍ **B.** Network
- ❍ **C.** Data Link
- ❍ **D.** Physical

7. At what layer of the OSI model do you find sequence numbers?

- ❍ **A.** Application
- ❍ **B.** Presentation
- ❍ **C.** Session
- ❍ **D.** Transport

8. At what layer of the OSI model do you find IP addresses?

- ❍ **A.** Transport
- ❍ **B.** Network
- ❍ **C.** Data Link
- ❍ **D.** Physical

9. What kind of PDU is used at the Data Link layer of the OSI model?

- ❍ **A.** Bit
- ❍ **B.** Segment
- ❍ **C.** Packet/Datagram
- ❍ **D.** Frame

10. What kind of PDU is used at the Network layer of the OSI model?

- ❍ **A.** Segment
- ❍ **B.** Packet/Datagram
- ❍ **C.** Bit
- ❍ **D.** Frame

11. What kind of PDU is used at the Transport layer of the OSI model?

- ❍ **A.** Segment
- ❍ **B.** Data
- ❍ **C.** Frame
- ❍ **D.** Bit

12. What is the correct order for data encapsulation?

- ❍ **A.** Segment, packet, frame, data, bit
- ❍ **B.** Data, segment, packet, frame, bit
- ❍ **C.** Bit, frame, packet, segment, data
- ❍ **D.** Data, packet, segment, frame, bit

13. Routers look at the _____ when making a routing decision.

- ❍ **A.** Destination IP address
- ❍ **B.** Source IP address
- ❍ **C.** Destination MAC address
- ❍ **D.** Source MAC address

14. What protocol is assigned to port numbers 20 and 21?

- ❍ **A.** DNS
- ❍ **B.** Telnet
- ❍ **C.** FTP
- ❍ **D.** SMTP

15. What protocol is assigned to port number 80?

- ❍ **A.** SNMP
- ❍ **B.** HTTP
- ❍ **C.** POP3
- ❍ **D.** DHCP

16. Which of the following are TCP? (Choose the 2 best answers.)

- ❍ **A.** Telnet
- ❍ **B.** HTTP
- ❍ **C.** TFTP
- ❍ **D.** NTP

17. Which of the following are UDP? (Choose the 2 best answers.)

- ❍ **A.** DHCP
- ❍ **B.** SMTP
- ❍ **C.** SNMP
- ❍ **D.** POP3

18. What commands use ICMP? (Choose the 2 best answers.)

- ❍ **A.** Show cdp neighbor
- ❍ **B.** traceroute
- ❍ **C.** Telnet
- ❍ **D.** ping

19. What protocol maps a known MAC address to an IP address?

- ❍ **A.** RARP
- ❍ **B.** ARP
- ❍ **C.** ICMP
- ❍ **D.** Proxy ARP

20. What TCP/IP protocol provides terminal emulation to a remote host?

- ❍ **A.** HTTP
- ❍ **B.** VPN
- ❍ **C.** Telnet
- ❍ **D.** SNMP

Answers to Review Questions

1. The following is a list of the protocols utilized at the Application layer of the OSI model and the functionality of each protocol.
   - **Telnet**—Terminal emulation to a remote host
   - **HTTP**—Web-browsing service
   - **HTTPS**—Secure web browsing
   - **FTP**—File transfer
   - **TFTP**—Bare-bones file transfer
   - **DNS**—Name management
   - **SMTP**—Send emails
   - **POP3**—Receive emails
   - **NFS**—File sharing
   - **NNTP**—Usenet newsgroups
   - **SNMP**—Network management
   - **NTP**—Time management
   - **DHCP**—Dynamic host configuration

2. The upper layers (Application, Presentation, and Session) pass data to the Transport layer. The Transport layer encapsulates the data into a segment that is handed down to the Network layer. The Network layer encapsulates the segment into a packet (or datagram) to be handed down to the Data Link layer. The Data Link layer encapsulates the packet (or datagram) into a frame and sends it to the Physical layer. The Physical layer then encapsulates the frame into a bit to be sent over the network.

3. Used by TCP, PAR is the process by which the source device begins a timer when a segment is sent and retransmits if the timer runs out before an acknowledgment is received. The source device keeps track of segments that are sent and requires an acknowledgment for each segment. The destination device acknowledges when a segment is received by sending a packet to the source that iterates the next sequence number for which it is looking from the source.

4. First, a connection agreement segment is sent to the recipient asking to synchronize systems. Second, a second and third segment acknowledge the request to connect and determine the rules of engagement. Sequencing synchronization is requested of the receiving device. A two-way connection is established. Third, a final segment is sent as an acknowledgment that the rules have been accepted and a connection has been formed.

5. The following table lists comparisons of the key characteristics of the TCP and UDP protocols.

TCP	UDP
Uses sequenced data transmissions	Does not use sequenced data transmissions
Reliable protocol	Unreliable protocol
Connection-oriented	Connectionless
Expensive to implement	Inexpensive to implement
Sends acknowledgments	Does not send acknowledgments
Uses windowing flow control	Does not use windowing or flow control

6. The following list includes the key functionalities of the Access layer of the Cisco hierarchical model:

   - Desktop layer
   - End-user connectivity
   - Virtual LAN (VLAN) workgroup definition
   - Continuation of the policies implemented at the distribution layer by using virtual access lists or filter lists
   - User access to locally available resources

7. The following list includes the key functionalities of the Distribution layer of the Cisco hierarchical model:

   - Control layer
   - Middleman between the access and core layers
   - Acts as an aggregation point for access layer devices
   - Determines how and when to traverse packets to the core layer
   - Policy implementation
   - Network security
   - Routing (best path determination)
   - Routing between VLANs
   - Filtering
   - Access lists
   - Packet filtering
   - Quality of Service (QoS)
   - Network address translation (NAT)

- Route filtering
- WAN access
- Defines broadcast and multicast domains
- Translates between different types of media (i.e. ethernet and token ring)

8. The following list includes the key functionalities of the Core layer of the Cisco hierarchical model:
   - Backbone layer
   - The Distribution layer manages access to the core.
   - High-speed switching
   - Reliability
   - Redundancy
   - Fault tolerance
   - Low latency
   - Enterprise servers (server farms)

Answers to Exam Questions

1. **B, C, D.** DHCP works dynamically to provide IP address, DNS, and default gateway information. Answer A is incorrect because the Network Time Protocol (NTP) provides clock information.
2. **A, B.** POP3 receives email on an Internet server and SMTP sends email across a network. Answer C is incorrect because SNMP is a network management protocol and answer D is incorrect because DHCP is the dynamic host configuration protocol.
3. **A, B, D.** When a collision occurs on an ethernet network a jam signal is sent to notify devices of a collision and a random back-off algorithm starts while every device stops transmitting for a short time. Answer C is incorrect because a jam signal is sent rather than a collision signal.
4. **D.** The OUI of a MAC address is the organizationally unique identifier that is assigned by the manufacturer of the network interface card (NIC). The OUI consists of the first 6 hexadecimal digits. Answer A is incorrect because it only consists of 2 hexadecimal digits. Answer B is incorrect because it is not the first 6 hexadecimal digits of the MAC address 01:AB:4D:F2:89:10. Answer C is incorrect because it only consists of 4 hexadecimal digits.
5. **A, C.** The MAC address is a unique hardware address in the broadcast domain and the manufacturer of the NIC provides MAC addresses. Answer B is incorrect because IP addresses are logical addresses used by the Network layer. Answer D is incorrect because a MAC address is not configured manually by a network administrator.

6. **C.** MAC addresses are found at the Data Link layer of the OSI model. Answers A, B, and D are incorrect because MAC addresses are not found at the Transport, Network, or Physical layer of the OSI model.

7. **D.** The Transport layer uses sequence numbers. Data segments are sequenced into their original order when they arrive at the destination. Answers A, B, and C are incorrect because sequence numbers are not found at the Application, Presentation, or Session layer of the OSI model.

8. **B.** Answer B is correct because IP addresses are found at the Network layer of the OSI model. IP addresses are logical or virtual addresses that are assigned at Layer 3 to identify the destination of a packet or datagram. Answers A, C, and D are incorrect because IP addresses are not found at the Transport, Data Link, or Physical layer of the OSI model.

9. **D.** The Data Link layer uses frame PDUs to encapsulate data. Answers A, B, and C are incorrect because segments are used at the Transport layer, whereas packet/datagrams are used at the Network layer and bits are used by the Physical layer of the OSI model.

10. **B.** The Network layer of the OSI model uses packets/datagrams. Answers A, C, and D are incorrect because the Application, Presentation, and Session layers of the OSI model transmit data.

11. **A.** Segments are used at the Transport layer of the OSI model. Answer B is incorrect because the three upper layers of the OSI model transmit data. Answer C is incorrect because the Data Link layer transmits frames, and answer D is incorrect because the Physical layer transmits bits.

12. **B.** Encapsulation occurs from the Application layer and then is passed down through the lower layers of the OSI model. The PDUs are sent by the Application layer as data and then they are encapsulated with a segment at the Transport layer. At the Network layer the segment is encapsulated into a packet/datagram that is passed down to the Data Link layer, which encapsulates a frame and hands it off to the Physical layer, which uses bits.

13. **A.** Routers look at the destination IP address to determine where to forward the packet. Answers B, C, and D are incorrect because a router does not examine the source IP address, destination MAC address, or source MAC address to make forwarding decisions.

14. **C.** FTP is assigned to port numbers 20 and 21. Answers A, B, and D are incorrect because Telnet is assigned port number 23, DNS is assigned port number 53, and SMTP is assigned port number 25.

15. **B.** HTTP is assigned port number 80. Answers A, C, and D are incorrect because SNMP is assigned port number 161, POP3 is port number 110, and DHCP is assigned ports 67 and 68.

16. **A, B.** Telnet and HTTP are both protocols that use TCP. Answers C and D are incorrect because TFTP and NTP use UDP.

17. **A, C.** DHCP and SNMP use UDP, whereas answers B and D are incorrect because SMTP and POP3 use TCP.

18. **B, D.** Traceroute and ping are both commands that use ICMP. Traceroute traces the route or path taken from a client to a remote host. Ping enables you to validate that an IP address exists and can accept requests. Answers A and C are incorrect because neither `show cdp neighbor` nor Telnet use ICMP.

19. **A.** RARP maps MAC addresses to an IP address, whereas answer B is incorrect because ARP maps an IP address to a MAC address. Answer C is incorrect because ICMP sends messages across the network via ping, and traceroute enables a router to respond to an ARP request that has been sent to a remote host. Answer D is also incorrect because some Unix machines (especially Solaris) rely on Proxy ARP rather than default gateways.

20. **C.** Telnet provides for terminal emulation to a remote host. Answers A, B, and D are incorrect because HTTP is a web-browsing application, VPN is a private network that can access public networks remotely, and SNMP is a network management application.

Suggested Readings and Resources

The following are some recommended readings on the subject of standard internetworking models:

1. "Open Systems Interconnection Protocols," http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/osi_prot.htm.
2. "OSI Model," http://en.wikipedia.org/wiki/OSI_model.
3. "TCP/IP Overview," http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/osi_prot.htm.
4. "TechEncyclopedia," www.techweb.com/encyclopedia.

CHAPTER 2

Physical Layer Networking Concepts

Objectives

This chapter covers the following Cisco-specified objective for the "Planning and Designing" section of the CCNA exam:

Design a simple LAN using Cisco technology

- Various network designs or layouts are commonly used to set up a LAN. To pass the CCNA exam, you need to familiarize yourself with four prevalent network topologies. Chapter 5, "Introduction to Cisco Routers and Switches," reviews specific Cisco devices that can be used as part of a new LAN network implementation.

Outline

Study Strategies

- Identify the four physical network topologies discussed in this chapter.
- Know the different types of network cables and the characteristics that differentiate them from one another.
- Review the wireless technology standards.
- Be able to identify devices that are used at the Physical layer.

Introduction

Chapter 1, "Standard Internetworking Models," went over the layers of the OSI and TCP/IP models. This chapter goes into more detail regarding the Physical layer. Remember that electrical, mechanical, procedural, and functional requirements are defined at this layer. Such requirements provide assistance with the activation, maintenance, and deactivation of physical connectivity between devices.

Concepts covered include the topologies, cabling, and devices that are relevant at the physical level and important to understand when studying for the CCNA exam. Also, because wireless communications are constantly evolving and are flourishing in today's marketplace, several significant wireless technologies are covered as well.

Network Topologies

Objective:

Design a simple LAN, using Cisco technology

Topology can be defined as either the physical or logical layout of a network. Typically, a physical topology is documented with a network diagram, such as a Visio diagram. Diagrams can prove to be extremely helpful when troubleshooting a network issue. Most companies keep a database with copies of their entire network as well as individual site connections. If you work in a sales capacity, diagrams are drawn up to plan out the network setup and to ensure that all bases are covered to meet customer expectations.

Just as you might imagine, a physical topology consists of the cables, workstations, and other peripheral devices that comprise the network. A logical topology refers to how the network actually communicates. This may differ from the physical topology; therefore, this section covers the four most common physical network topologies and what the associated logical network topology is for the physical star network.

The Bus Topology

A *bus network* topology may also be referred to as a *linear bus* topology. This topology is set up so that the network nodes are connected via a single cable (also referred to as a *trunk* or a *backbone*). Electrical signals are sent from one end of the cable to the other. When this occurs, all connected devices receive that electrical signal transmission. Network devices are connected directly to the trunk with a T connector. Both ends of the trunk use a terminator to stop the electrical signal from echoing back down the cable. Figure 2.1 represents a physical bus topology.

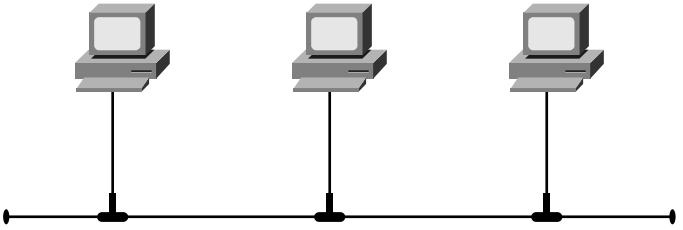


FIGURE 2.1 Example of a physical bus topology.

Because the bus topology uses a single cable, it is a low-cost option that is easily implemented. The downside to this setup is the lack of redundancy. If the cable breaks, the entire network goes down.

The Ring Topology

A *ring network* topology is set up so that one device is directly connected to two other devices on the same network. When a device emits a data signal transmission, the transmission is sent in a single direction to the next connected device. The transmission continues to pass along each device successively until it arrives back at the original transmitting device. This method creates a ring or a loop. Figure 2.2 shows an example of a physical ring topology.

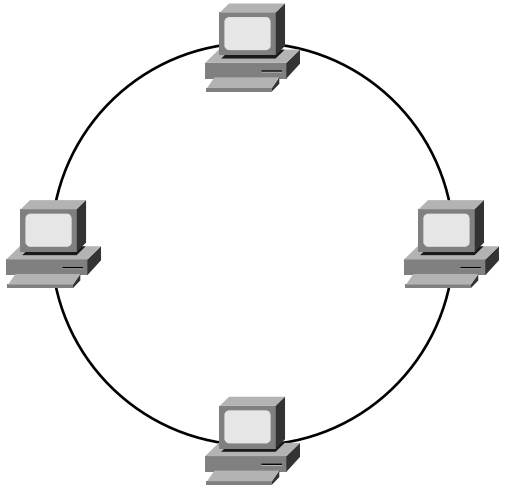


FIGURE 2.2 Example of a physical ring topology.

With this topology, a single ring configuration lacks a failover solution. If there is a break anywhere on the ring, it brings down the entire network. This was the same situation with the bus network topology. For this reason, you may also configure a dual ring topology. If there is a failure on one physical ring, the other physical ring passes data transmissions to ensure network operability. Figure 2.3 shows an example of a physical dual ring network topology.

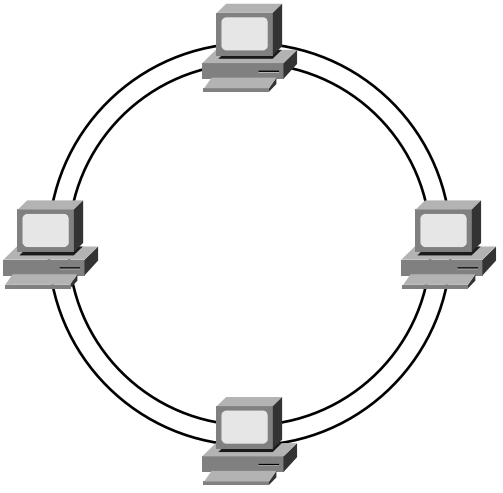


FIGURE 2.3 Example of a physical dual ring topology.

The Star Topology

The *star network* topology is the most commonly implemented network design. With this topology, there is a central device with separate connections to each end node. Each connection uses a separate cable, which adds to the cost of implementation. When hubs are used in a star topology, a logical bus is created. This type of network star is called a hub-and-spoke topology. Figure 2.4 shows an example of a physical star topology.

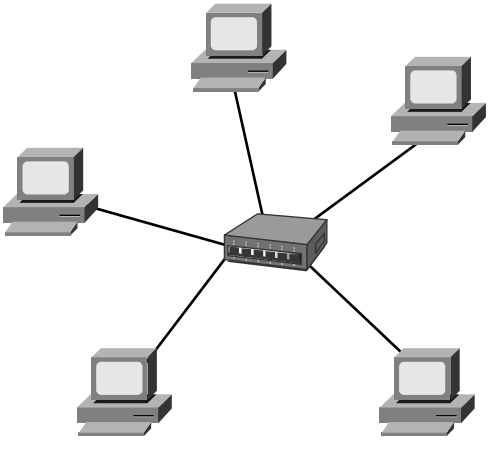


FIGURE 2.4 Example of a physical star topology.

NOTE

Although the star topology is a physical star, it also can be referred to as a logical bus topology because hubs are used to control communication.

Because there are separate connections between end nodes and the central device, this topology enables the network administrator to add or remove end nodes without affecting service to all other nodes on that network. This is also possible with the token ring topology, which enables you to add multistation access units (MAUs) to the network without disrupting service. The same cannot be said for the physical bus network topologies.

The Mesh Topology

The full mesh network topology is set up so that each device is directly connected to every other device on the network. This connection method has built-in redundancy. If one link goes down, the device transmits via another link. Figure 2.5 shows an example of a physical full mesh topology.

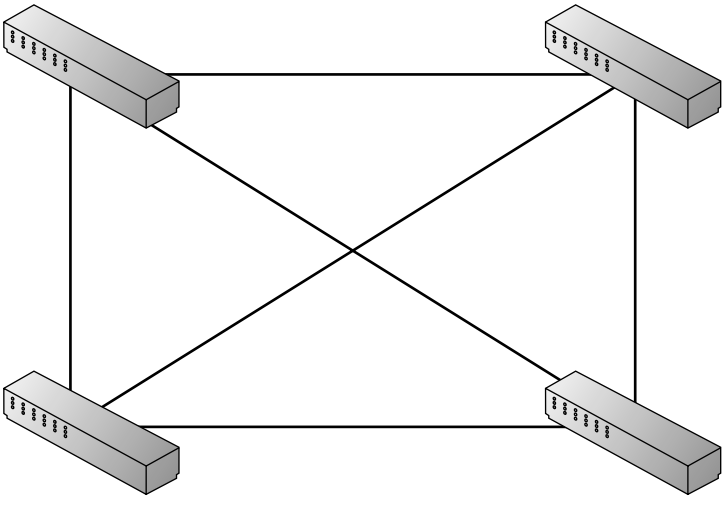


FIGURE 2.5 Example of a mesh topology.

A partial mesh network topology has direct connectivity between some of the network devices, but not all of them, as the full mesh topology does. Figure 2.6 shows an example of a physical partial mesh topology.

Overall, mesh topologies are much more expensive to implement. However, the cost may be acceptable given the reliability of this design.

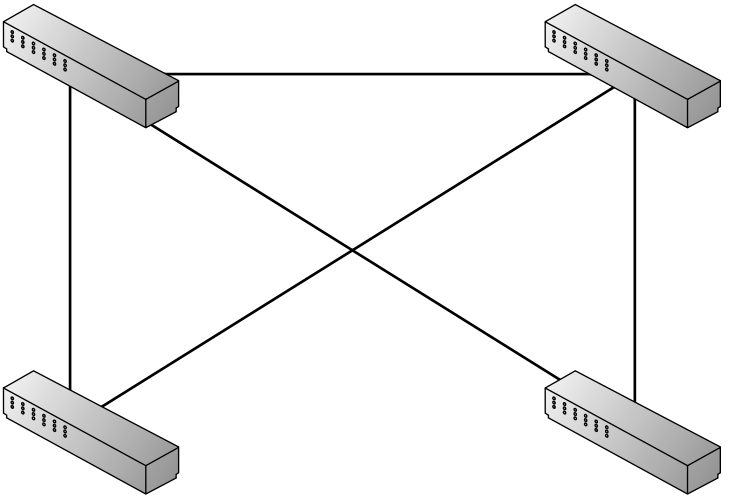


FIGURE 2.6 Example of a partial mesh topology.

Cabling

This section reviews the types of media or cable that are used for LAN connectivity. The primary media types include coaxial, twisted-pair, and fiber-optic cables. Cable media offer physical connectivity to network devices. Cables may consist of metal, glass, or plastic. Copper is the most popular metal cable. Fiber-optic uses glass or plastic cabling.

Before you look at each medium in greater detail, it's a good idea to discuss several important terms related to data transmission that are directly affected by what type of cable media is used on a network.

Review the following terminology:

- **Bandwidth**—The total amount of information that can traverse a communications medium, measured in bits per second. Measurement of bandwidth is helpful for network performance analysis. Also, availability is increasing but limited.

EXAM ALERT

For the exam, remember that bandwidth is used to analyze network performance and that although availability is increasing, it is also limited.

- **Attenuation**—Occurs over long distances as a signal loses strength.
- **Electromagnetic Interference (EMI)**—Interference or noise caused by electromagnetic signals, which can decrease data integrity.

- **Crosstalk**—An electrical or magnetic field originating from one communications signal that can affect the signal in a nearby circuit.
  - **Near-end Crosstalk (NEXT)**—Crosstalk measured at the transmitting end of a cable.
  - **Far-end Crosstalk (FEXT)**—Crosstalk measured at the far end of the cable from where the transmission was sent.

EXAM ALERT

Know the terms NEXT and FEXT and what they represent for the CCNA exam.

Coaxial Cable

Coaxial cables for data consist of a single copper wire surrounded by a plastic insulation cover and a braided copper shield. Primarily, two types of coaxial cables are used in conjunction with Ethernet LAN networks. They are called *thin* and *thick coax*.

Thin coax has the following characteristics:

- Also called thinnet
- .25 inches in diameter
- Maximum cable length = 185 meters
- Uses Bayonet Neill Concelman connectors (BNCs)
- 10BASE-2 ethernet standard

NOTE

The Institute for Electrical and Electronics Engineers (IEEE) ethernet standards are reviewed in Chapter 3, "Data Link Networking Concepts."

Thick coax has the following characteristics:

- Also called thicknet
- Maximum cable length = 500 meters
- Uses vampire taps (where the tap goes through the shield to touch the copper wire)
- Uses attachment unit interface (AUI) adapters
- 10BASE-5 ethernet standard

The coaxial cable media is not nearly as popular as twisted pair or fiber optic. It is not as flexible or cost effective as other options. You may see this cable implemented on an older network.

Twisted-Pair Cable

Just as the name indicates, twisted-pair cables twist two wires together to form a pair. This solution helps to reduce interference and attenuation. There are two types of twisted-pair cabling defined by the Telecommunications Information Association (TIA). Those types are unshielded twisted pair (UTP) and shielded twisted pair (STP). UTP is the more common and cost-effective solution. STP has an additional shield, which provides additional reduction of interference and attenuation, but also makes it the more expensive solution. For the exam, UTP is reviewed in greater detail.

UTP key characteristics include the following:

- Eight color-coded wires
- Four pairs
- Uses an RJ-45 connector
- Vulnerable to EMI
- Maximum, practical length is 100 meters
- 10BASE-T, 100BaseT, and 1000BaseT ethernet standards

TIP

When reviewing for the exam, note that UTP is vulnerable to EMI and uses an RJ-45 connector.

EXAM ALERT

Because attenuation causes a signal to lose strength as the length of a cable increases, the maximum, practical length of a UTP cable is 100 meters.

UTP can be broken down into six more categories. You may have heard someone talk about a Cat5 cable. They are referring to a Category 5 UTP cable. Each category has different characteristics:

- **Category 1**—Telephone cable that is not used for data transmission.
- **Category 2**—Data cable that can handle speeds up to 4Mbps. This is no longer fast enough for networks today.

- **Category 3**—Data cable that can handle speeds up to 10Mbps. It is faster than the Cat2 cable, and this was quite popular until network speeds surpassed the 10Mbps threshold.
- **Category 4**—Data cable that can handle speeds up to 16Mbps. Meant to be used with token ring.
- **Category 5**—Data cable that can handle speeds up to 100Mbps. This is currently the most popular cable selection.
- **Category 5e**—Data cable that can handle speeds up to 1Gbps. This is a popular choice for Gigabit Ethernet networks.
- **Category 6**—This cable was created to exceed speeds of 1Gbps.

It is also important to know the pinouts for twisted-pair cables. The term *pinout* is used in the electronic industry to describe the purpose of each pin in a connector. When choosing your cable, you need to know which pinout is appropriate to connect the devices on your network. The following sections cover the straight-through and cross-over cables.

Straight-Through Cable

Straight-through cables use four wires and pins 1, 2, 3, and 6. Given those pins, pin 1 is connected on one end of the cable to pin 1 on the opposite end of the cable. Pin 2 at one end is connected to pin 2 on the far end, and so on. Figure 2.7 shows an example of a straight-through cable pinout.

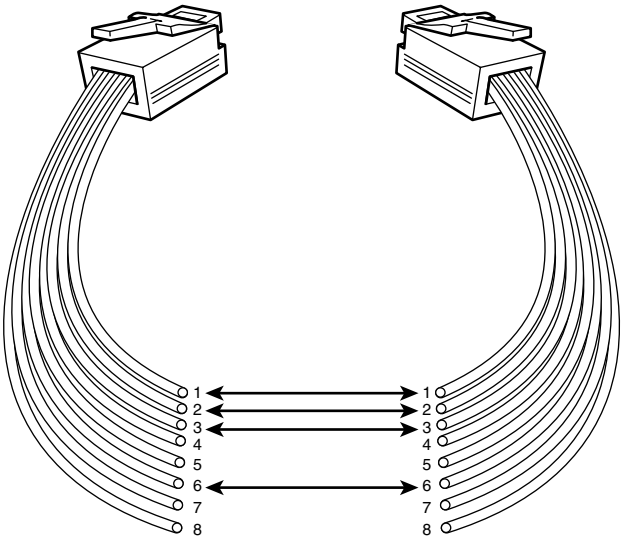


FIGURE 2.7 Example of a straight-through cable pinout.

These cables are meant only for interface to interface connections on ethernet networks, so you cannot use them with token ring, ISDN, and so on.

Use a straight-through cable for the following connection types:

- From a PC to a switch or a hub
- From a router to a switch or a hub

TIP

For the CCNA exam, you need to know which devices can be connected with a straight-through cable. Remember that straight-through cables are used to connect unlike device interfaces. Different devices = straight-through cable.

Cross-Over Cable

Cross-over cables also use four wires and pins 1, 2, 3, and 6. The difference is in how the pins are connected at each end. With cross-over cables, pin 1 connects to pin 3 and pin 2 connects to pin 6. Figure 2.8 shows an example of a cross-over cable pinout.

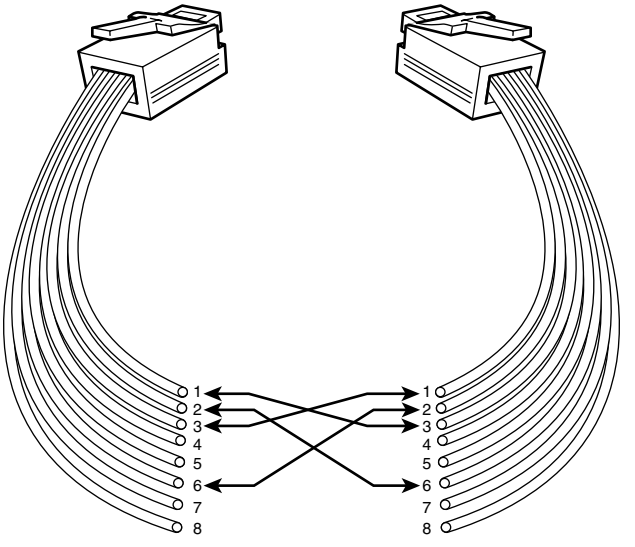


FIGURE 2.8 Example of a cross-over cable pinout.

Use a cross-over cable for the following connection types:

- From a switch to another switch
- From a router to another router
- From a PC to another PC

- From a PC to a router
- From a hub to another hub
- From a hub to a switch

TIP

For the CCNA exam, you need to know which devices can be connected with a cross-over cable. Remember that for the most part cross-over cables are used to connect similar device interfaces.

Rolled Cable

Rolled or rollover cables use eight wires and connect from a host to a console serial communications (com) port on a router. You may also hear this cable referred to as a *console cable*. Make sure not to confuse a rollover cable with a cross-over cable for the CCNA exam.

Challenge

Knowing the type of twisted-pair cable that is used to connect one device to another is an important networking concept. If you use the wrong cable, you will not have a working connection. So in this challenge I give you various connectivity scenarios and you must decide whether you should use a straight-through or cross-over cable between the devices.

Connecting a…	Type of Cable
Switch to a switch	
Hub to a switch	
PC to a switch or hub	
PC to a PC	
Hub to a hub	
Router to a router	
PC to a router	
Router to a switch or hub	

Fiber-Optic Cable

Fiber-optic cables use light rather than electric signals to send data transmissions. These optical light signals travel a fiberglass core and you may hear this technology referred to as *fiber optics* or *optical cabling*.

Two categories of fiber-optic cabling are

- *Multimode (MM)*—This is generally used for shorter distances and is ideal for a campus-sized network. MM also has a larger diameter of optical fiber than SM fiber.
- *Single-mode (SM)*—This mode is used to span longer distances. SM also allows for a higher data rate than MM and faster data transmission speeds.

Fiber-optic cables may use a subscriber connector (SC), straight tip (ST), or MegaTransfer-Registered Jack (MT-RJ) connector. There are several Layer 2 ethernet protocols that can pass data over fiber-optic cables. Those Layer 2 ethernet standards are 10BASE-FL, 100Base FX, 1000BaseSX, 1000BaseLX, and 1000BaseZX.

All in all, fiber is the best choice for a secure connection over longer distances. Because fiber uses optical light signals for data transmission, it is not as easy to "eavesdrop" on communications as it is with copper cabling using electrical signals. Fiber is not susceptible to EMI and crosstalk, as coaxial and twisted-pair cables are. It also offers the highest maximum speed of the different cable types. You may have already guessed, but fiber is also the most expensive option.

TIP

Fiber-optic cables are not susceptible to EMI.

TIP

On the CCNA exam, you may see the terms *Main Distribution Frame (MDF)* and an *Intermediate Distribution Frame (IDF)*. A distribution frame is a physical rack that allows for the termination and interconnection of cables. This process creates network cross-connects. With that in mind, the MDF provides a point of interconnection between external telecommunications cabling and internal cabling in a facility. The IDF is the point of interconnection for cabling between the MDF and end-user devices.

Wireless

Wireless technology uses radio transmissions rather than data transmissions over copper wire or fiber-optic media. With wireless LANs (WLANs), a physical connection is no longer necessary. Electromagnetic energy, whose existence was proven way back in 1867, passes through the atmosphere in varied wavelengths. Different wavelengths are differentiated by their different names. Spread Spectrum WLANs determine how data traverses the Radio Frequency (RF) media. The most common applications for wireless technology are Wireless Fidelity, Infrared, and Bluetooth technologies.

TIP

Keep in mind that Spread Spectrum WLANs allow for high-speed transmissions over short distances. There are two types of spread spectrum radio: Direct Sequencing Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS).

Wireless Fidelity (Wi-Fi)

IEEE created the 802.11 designation as the standard for wireless networking. IEEE 802.11 may be further defined by three more specific standards: 802.11a, 802.11b, and 802.11g. The speed, distance, and features of 802.11 specifications are variable. The most common of these specifications is the 802.11b standard, which may also be referred to as Wireless Fidelity (Wi-Fi) or High Rate 802.11. IEEE 802.11b can allow for transmission speeds of up to 1–2Mbps. It also uses a Radio Frequency (RF) of 2.4GHz.

TIP

For the CCNA exam, remember that the 802.11b standard is also known as Wi-Fi or High Rate 802.11.

802.11 can also be broken down again into the following wireless standards:

- 802.11a
  - RF is 5GHz.
  - Speed up to 54Mbps.
  - Range of transmission is generally lower than that of 802.11g.
- 802.11b
  - RF is 2.4GHz.
  - Uses different channels to cover subfrequencies in the 2.4Ghz band.
  - Speed up to 11Mbps.
  - Range of transmission is generally greater than that of 802.11a and 802.11g.
- 802.11g
  - RF is 2.4GHz.
  - Speed up to 54Mbps.
  - Range of transmission is generally lower than that of 802.11b.

Based on these summarizations, you can see the similarities and differences of each standard. Please note that only 802.11a uses a different RF. This means that 802.11a is not compatible with either 802.11b or 802.11g.

Infrared

Infrared resides in a region of the electromagnetic spectrum just beyond the red end of our visible spectrum. Infrared wireless technology uses infrared beams to pass data across a network. Your television remote uses infrared technology to send requests to the television set. Speeds can reach a maximum of 16Mbps and signals are used for short-distance communications.

Infrared can eliminate the need for those pesky cables that connect your keyboard or mouse to your PC and cause clutter in your workspace. On the other hand, infrared may be easily refracted or reflected so it should not be used near windows or glass objects.

Bluetooth

Bluetooth technology utilizes a short-range wireless radio connection to enable various devices to interconnect. Such devices include cell phones, PCs, and Personal Digital Assistants (PDAs). The only requirement to establish connectivity is a 10-meter range (approximately 33 feet) between communicating devices. When in range, Bluetooth uses an RF link in the 2.4GHz range that has a 720Kbps per channel capacity to transfer voice or data. The Bluetooth specification also has two power levels defined; a lower power level that covers the shorter personal area within a room, and a higher power level that can cover a medium range like the range within a home.

Physical Layer Devices

The discussion so far of physical layer networking concepts has gone over the physical network topologies, cables, and wireless technology standards. Several network devices also are utilized at the Physical layer. Those include repeaters, hubs, and network interfaces.

Repeaters

Chapter 1, with its discussion of the Physical layer, mentioned that repeaters and hubs extend a network rather than segment a network. In fact, repeaters were introduced to increase or extend the distance between end nodes. A repeater consists of a transmitter and a receiver. When a signal is received by the repeater, it amplifies the signal and then retransmits. This effectively enables the signal to travel over a greater distance.

Please note that repeaters are an outdated technology. A separate device is no longer needed to perform this functionality. Both active hubs and switches can be used in place of a repeater.

Hubs

A *hub* can be defined as a multiple port repeater. A hub consists of 2 to 24 ports and may be called a *workgroup hub*. When data is received, the hub then retransmits that data out on all the other ports. Physical connectivity is achieved via a twisted-pair cable.

There are active and passive hubs. Active hubs have a separate power supply to assist with the gain of a signal before it is forwarded out all connected ports. *Gain* is an electrical term used to identify the ratio of signal output to signal input of a system. A power signal increased by a factor of 10 would indicate a gain of 10. Passive hubs do not regenerate the incoming signal.

Although they are very inexpensive, hubs may not be the best solution if you require a more efficient use of bandwidth and its distribution among ports. Traffic may become congested because of collisions on the network. Traffic is being forwarded out on all ports of a single collision domain. To decrease congestion, the network administrator might consider replacing the hub with a switch.

TIP

Know that a viable solution to decrease network congestion is replacing a hub with a switch. A switch creates a separate collision domain for each network segment.

Network Interfaces

A network interface provides connectivity from an end-user PC or laptop to the public network. Depending on the interface, you might see up to three light-emitting diodes (LEDs) that help to determine the connection's status. The link light LED should light up if you have connectivity. The activity light LED should flicker if there is activity on the line. There may also be a speed light LED that is used to verify the connection speed in a 10/100/1000Mbps network. Blinking lights and colors other than green can indicate error conditions that can be investigated by a technician.

Chapter Summary

Chapter 2 has taken the Physical layer and expanded the discussion to include physical network topologies and various network components. All these concepts are relevant when mapping out the design of a new network. Many of the topics in this chapter also touch upon ethernet technologies, which Chapter 3 continues to discuss, along with devices that are used at the Data Link layer.

Key Terms

- physical topology
- logical topology
- bus topology
- ring topology
- dual ring topology
- star topology
- full mesh topology
- partial mesh topology
- bandwidth
- attenuation
- EMI
- crosstalk
- NEXT
- FEXT
- coaxial cable
- twisted-pair cable
- unshielded twisted-pair cable
- shielded twisted-pair cable
- straight-through cable
- cross-over cable
- fiber-optic cable
- multimode
- single-mode
- wireless fidelity
- 802.11
- 802.11a
- 802.11b
- 802.11g
- infrared
- Bluetooth
- repeaters
- hubs
- network interface

Apply Your Knowledge

Exercises

2.1 UTP Cable Categories

Each category of UTP cabling has different characteristics. In this exercise, please list the characteristics of each category of UTP cable.

Estimated Time: 10 minutes

UTP Category	Characteristics
Category 1	
Category 2	
Category 3	
Category 4	
Category 5	
Category 6	

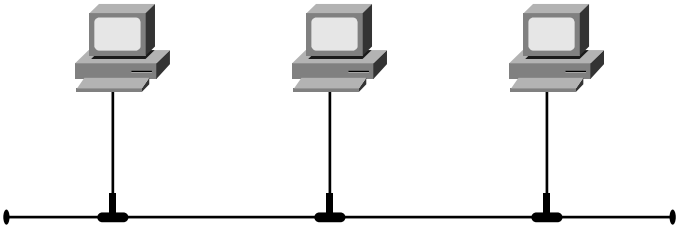
Review Questions

1. Draw out a simple physical bus topology.
2. Draw out a simple physical single ring and dual ring topology.
3. Draw out a simple physical star topology.
4. Draw out a simple physical partial mesh and full mesh topology.
5. Describe the pinout of a straight-through cable.
6. Describe the pinout of a cross-over cable.

Exam Questions

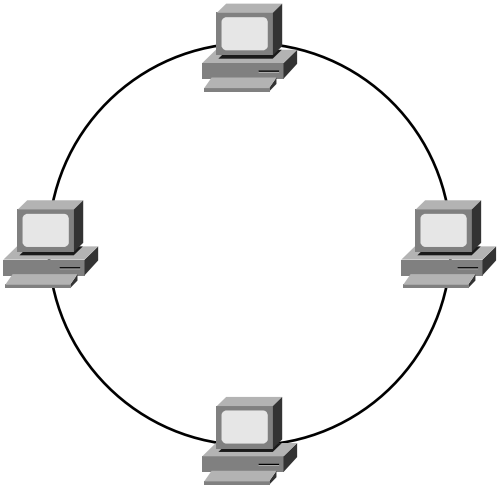
1. Which physical network topology is shown in the following diagram?

- ❍ **A.** Ring
- ❍ **B.** Bus
- ❍ **C.** Star
- ❍ **D.** Mesh



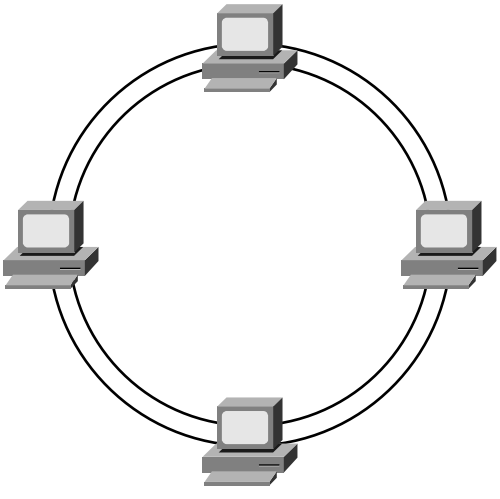
2. Which physical network topology is shown in the following diagram?

- ❍ **A.** Ring
- ❍ **B.** Bus
- ❍ **C.** Star
- ❍ **D.** Mesh



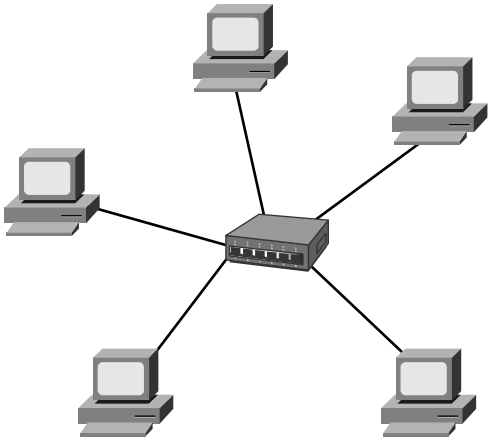
3. Which physical network topology is shown in the following diagram?

- ❍ **A.** Single ring
- ❍ **B.** Partial mesh
- ❍ **C.** Full mesh
- ❍ **D.** Dual ring



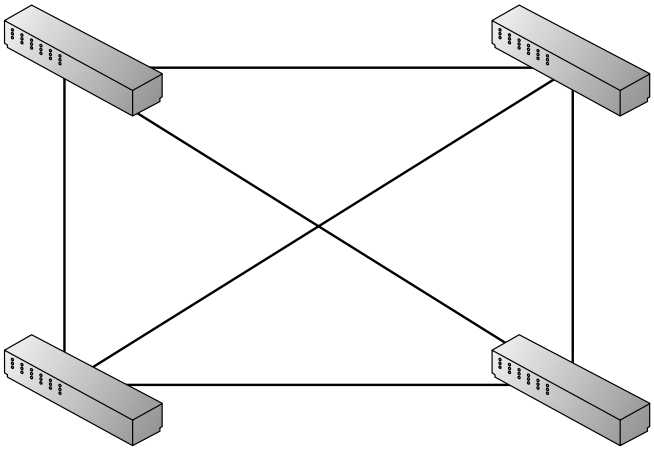
4. Which physical network topology is shown in the following diagram?

- ❍ **A.** Ring
- ❍ **B.** Bus
- ❍ **C.** Star
- ❍ **D.** Mesh



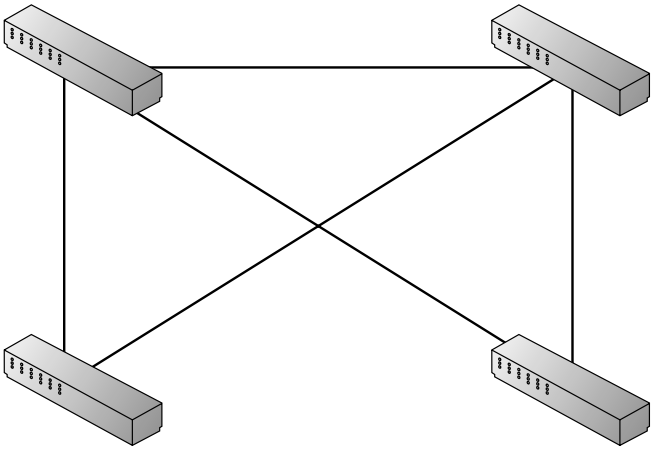
5. Which physical network topology is shown in the following diagram?

- ❍ **A.** Single ring
- ❍ **B.** Partial mesh
- ❍ **C.** Dual ring
- ❍ **D.** Full mesh



6. Which physical network topology is shown in the following diagram?

- ❍ **A.** Single ring
- ❍ **B.** Partial mesh
- ❍ **C.** Dual ring
- ❍ **D.** Full mesh



7. Which of the following is not susceptible to EMI?

- ❍ **A.** Fiber
- ❍ **B.** Thin coaxial cable
- ❍ **C.** Category 3 UTP cable
- ❍ **D.** Category 5 UTP cable

8. Which connector does a UTP cable use?

- ❍ **A.** MT-RJ
- ❍ **B.** SC
- ❍ **C.** ST
- ❍ **D.** RJ-45

9. Because of attenuation, the maximum, practical length of a UTP cable is _____.

- ❍ **A.** 10 meters
- ❍ **B.** 100 meters
- ❍ **C.** 200 meters
- ❍ **D.** 500 meters

10. The total flow of information over a certain time period on a communications medium measured in bits per second is called _____.

- ❍ **A.** Bandwidth
- ❍ **B.** Crosstalk
- ❍ **C.** Attenuation
- ❍ **D.** Electromagnetic interference

11. Which cable consists of a single copper wire surrounded by a plastic insulation cover and a braided copper shield?

- ❍ **A.** Coaxial cable
- ❍ **B.** UTP
- ❍ **C.** STP
- ❍ **D.** Category 5 cable

12. What type of UTP cable would you use to connect a switch to a router?

- ❍ **A.** Coaxial cable
- ❍ **B.** Straight-through cable
- ❍ **C.** Cross-over cable
- ❍ **D.** Thin coax

13. What type of UTP cable would you use to connect a PC directly to another PC?

- ❍ **A.** Coaxial cable
- ❍ **B.** Straight-through cable
- ❍ **C.** Cross-over cable
- ❍ **D.** Thick coax

14. If you have a network that is connected through a hub and experiencing congestion, which of the following is the best solution to decrease congestion on your network?

- ❍ **A.** Install a second hub.
- ❍ **B.** Replace the hub with a repeater.
- ❍ **C.** Replace the hub with a switch.
- ❍ **D.** Replace the hub with a network interface.

15. What is the IEEE standard for wi-fi?

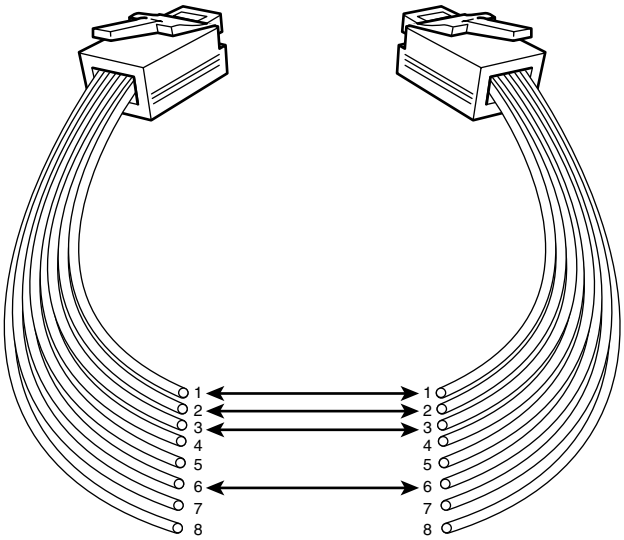
- ❍ **A.** 802.1q
- ❍ **B.** 802.11b
- ❍ **C.** 802.3u
- ❍ **D.** 802.3ab

16. Which IEEE wireless standard uses a 5GHz radio frequency and is not compatible with other wireless standards?

- ❍ **A.** 802.11
- ❍ **B.** 802.11a
- ❍ **C.** 802.11b
- ❍ **D.** 802.11g

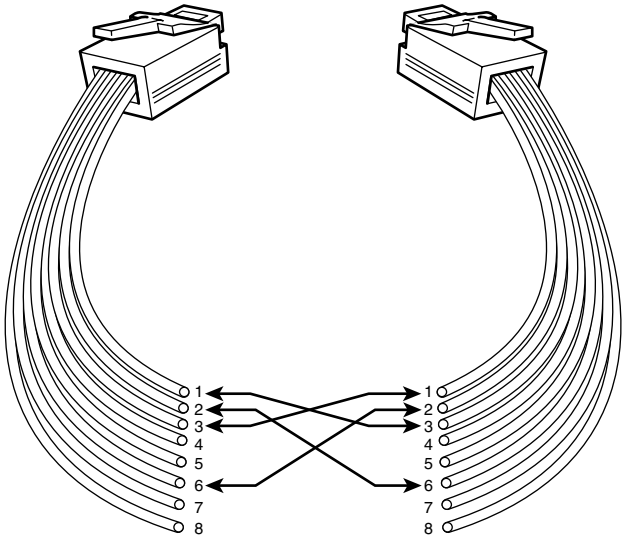
17. Which cable pinout is shown in the following diagram?

- ❍ **A.** Thin coax cable
- ❍ **B.** Thick coax cable
- ❍ **C.** Straight-through cable
- ❍ **D.** Cross-over cable



18. Which cable pinout is shown in the following diagram?

- ❍ **A.** Thin coax cable
- ❍ **B.** Thick coax cable
- ❍ **C.** Straight-through cable
- ❍ **D.** Cross-over cable



19. Which of the following connectors are used by fiber? (Choose the 3 best answers.)

- ❍ **A.** MT-RJ
- ❍ **B.** SC
- ❍ **C.** ST
- ❍ **D.** RJ-45

20. Which of the following are wireless technologies? (Choose the 3 best answers.)

- ❍ **A.** Fast Ethernet
- ❍ **B.** Bluetooth
- ❍ **C.** Infrared
- ❍ **D.** Wi-fi

Answers to Review Questions

1. Refer to Figure 2.1 to check your design of a physical bus topology.

2. Refer to Figure 2.2 to check your design of a physical single ring topology and Figure 2.3 to check your design of a physical dual ring topology.

3. Refer to Figure 2.4 to check your design of a physical star topology.

4. Refer to Figure 2.6 to check your design of a physical partial mesh topology and Figure 2.5 to check your design of a physical full mesh topology.
5. Straight-through cables use four wires and pins 1, 2, 3, and 6. Given those pins, pin 1 is connected on one end of the cable to pin 1 on the opposite end of the cable. Pin 2 at one end is connected to pin 2 on the far end. Pin 3 is connected to pin 3 and pin 6 is connected to pin 6.
6. Cross-over cables also use four wires and pins 1, 2, 3, and 6. The difference is in how the pins are connected at each end. With cross-over cables, pin 1 connects to pin 3 and pin 2 connects to pin 6.

Answers to Exam Questions

1. Answer B is correct. This diagram represents the physical bus topology or the linear bus topology. This topology uses one cable as the trunk or backbone.
2. Answer A is correct. This diagram represents the physical ring topology. Each device is connected to two other devices on the network. Data traverses the network and creates a ring or loop.
3. Answer D is correct. This diagram represents the physical dual ring topology. Unlike a single ring topology, this design offers redundancy if either ring breaks.
4. Answer C is correct. This diagram represents the physical star topology. It may also be referred to as a hub-and-spoke topology.
5. Answer D is correct. This diagram represents the full mesh topology. All the devices on the network are directly connected to every other device on that same network.
6. Answer B is correct. This diagram represents the partial mesh topology. Some but not all of the devices are connected to all of the other devices on the network.
7. Answer A is correct. Fiber is not susceptible to EMI. Answers B, C, and D are all incorrect because thin coaxial cable, category 3 UTP, and category 5 UTP are all susceptible to EMI.
8. Answer D is correct. UTP cables use RJ-45 connectors. Answers A, B, and C are incorrect because fiber uses ST, SC, or MT-RJ connectors.
9. Answer B is correct. Because of attenuation, the maximum, practical length of a UTP cable is 100 meters.
10. Answer A is correct. The total flow of information over a certain time period on a communications medium measured in bits per second is called bandwidth. Answer B is incorrect because crosstalk is an electrical or magnetic field that is a result of one communications signal affecting the signal in a nearby circuit. Answer C is incorrect because attenuation occurs over long distances as a signal loses strength. Answer D is incorrect because EMI is the interference caused by electromagnetic signals.
11. Answer A is correct. A coaxial cable consists of a single copper wire surrounded by a plastic insulation cover and a braided copper shield. Answer B is incorrect because UTP cables use eight colored wires in four pairs. Answer C is incorrect because STP has an additional layer of shielding. Answer D is incorrect because Category 5 is a UTP cable.

12. Answer B is correct. When connecting a switch to a router you must use a straight-through UTP cable.

13. Answer C is correct. When directly connecting two PCs you can use a cross-over UTP cable.

14. Answer C is correct. The best answer here is to replace a hub with a switch. Switches can segment the network. Answers A and B are incorrect because a repeater or an additional hub simply extends the network further. Answer D is incorrect because the network interface connects a PC or laptop to the public network.

15. Answer B is correct. The IEEE standard for Wireless Fidelity is 802.11b. Answer A is incorrect because IEEE standard 802.1q defines VLAN. Answer C is incorrect because IEEE standard 802.3u defines Fast Ethernet. Answer D is incorrect because IEEE standard 802.3ab defines Gigabit Ethernet on a Category 5 cable.

16. Answer B is correct. 802.11a uses a 5GHz RF. Answer A is incorrect because IEEE standard 802.11 is the basis for the 802.11a, 802.11b, and 802.11g wireless standards. Answers C and D are incorrect because 802.11b and 802.11g use 2.4GHz RF. 802.11a is not compatible with 802.11b and 802.11g.

17. Answer C is correct. A straight-through cable uses pins 1, 2, 3, and 6. Given those pins, pin 1 is connected on one end of the cable to pin 1 on the opposite end of the cable. Pin 2 at one end is connected to pin 2 on the far end, and so on. Answers A and B are incorrect because pinouts do not apply to coaxial cable because it is a single copper wire. Answer D is incorrect because cross-over cables also use four wires and pins 1, 2, 3, and 6. The difference is in how the pins are connected at each end. With cross-over cables, pin 1 connects to pin 3 and pin 2 connects to pin 6.

18. Answer D is correct. Cross-over cables also use four wires and pins 1, 2, 3, and 6. The difference is in how the pins are connected at each end. With cross-over cables, pin 1 connects to pin 3 and pin 2 connects to pin 6. Answers A and B are incorrect because pinouts do not apply to coaxial cable because it is a single copper wire. Answer C is incorrect because straight-through cable uses pins 1, 2, 3, and 6. Given those pins, pin 1 is connected on one end of the cable to pin 1 on the opposite end of the cable. Pin 2 at one end is connected to pin 2 on the far end, and so on.

19. Answers A, B, and C are correct. Fiber uses an MT-RJ, SC, or ST connector. Answer D is incorrect because RJ-45 is used by a UTP cable.

20. Answers B, C,and D are correct. Bluetooth, infrared, and wi-fi are all wireless technologies. Answer A is incorrect because Fast Ethernet is an ethernet LAN technology.

Suggested Readings and Resources

The following are some recommended readings on network components and related terminology:

1. Habraken, Joe. *Absolute Beginner's Guide to Networking, fourth edition*. Que Publishing, 2003.

2. "Fiber Optic Connector Guide," http://www.commspecial.com/connectorguide.htm.

3. "Network Cabling Help," www.datacottage.com.

CHAPTER 3

Data Link Networking Concepts

Objectives

This chapter covers the following Cisco-specified objectives for the "Technology" section of the CCNA exam:

Compare and contrast key characteristics of LAN environments

Describe network communications using layered models

Describe the components of network devices

This chapter also covers the following Cisco-specified objective for the "Planning and Designing" section of the CCNA exam:

Design a simple LAN using Cisco technology

- A network device may utilize various components to achieve connectivity and increase functionality. These components are fundamental to internetworking.
- This chapter specifically focuses on the Data Link layer of the OSI model and how network communications occur at this layer.
- LAN environments at the Data Link layer may be set up with token ring, Fiber Distributed Data Interface (FDDI), or one of many ethernet data-link protocols.
- Various network designs or layouts commonly are used to set up a LAN. At the Data Link layer, LANs may be connected with either a bridge or a switch. The operation of these devices is described in Chapter 8, "Bridging and Switching Operations."

Outline

Study Strategies

- Read the objectives at the beginning of the chapter.
- Familiarize yourself with token ring and FDDI protocols.
- Define the IEEE MAC unicast, broadcast, and multicast addresses.
- Review the ethernet family of protocols and be able to identify the characteristics of each protocol.
- Name the devices that are used at the Data Link layer and important traits of each device.
- Define *duplex*.
- Describe microsegmentation.

Introduction

Several data link networking concepts were first introduced in the discussion of the Data Link layer or Layer 2 of the OSI model in Chapter 1, "Standard Internetworking Models." Again, it is important to understand the layered architecture of the OSI model to grasp the fundamentals of how a network operates. Although Chapter 2, "Physical Layer Networking Concepts," went over concepts that define the Physical layer of the OSI model, this chapter goes over concepts that define how a network operates at the Data Link layer specifically.

Important Data Link LAN topics to understand for the CCNA exam include the protocols, addressing, and devices that are used at Layer 2. Cisco specified several objectives related to LAN technologies, which are prevalent at Layer 1 and Layer 2. Let's begin with three Data Link layer protocols: token ring, FDDI, and ethernet.

NOTE

Remember that the Physical and Data Link layers are combined in the TCP/IP model to form the Network Interface layer.

Data Link Protocols

Objective:

Compare and contrast key characteristics of LAN environments

In this section, you will learn about network protocols that can be utilized at the Data Link layer of the OSI model. These protocols include token ring, FDDI, and ethernet. Ethernet Data Link protocols are broken out into addressing and framing standards.

Token Ring

Token ring is a LAN protocol that utilizes a token-passing media access technology in a physical ring or physical star topology, which creates a logical ring topology. This protocol was first developed by IBM but then standardized by IEEE with the 802.5 specification. With token-passing, a three-byte token (or special bit pattern) is inserted in a frame and passed in a single direction from one node to another until it forms a complete loop. The node that has possession of the token is the only one that can send data at any given time on that LAN. Because only one node can send data at a time, collisions are avoided.

Rather than using a hub or switch, Token ring uses a multistation access unit (MAU) to send a token across the network. The MAU has Ring In (RI) and Ring Out (RO) ports. The RO of the first MAU is connected to the RI of the next MAU. This continues until the final MAU,

which connects back to the first MAU RI port via its own RO port. As mentioned, a logical ring is created with this setup. Figure 3.1 shows how a token ring network operates with MAUs.

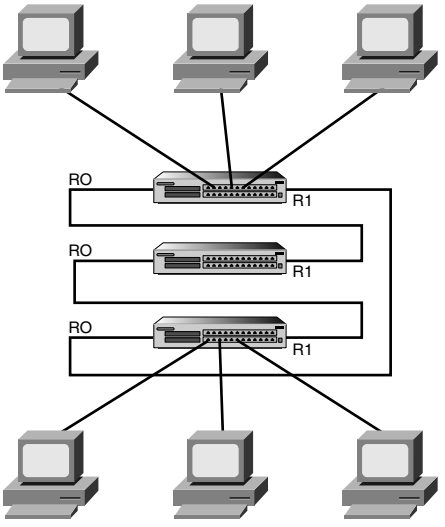


FIGURE 3.1 Token ring network.

A token ring LAN can run at either 4Mbps or 16Mbps. Each device must be configured for the same speed; otherwise the token-passing does not work at all. Overall, although this protocol provides a collision-free network, it is also more expensive to implement than ethernet. This is a major reason why ethernet is the most popular Data Link layer protocol, making token ring a rather distant second.

Let's recap what you've learned about token ring:

- Standardized by the IEEE 802.5 specification
- A token-passing media access technology
- Set up as a physical ring or physical star topology
- Creates a logical ring topology
- Speeds are assigned as either 4Mbps or 16Mbps
- Utilizes an MSAU rather than a switch or hub
- Provides collision-free data transfer
- High overhead

FDDI

FDDI is a LAN protocol that utilizes a token-passing media access method on a dual ring topology. This protocol was created by the American National Standards Institute (ANSI) with the ANSI X3T9.5 specification. Data transmission occurs on fiber-optic cables at a rate of 100Mbps. Primarily, FDDI was developed to run data across the network backbone of a larger company. Dual ring is configured for FDDI to provide redundancy and fault-tolerance. Also, because it runs over fiber it is not susceptible to EMI like other media options. Figure 3.2 shows the dual ring topology of an FDDI network.

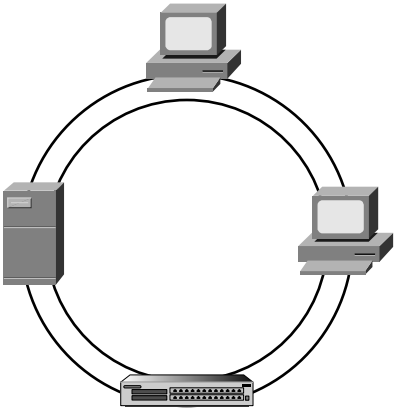


FIGURE 3.2 FDDI network.

NOTE

Copper Distributed Data Interface (CDDI) is a 100Mbps token-passing protocol that runs over copper wire rather than fiber-optic cable.

FDDI uses a method called *beaconing* to signal when a failure is detected on the network. Beaconing enables a device to send a signal informing the other devices on that LAN that token passing has stopped. The beacon travels around the loop from one device to the next until it reaches the last device in that ring. To troubleshoot, the network administrator can find the beacon at that last device and then check the connection between that device and the next connected device on the FDDI network.

Like token ring, FDDI is costly to implement, which is a disadvantage when designing a small network.

Let's recap what you've learned about FDDI:

- Developed by ANSI with the ANSI X3T9.5 specification
- A token-passing media access technology

- Set up as a dual ring topology
- Redundant, fault-tolerant network
- Speed is 100Mbps
- Runs over fiber-optic cable
- Not susceptible to EMI
- Provides collision-free data transfer
- Fault-detection provided by beaconing
- High overhead

Ethernet at the Data Link Layer

Objective:

Describe network communications using layered models

Ethernet, ethernet, ethernet…

The most popular LAN by a mile, ethernet is a group of protocols and standards that work at either the Physical or Data Link layer of the OSI model. This section covers ethernet technology that is relevant to Layer 2. Ethernet is defined by the IEEE 802.3 specification. As technology advancements occur, IEEE has defined additional classifications of 802.3, which include Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, and Long Reach Ethernet. The physical implementations of each Ethernet standard are covered in greater detail in a moment, but first I would like to review ethernet addressing and ethernet framing. Ethernet addressing can be achieved with unicast, multicast, or broadcast addresses at the Data Link layer.

Ethernet Addressing

The Data Link layer uses physical or hardware addressing to make sure data is delivered to the appropriate end device in a LAN. Physical addresses or what are commonly referred to as *MAC addresses* are used at Layer 2. Before you go any further, it's a good idea to take a minute to review what you learned in Chapter 1.

The Data Link layer of the OSI model is the only one that has sublayers. Table 3.1 shows the breakout of Layer 2.

TABLE 3.1 Data Link Layer and Sublayers

OSI Model Layer	Sublayer
Data Link Layer	Media Access Control (MAC) IEEE 802.3
	Logical Link Control (LLC) IEEE 802.2

A MAC address is hard-coded (burnt in) on the network interface controller (NIC) of the Physical Layer device attached to the network. Each MAC address must be unique and use the following format:

- The address must consist of 48 bits (or 6 bytes).
- It must be displayed by 12 hexadecimal digits (0–9, A–F).
- The first 6 hexadecimal digits in the address are a vendor code or organizationally unique identifier (OUI) assigned to that NIC manufacturer.
- The last 6 hexadecimal digits are assigned by the NIC manufacturer and must be different from any other number assigned by that manufacturer.

An example of a MAC address would be 00:00:07:A9:B2:EB. The OUI in this example is 00:00:07.

EXAM ALERT

MAC Address Structure Know that a MAC address consists of 48 bits and is expressed as 12 hexadecimal digits from either 0–9 or A–F. Also, know that the vendor code or OUI is the first 6 hexadecimal digits of the MAC address.

NOTE

Check out an actual example of a physical address on your own PC. From the Start menu, select Run. Then type in **`cmd`** to enter the command prompt for your PC. You should see a new window open on the screen where you can type in **`ipconfig /all`** at the prompt. Among other things, the output includes the physical or MAC address of your PC.

Ethernet LAN addresses can be broken down into two subcategories: individual and group addresses. An individual address is referred to as a *unicast address*. A unicast address identifies the MAC address of an individual LAN or NIC card. The source address on an ethernet frame will always be a unicast address. When a packet from the Network layer is framed for transport and is being forwarded to a single destination, a unicast address is also the destination address on an ethernet frame. Figure 3.3 represents an example of frame forwarding between a unicast source and a unicast destination device. Cisco devices typically use three

groups of four hexadecimal digits separated by periods, such as 0000.0C12.3456. Cisco's OUI is 0000.0C.

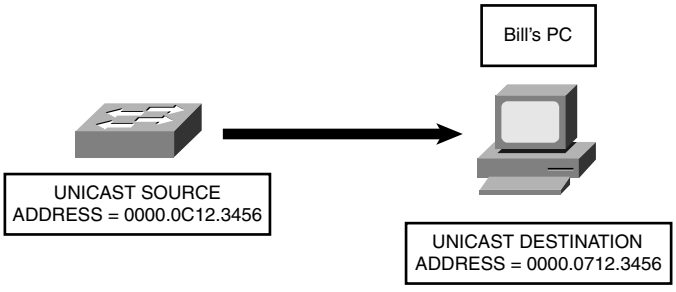


FIGURE 3.3 Unicast frame transmission.

In the example in Figure 3.3, Bill's computer checks the destination address on the ethernet frame. If the destination address is the MAC on his computer, the frame is processed. If the destination address does not match up, the frame is dropped.

Group Ethernet LAN addresses classify more than one LAN or NIC card. Multicast and broadcast addresses are both classified as group addresses and can be described as follows:

- **Multicast addresses**—Addresses where a frame can be sent to a group of devices in the same LAN. IEEE ethernet multicast addresses always begin with 0100.5E in hexadecimal format. The last three bytes can be any combination of hexadecimal digits. The IP routed protocol supports multicast addressing with three groups of four hexadecimal digits separated by periods (like Cisco devices), so it appears as 0100.5Exx.xxxx, where the x's can represent any hex digit from 0–9 or A–F. Figure 3.4 shows a frame that is being forwarded from a unicast source to an IP multicast destination address.

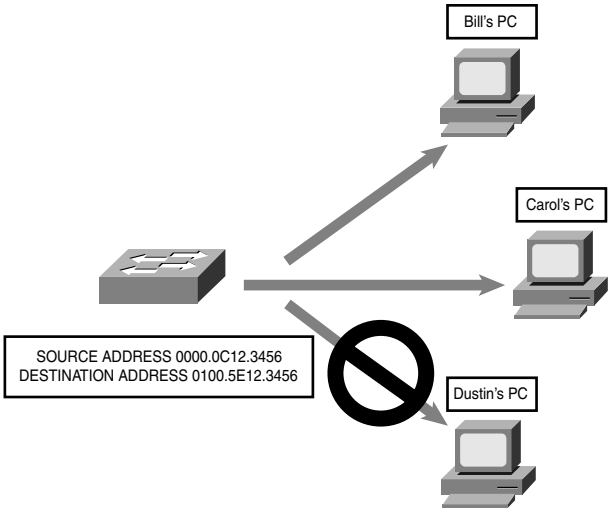


FIGURE 3.4 Multicast frame transmission.

In this example, the switch sends a frame from its own unicast address to the multicast address of 0100.5E12.3456. Each device in that LAN segment checks the destination address to see whether it should be processed. Although Bill and Carol's computer will review and process the frame, Dustin's does not care about it and therefore drops the frame.

- **Broadcast addresses**—Addresses where a frame is sent to all devices in the same LAN segment. Multicast and broadcast addresses are limited to a LAN or network segment. Broadcast addresses are always the same value, which is FFFF.FFFF.FFFF. Figure 3.5 shows a switch sending a frame to the destination address FFFF.FFFF.FFFF. Because this is the broadcast address value, all the devices in that LAN should process the frame.

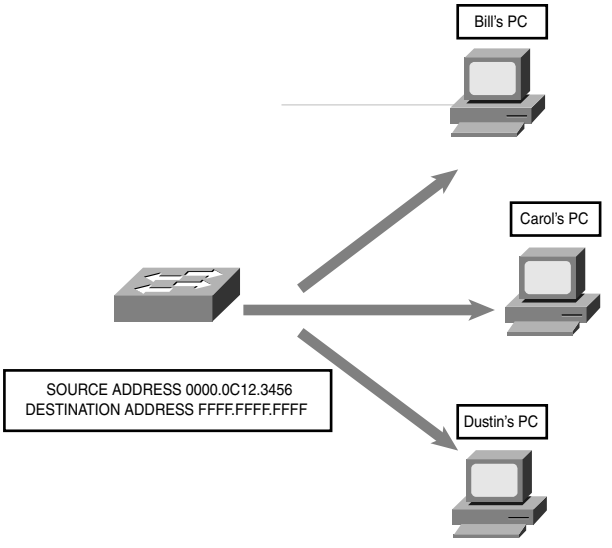


FIGURE 3.5 Broadcast frame transmission.

EXAM ALERT

The broadcast address value is FFFF.FFFF.FFFF.

Challenge

You should be able to recognize the difference between a unicast, multicast, and broadcast address for the exam. In this challenge, I give you an address and ask that you identify whether it is a unicast, multicast, or broadcast address.

(continues)

(continued)

TABLE 3.2 Unicast, Multicast, and Broadcast Addresses

This Address Is…	Unicast, Multicast, or Broadcast
0100.5C12.3456	
0100.5E11.2345	
FFFF.FFFF.FFFF	
0100.5E12.3456	
0000.0C12.3456	

Ethernet Framing

As you will recall from Chapter 1, data traverses the layers of the OSI model and is encapsulated from layer to layer.

Table 3.3 shows the process of using the OSI model to encapsulate data.

TABLE 3.3 OSI Model Layer and Related Control Information

OSI Layer	Control Information Name
Application Presentation Session	Data
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit

EXAM ALERT

The correct order for data encapsulation is data, segment, packet, frame, and bit.

The Data Link layer uses frames to transport data between layers. Framing is the process of interpreting data that is either received or sent out across the network. The 802.2 LLC Data Link sublayer is an extension of 802.3 and is responsible for framing, error-detection, and flow control. Figure 3.6 represents an 802.3 frame.

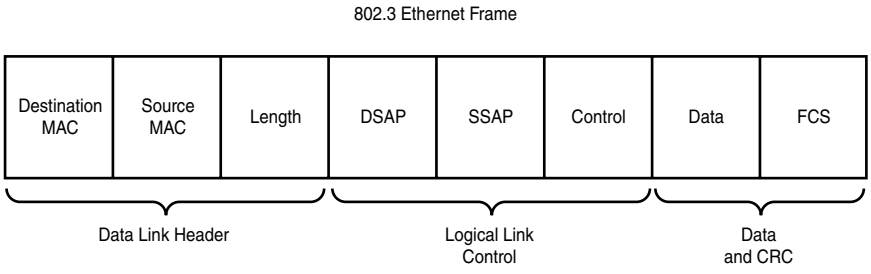


FIGURE 3.6
802.3 frame.

EXAM ALERT

For the CCNA exam, review the structure of the 802.3 frame, specifically, the Destination/Source MAC address fields of the data-link header, the DSAP/SSAP fields of the LLC portion of the frame, and the FCS field of the Data and CRC data-link trailer.

The three main parts of an 802.3 frame can be broken down and described as follows:

- The Data Link header portion of the frame contains the destination MAC address (6 bytes), source MAC address (6 bytes), and length (2 bytes).
- The Logical Link Control portion of the frame contains Destination Service Access Point (DSAP), Source Service Access Point (SSAP), and control information. All three are 1 byte long. The Service Access Point (SAP) identifies an upper-layer protocol such as IP (06) or IPX (E0).
- The data and cyclical redundancy check (CRC) portion of the frame is also called the *data-link trailer*. The data field can be anywhere from 43 to 1497 bytes long. The frame check sequence (FCS) field is 4 bytes long. FCS or CRC provides error detection.

Error detection is used to determine whether bit errors happened during frame transmission. The sender and receiver of a frame use the same mathematical formula to analyze the information in the FCS field of the data-link trailer. If the calculations match up, there were no errors on that frame transmission.

EXAM ALERT

The FCS field of a frame is used for error detection.

Challenge

Given the necessity that you know the layout of the 802.3 frame, I will provide you with an outline. Fill out the fields that belong to each portion of the frame.

Data Link Header			Logical Link Control			Data and CRC	

Now that you have filled out the fields, provide the full names of the following acronyms that are used in conjunction with the 802.3 frame.

MAC =

LLC =

DSAP =

SSAP =

CRC =

FCS =

I mentioned how the SAP in the 802.3 frame identifies an upper-layer protocol with 1 byte or 2 hexadecimal digits. The IP SAP is 06. Well, it turns out that 1 byte was insufficient for the number of protocols that need to be recognized by an 802.3 frame. To accommodate the influx of protocols, IEEE permitted for an additional header in the 802.3 frame called a *Subnetwork Access Protocol (SNAP)* header.

The SNAP header serves the same purpose as the DSAP field; however, it consists of 2 bytes. For example, 0800 is the hexadecimal format assigned to IP with SNAP. RFC 1700 identifies all the values that are associated with SAP and SNAP.

Physical Ethernet Standards

Objective:

Describe the components of network devices

Have I said that ethernet is the most popular LAN protocol? Ethernet started in the 1970s when Xerox needed a networking system to connect personal computers. Xerox joined forces with Digital Equipment Corp. (DEC) and Intel to develop the protocol, which is why the very first ethernet standards were referred to as DIX Ethernet. This section covers the progression of ethernet standards from the earlier 10Mbps connections to the more recent 10 gigabit ethernet connections.

Each standard has a maximum connection length and speed. Individual ethernet standards also specify which cables and connectors can be used for network connectivity. You will be introduced to each group of standards starting with the 10Mbps ethernet connections, then the 100Mbps Fast Ethernet connections, 1Gbps ethernet, and 10Gbps ethernet connections.

Ethernet

The IEEE 802.3 ethernet standards are covered in the following sections. The following list contains all the ethernet standards that are covered in this chapter, in order.

- 10BASE-2
- 10BASE-5
- 10BASE-T
- 10BASE-FL
- 100BaseT4
- 100BaseTX
- 100BaseFX
- 1000BaseT
- 1000BaseTX
- 1000BaseCX
- 1000BaseSX
- 1000BaseLX
- 10GbE

10BASE-2

10BASE-2 networks are connected with RG-58 coaxial cables that use Bayonet Neill Concelman (BNC) connectors. There are no other hardware devices such as hubs or switches to connect devices, just the coaxial cables. This creates a physical bus topology. An electrical signal is sent by each device that wants to transmit data on that network. If more than one device sends a signal at the same time, this causes a collision and the signal is lost. To prevent loss of data transmissions, an algorithm called *Carrier Sense Multiple Access Collision Detection (CSMA/CD)* was defined. This algorithm sends a jam signal to notify the devices that there has been a collision. The devices then halt transmission for a random back-off time. CSMA/CD must be activated for 10Base ethernet LANs that are connected with a hub.

EXAM ALERT

For the exam, know the definition of CSMA/CD and its capability to act as an arbitrator for devices in an ethernet LAN.

The name 10BASE-2 breaks down as follows:

10—10Mbps data transmission speed

Base—Represents *baseband*, the signaling mode where the media can only send one signal per wire at a time

2—Actually refers to 185m or the maximum segment length (where 185 is rounded up to 200 and 2 is a multiple of 100m)

NOTE

So what you can see from the naming scheme is that the first number represents the speed, the word *base* means the baseband signaling mode, and the last helps you determine the type of cable used.

10BASE-5

10BASE-5 has the same characteristics as 10BASE-2, but with a maximum segment length of 500m. The 5 is also a multiple of 100m.

10BASE-T

10BASE-T has a maximum segment length of 100m and has a 10Mbps data transmission speed. 10BASE-T can use Category 3, 4, or 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cables for connectivity. If you recall, UTP is the more common and cost-effective solution. STP has an additional shield that provides additional reduction of interference and attenuation, but it is also the more expensive solution. The following cables can be used with a 10BASE-T connection:

- **Category 3**—Data cable that can handle speeds up to 10Mbps.

  Although it is faster than the Cat2 cable, this was quite popular until network speeds surpassed the 10Mbps threshold.

- **Category 4**—Data cable that can handle speeds up to 16Mbps and is meant to be used with token ring LANs.

- **Category 5**—Data cable that can handle speeds up to 100Mbps and is currently the most popular cable selection.

EXAM ALERT

UTP is vulnerable to electromagnetic interference (EMI) and uses an RJ-45 connector.

10BASE-FL

10BASE-FL also has a 10Mbps data transmission speed, but it runs over fiber-optic cables. This option allows for a maximum segment length up to 2km.

Table 3.4 compares the 802.3 ethernet characteristics, listing the key characteristics of each specification.

TABLE 3.4 Summary of Ethernet 802.3 Characteristics

Standard	Speed	Maximum Distance	Media Type	Connector Used
10BASE-2	10Mbps	185m	RG-58 coaxial	BNC
10BASE-5	10Mbps	500m	RG-58 coaxial	BNC
10BASE-T	10Mbps	100m	Category 3, 4, or 5 UTP or STP	RJ-45
10BASE-FL	10Mbps	Up to 2km	Fiber-optic	SC or ST

As you can see, the early standards are all limited to 10Mbps. More recent ethernet specifications allow for faster data transmission speeds and are more popular for today's networks.

Fast Ethernet

Fast Ethernet was derived for networks that needed speeds in excess of 10Mbps. The IEEE 802.3u defines standards for 100BaseT4, 100BaseTX, and 100BaseFX. You may also hear them collectively referred to as 100BaseX. Based on what you learned from the 10Base naming scheme, you would be correct to infer that the 100 represents 100Mbps. Also, all three standards are baseband like the 10Mbps family of protocols.

NOTE

Fast Ethernet is defined in the IEEE 802.3u standard.

100BaseT4

100BaseT4 has the same characteristics as 100BaseTX except that it can use Category 3, 4, or 5 UTP or STP cables.

100BaseTX

100BaseTX, like 10BASE-T, uses either UTP or STP. Category 5 UTP cable is used with this implementation. 10BASE-T has a maximum segment length of 100m.

100BaseFX

100BaseFX uses either single-mode or multimode fiber-optic cables to connect. Multimode (MM) fiber set for half-duplex can reach a distance of 412m. Single-mode (SM) fiber set for full-duplex can reach a distance of 10,000m. SC or ST connectors can be used. The drawback, as mentioned before with fiber implementations, is the high overhead.

- **Multimode (MM) fiber**—This is generally used for shorter distances and is ideal for a campus-sized network. MM also has a larger diameter of optical fiber than SM fiber.
- **Single-mode (SM) fiber**—This mode is used to span longer distances. SM also allows for a higher data rate than MM and faster data transmission speeds.

EXAM ALERT

Fiber-optic cable is not susceptible to EMI, Near-end Crosstalk (NEXT), or Far-end Crosstalk (FEXT).

REVIEW BREAK

Table 3.5 compares Fast Ethernet 802.3u standards.

TABLE 3.5 Comparison of Fast Ethernet 802.3u Characteristics

Standard	Speed	Maximum Distance	Media Type	Connector Used
100BaseT4	100Mbps	100m	Category 3, 4, or 5 UTP or STP	RJ-45
100BaseTX	100Mbps	100m	Category 5 UTP or STP	RJ-45
100BaseFX	100Mbps	412m with half-duplex MM fiber 10,000m with full-duplex SM fiber	Fiber-optic	SC or ST

Gigabit Ethernet

Gigabit Ethernet standards all have a data transmission speed of 1000Mbps (1Gbps) and use a baseband signaling mode. Gigabit Ethernet can be broken down into two IEEE standards, 802.3ab or 1000BaseT and 802.3z or 1000BaseX.

1000BaseT 802.3ab

1000BaseT or 1000BaseTX is defined by the 802.3ab standard and can reach a maximum total distance per segment of 75m. This standard uses a minimum of Category 5 UTP cable with an RJ-45 connector.

- **Category 5e**—Data cable that can handle speeds up to 1Gbps; a popular choice for Gigabit Ethernet networks.
- **Category 6**—Cable that was created to exceed speeds of 1Gbps.

Table 3.6 summarizes the primary points of interest that are relevant for the 1000BaseT standard.

TABLE 3.6 Summary of Gigabit Ethernet 802.3ab Characteristics

Standard	Speed	Maximum Distance	Media Type	Connector Used
1000BaseT or 1000BaseTX	1000Mbps or 1Gbps	75m	Category 5 UTP or higher	RJ-45

1000BaseX 802.3z

1000BaseX is the collective name for 802.3z standards 1000BaseCX, 1000BaseSX, and 1000BaseLX that have the following characteristics respectively:

- **1000BaseCX**—1000BaseCX is the unique standard in this family because it uses shielded copper wire cable with a 9-pin shielded connector instead of fiber-optic cable for connectivity. The maximum total distance per segment is a mere 25m.
- **1000BaseSX—**1000BaseSX transmits short-wavelength laser over fiber-optic cable. Either 50-micron or 62.5-micron (diameter) MM fiber can be used with this option. Lengths may vary depending on the type of MM fiber and duplex chosen for each connection as follows:
  - Half-duplex 62.5-micron MM fiber connections can reach a maximum segment length of 275m.
  - Half-duplex 50-micron MM fiber connections can reach a maximum segment length of 316m.
  - Full-duplex 62.5-micron MM fiber connections can reach a maximum segment length of 275m.
  - Full-duplex 50-micron MM fiber connections can reach a maximum segment length of 550m.

As you can see, the 50-micron MM fiber can offer longer segment distances. The 62.5-micron MM fiber reaches the same maximum segment length of 275m regardless of the duplex.

- **1000BaseLX—**1000BaseLX transmits long-wavelength laser over fiber-optic cable. Either 50-micron or 62.5-micron (diameter) MM fiber can be used with this option. SM fiber can also be used with 1000BaseLX, which differentiates this standard from 1000BaseSX. The same MM fiber length restrictions apply based on the implementation of half- or full-duplex. The following lengths apply when SM fiber is used:
  - Half-duplex SM fiber connections can reach a maximum segment length of 316m.
  - Full-duplex SM fiber connections can reach a maximum segment length of 5000m.

  Using full-duplex SM fiber allows for a huge increase in distance. As you can imagine, this is also the more expensive option.

Table 3.7 compares Fast Ethernet 802.3z standards.

TABLE 3.7 Comparison of Gigabit Ethernet 802.3z Characteristics

Standard	Speed	Maximum Distance	Media Type	Connector Used
1000BaseCX	1000Mbps or 1Gbps	25m	Shielded copper wire	9-pin shielded connector
1000BaseSX	1000Mbps or 1Gbps	275m with half or full-duplex 62.5-micron MM fiber 316m with half-duplex 50-micron MM fiber 550m with full-duplex 50-micron MM fiber	MM fiber-optic	SC or ST
1000BaseLX	1000Mbps or 1Gbps	275m with half- or full-duplex 62.5-micron MM fiber 316m with half-duplex 50-micron MM fiber or SM fiber 550m with full-duplex 50-micron MM fiber 5000m with full-duplex SM fiber	MM or SM fiber-optic	SC or ST

EXAM ALERT

Gigabit Ethernet comprises the 802.3ab and the 802.3z standards.

10-Gigabit Ethernet (10GbE)

You guessed it: 1Gbps just wasn't a fast enough option. Actually, it is just the nature of technology to constantly strive for faster speeds. Yet another new standard was defined by IEEE and labeled 802.3ae. Earlier in this chapter you saw 10BASE-2, which has data transmission speeds of 10Mbps. 10-Gigabit Ethernet transmits data at 10,000Mbps. That is quite an upgrade! IEEE 802.3ae uses 62.5-micron MM, 50-micron MM, or SM fiber-optic cabling for connectivity and a baseband signaling mode.

NOTE

All of the ethernet standards, regardless of their speed, use the same 802.3 MAC and 802.2 LLC headers and trailers.

Long Reach Ethernet

Cisco Long Reach Ethernet (LRE) was developed to provide broadband service over existing telephone-grade or Category 1, 2, or 3 wiring. Speeds vary between 5–15Mbps and can reach a maximum segment length of up to 5000m. Cisco LRE may be a viable networking solution for a LAN or MAN that already has Category 1/2/3 cabling installed. A hotel could benefit from Cisco LRE to provide high-speed Internet or video conferencing solutions to their clientele.

NOTE

Broadband is a signaling method that supports various frequencies such as audio and video.

Data Link Layer Devices

Objective:

Design a simple LAN using Cisco technology

At the Data Link layer, either a bridge or a Layer 2 switch can be installed to segment a LAN. Hubs and repeaters at the Physical layer only serve to extend a network. With segmentation,

switches and bridges create a separate collision domain for each connected node, which effectively reduces the number of collisions that occur on that network.

Remember from Chapter 1 that a collision domain is a group of nodes that shares the same media and are segmented by switches or bridges. A collision occurs if two nodes attempt a simultaneous transmission within the same collision domain. This reinforces the need for an increased number of collision domains. Figure 3.7 demonstrates how a bridge creates two collision domains.

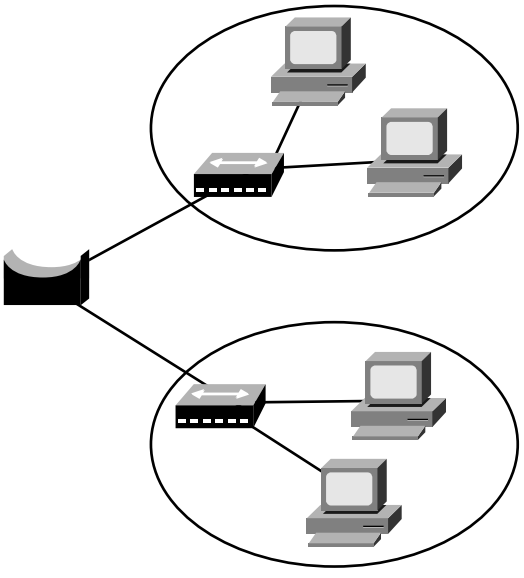


FIGURE 3.7 Example of a bridged network.

Figure 3.8 provides an example of a situation in which a switch creates separate collision domains.

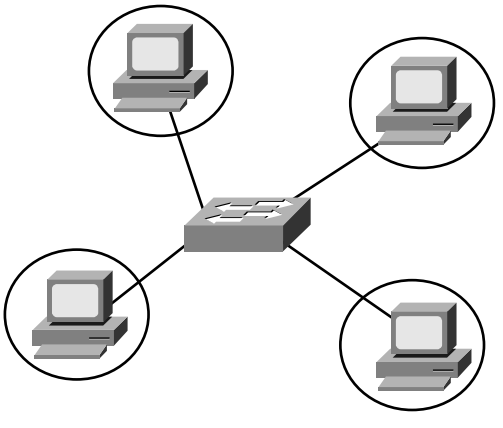


FIGURE 3.8 Example of a switched network.

EXAM ALERT

Know what a collision domain is and that a bridge and/or switch will segment a network and create an additional collision domain for each segment. Routers not only segment collision domains, but they also segment broadcast domains.

Bridges

Bridges were created to alleviate several expansion-related network issues. As networks were growing and becoming more complex, hubs and repeaters no longer provided sufficient network resources. Because they do not segment the network, all the devices connected to a hub or repeater had to share the same bandwidth. Also, if one device sent a frame it could collide with a frame from another device on that LAN. This meant that all devices on that LAN had to take turns sending frames. Again, this is not very efficient as additional devices are added to a network.

Transparent bridges were introduced and helped solve these growing pains. The word *transparent* is used to indicate that the other devices on a network are not aware of its existence. Bridges use a software application to forward frames.

The following are the primary tasks performed by both bridges and switches:

- The source MAC address of every inbound frame is examined to learn its MAC address.
- Frames may either be forwarded or filtered depending on the destination MAC address (they can also be flooded if the destination is unknown).
- Eliminates loops that are caused by redundant connections by configuring Spanning Tree Protocol (STP).

Learned MAC addresses and their interfaces are stored in a *bridge table* on the bridge or switch. When a new frame arrives on that bridge or switch, the device refers to the bridge table to decide how to forward or filter the frame. If the frame's destination MAC address is on a different segment of that LAN, the device forwards the frame to that segment. If the frame's destination MAC address is on the same segment as the source MAC address, the device filters the frame. That frame reaches its destination without the assistance of a bridge or switch. Figure 3.9 shows a segmented LAN with the MAC addresses of each end user.

As frames are received by the bridge or switch from each end user, it updates its bridge table with their MAC addresses and the interface on which the frame came into the device. Table 3.8 shows the bridge table of this bridge.

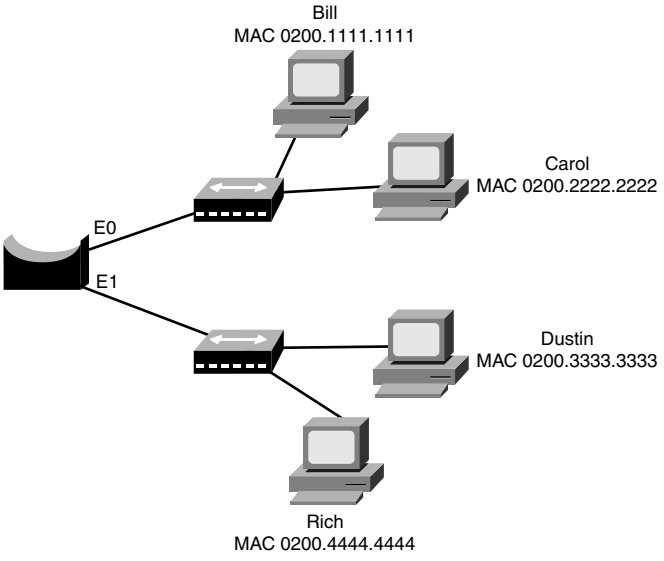


FIGURE 3.9 Bridge LAN.

TABLE 3.8 Example Bridge Table for Figure 3.9

MAC Address	Interface
0200.1111.1111	E0
0200.2222.2222	E0
0200.3333.3333	E1
0200.4444.4444	E1

If the incoming frame destination address is…

- **Unicast**—The bridge checks the bridge table first. If the destination unicast address is not in the bridge table, it forwards the frame to all interfaces except for the interface that originally sent the frame. If the destination unicast address is in the bridge table and on a different interface than the interface that originally sent the frame, it forwards the frame. If the destination unicast address is in the bridge table and on the same interface as the sender, the frame is filtered.
- **Multicast**—The bridge forwards the frame to all interfaces except for the interface that originally sent the frame.
- **Broadcast**—The bridge forwards the frame to all interfaces except for the interface that originally sent the frame.

Challenge

Based on what you just learned about bridge and switch frame filtering or forwarding, take a look at Figure 3.10 and fill out the bridge table for this network that is using a switch for connectivity.

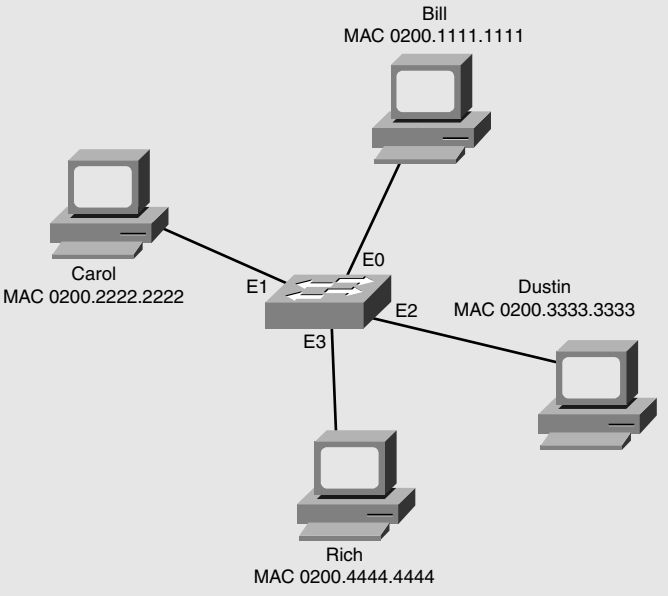


FIGURE 3.10 Switch LAN.

Bridge Table

Address	Interface

Using the same diagram and your new bridge table, I will give you a source and destination address. Please fill out whether the frame will be filtered or forwarded. If it is forwarded, also fill out the outbound interface to which the frame will be sent.

TABLE 3.9 MAC Filtering or Forwarding

Source Address	Destination Address	Filter or Forward	Outbound Interface(s)
0200.1111.1111	0200.2222.2222		
0200.2222.2222	0200.3333.3333		
0200.3333.3333	0200.4444.4444		

(continues)

(continued)

TABLE 3.9 *Continued*

Source Address	Destination Address	Filter or Forward	Outbound Interface(s)
0200.2222.2222	FFFF.FFFF.FFFF		
0200.4444.4444	0200.1111.1111		
0200.1111.1111	0100.5E12.3456		

EXAM ALERT

Bridges and switches examine the source MAC address of each inbound frame to learn MAC addresses.

Switches

Layer 2 switches are multi-port bridges; therefore, they have all the same functionality of bridges. There are differences that differentiate a switch from a bridge. For example, switches utilize hardware or Application-Specific Integrated Circuit (ASIC) chips to forward frames rather than software. Also, each port of the switch has a dedicated bandwidth. If the dedicated port on a switch is 10Mbps, the connected LAN segment has a dedicated bandwidth of 10Mbps. This works in the same manner for 100Mbps and 1000Mbps dedicated switch ports. This feature also sets a switch apart from a bridge that has a low port density.

EXAM ALERT

For the test, know that switches are multi-port bridges that use ASIC hardware chips for frame forwarding. Dedicated bandwidth enables the switch port to guarantee the speed assigned to that port. For example, 100Mbps port connections get 100Mbps transmission rates.

A popular ethernet switch port is the 10/100 ethernet port, where you can set the port to pass traffic at 10Mbps or 100Mbps. Chapter 4, "IP at the Network Layer," goes into more detail regarding specific Cisco devices, including the 2950 series switches.

Challenge

Do you recall the difference between straight-through and crossover cables? Both cables are used with ethernet networks. In Chapter 2, Figure 2.7 and Figure 2.8 demonstrate the differences between straight-through and crossover. Selecting the right cable for your network connections is vital. The following connections are all related specifically to switch connectivity. Please determine whether you should use a straight-through or crossover cable between the devices.

Connecting a…	Type of Cable
Switch to a switch	
Switch to a hub	
Switch to a PC	
Plugged into a dedicated switch port	
Switch to a router	

NOTE

Chapter 8 elaborates on the general concepts that are put forth in this chapter.

Duplex

It is important that you understand duplex logic and how it affects traffic on a network. The communication mode of a device may either be half-duplex or full-duplex, depending on the connection type.

Half-duplex allows for one-way communication, which means that a device can only send or receive a data transmission at any given time. This option does not allow for simultaneously sending and receiving data. As part of a shared collision domain, hubs are inherently set up for half-duplex. Bandwidth suffers because a collision detection technology such as the CSMA/CD algorithm must be implemented. Collision detection can chew up 50–60% of the bandwidth on that ethernet LAN.

Full-duplex allows for two-way communication, which means that a device can simultaneously send and receive data transmissions. Full-duplex is available with dedicated switch port connections to a single device. If a switch port connection is configured for full-duplex, the CSMA/CD algorithm must be disabled. An ethernet connection set for full-duplex allows for 100% transmission speeds in both directions. For example, a 100Mbps connection can transmit data simultaneously at 100Mbps in each direction.

With ethernet, if a switch port and NIC offer multiple speed options as well as half- and full-duplex settings, autonegotiation can be configured on both devices. The switch and NIC automatically negotiate the connection speed and duplex so that the settings on both ends match. You may have heard of a 10/half or 100/full connection before. The term 10/half refers to a 10Mbps half-duplex connection. It is more likely that you will see 100/full, which indicates a 100Mbps full-duplex connection.

NOTE

Autonegotiation may not always be a reliable option. There have been some instances where the switch port goes into error disable mode because of massive errors. Configuring or "hard coding" the port and NIC to the appropriate speed and duplex settings may resolve the issue when the port is reactivated.

EXAM ALERT

Hubs use half-duplex technology. Switches can be set up for full-duplex.

Microsegmentation

Microsegmentation occurs when a switch creates a dedicated path for sending and receiving transmissions with each connected host. Each host then has a separate collision domain and a dedicated bandwidth.

Chapter Summary

Many important functions occur at the Data Link layer of the OSI model. Different technologies can be implemented at Layer 2 to transmit data across the network. Token ring and FDDI networks use token-passing to send frames, whereas ethernet uses the 802.3 frame standard with 802.2 LLC specifications. Ethernet framing and ethernet addressing are both significant topics for the CCNA exam. Other key ethernet functions include error detection and arbitration. Although the FCS field of the 802.3 frame detects errors on a LAN, the CSMA/CD algorithm arbitrates how data is transmitted on a LAN.

Data Link layer devices include bridges and switches. Switches are really multi-port bridges, so they share the same general functionalities. New networks are most likely to use a Layer 2 switch in place of a bridge. Switches have been improved upon over the years and offer more options for the consumer, such as dedicated bandwidth and full-duplex communications.

Although the Data Link layer uses frames to transmit data, the Network layer uses Internet Protocol or IP addresses to route traffic. Chapter 4 discusses IP addressing and subnetting at length. Both topics are imperative for the CCNA exam.

Key Terms

- token-passing
- token ring
- 802.5
- MSAU
- RI
- RO
- FDDI
- ANSI X3T9.5
- unicast
- multicast
- broadcast
- frame
- 802.2
- MAC
- LLC
- SAP
- DSAP
- SSAP
- SNAP
- 802.3
- 10BASE-2
- 10BASE-5
- 10BASE-T
- 10BASE-FL
- 802.3u
- 100BaseT4
- 100BaseTX
- 100BaseFX
- 802.3ab
- 1000BaseT
- 802.3z
- 1000BaseCX
- 1000BaseSX
- 1000BaseLX
- 802.3ae
- 10GbE
- baseband
- broadband
- LRE

- EMI
- coaxial cable
- unshielded twisted-pair cable
- shielded twisted-pair cable
- fiber-optic cable
- multimode
- single-mode
- switch
- ASIC
- bridge
- transparent bridges
- Spanning Tree Protocol
- duplex
- microsegmentation

Apply Your Knowledge

Exercises

3.1 IEEE 802.3 Ethernet Standards

You may be asked to identify the standards associated with IEEE Ethernet on the CCNA exam. In this exercise, I am listing the ethernet specification and want you to complete the table to include the IEEE-defined standard, the associated speed, and the cable or media type used for each specification. You may refer back to Tables 3.4, 3.5, 3.6, and 3.7 to check your answers.

Estimated Time: 10 minutes

IEEE Standard	IEEE Standard #	Maximum Speed	Cable or Media
10BASE-2			
10BASE-5			
10BASE-T			
10BASE-FL			
100BaseT4			
100BaseTX			
100BaseFX			
1000BaseT or 1000BaseTX			
1000BaseCX			
1000BaseSX			
1000BaseLX			
10GbE			

Review Questions

1. Define token-passing.
2. List the characteristics of a token ring network.
3. List the characteristics of an FDDI network.
4. Define unicast, multicast, and broadcast.
5. Describe CSMA/CD.
6. What are the primary tasks performed by both bridges and switches?
7. Describe half- and full-duplex.
8. Define microsegmentation.

Exam Questions

1. Which of the following is the IEEE standard for token ring?
   - ❍ **A.** 802.2
   - ❍ **B.** 802.3a
   - ❍ **C.** 802.3u
   - ❍ **D.** 802.5

2. ANSI X3T9.5 is the specification for which LAN technology?
   - ❍ **A.** Token ring
   - ❍ **B.** Fast Ethernet
   - ❍ **C.** FDDI
   - ❍ **D.** LLC

3. What Data Link layer technology inserts a three-byte token (or special bit pattern) into a frame and passes it in a single direction from one node to another until it forms a complete loop?
   - ❍ **A.** Token-passing
   - ❍ **B.** Unicast
   - ❍ **C.** Multicast
   - ❍ **D.** Broadcast

4. Which of the following LAN protocols use token-passing for frame transmission? (Choose the 2 best answers.)

- ❍ **A.** Fast Ethernet
- ❍ **B.** Token ring
- ❍ **C.** Gigabit Ethernet
- ❍ **D.** FDDI

5. This MAC sublayer address type identifies the MAC address of an individual LAN or NIC card.

- ❍ **A.** Unicast
- ❍ **B.** Multicast
- ❍ **C.** Broadcast
- ❍ **D.** Token

6. Which of the following addresses is an example of a unicast address? (Choose all that apply.)

- ❍ **A.** 0000.0C12.3456
- ❍ **B.** 0100.5E12.3456
- ❍ **C.** FFFF.FFFF.FFFF
- ❍ **D.** 0200.1111.1111

7. This MAC sublayer address type sends a frame to a subset of devices on the LAN.

- ❍ **A.** Unicast
- ❍ **B.** Multicast
- ❍ **C.** Broadcast
- ❍ **D.** Token

8. Which of the following addresses is an example of a multicast address?

- ❍ **A.** 0000.0C12.3456
- ❍ **B.** 0100.5E12.3456
- ❍ **C.** FFFF.FFFF.FFFF
- ❍ **D.** 0200.1111.1111

9. This MAC sublayer address type sends a frame to all the devices on the LAN.

- ❍ **A.** Unicast
- ❍ **B.** Multicast
- ❍ **C.** Broadcast
- ❍ **D.** Token

10. Which of the following addresses is an example of a broadcast address?

- ❍ **A.** 0000.0C12.3456
- ❍ **B.** 0100.5E12.3456
- ❍ **C.** FFFF.FFFF.FFFF
- ❍ **D.** 0200.1111.1111

11. The OSI model Data Link layer uses _____ to transport data between layers.

- ❍ **A.** Bits
- ❍ **B.** Frames
- ❍ **C.** Packets
- ❍ **D.** Segments

12. Which field of a frame is used for error detection?

- ❍ **A.** SAP
- ❍ **B.** DSAP
- ❍ **C.** SSAP
- ❍ **D.** FCS

13. Which IEEE Ethernet standards define Gigabit Ethernet? (Choose all that apply.)

- ❍ **A.** 802.3u
- ❍ **B.** 802.3ab
- ❍ **C.** 802.3z
- ❍ **D.** 802.3ae

14. Bridges and switches segment a network and create an additional _____ domain for each segment.

- ❍ **A.** Collision
- ❍ **B.** Broadcast
- ❍ **C.** Unicast
- ❍ **D.** Multicast

15. Bridges and switches examine the _____ of each inbound frame to learn MAC addresses.

- ❍ **A.** Multicast MAC address
- ❍ **B.** Broadcast MAC address
- ❍ **C.** Source MAC address
- ❍ **D.** Destination MAC address

16. Which device uses ASIC hardware chips for frame forwarding?

- ❍ **A.** Hub
- ❍ **B.** Repeater
- ❍ **C.** Bridge
- ❍ **D.** Switch

17. With a 10Mbps ethernet LAN, dedicated bandwidth enables a switch port to guarantee what data transmission speed?

- ❍ **A.** 10Mbps
- ❍ **B.** 100Mbps
- ❍ **C.** 1000Mbps
- ❍ **D.** 10,000Mbps

18. This Data Link protocol eliminates loops that are caused by redundant connections.

- ❍ **A.** CRC
- ❍ **B.** FCS
- ❍ **C.** CSMA/CD
- ❍ **D.** STP

19. This communication mode allows for only one-way data transmissions at any time.

- ❍ **A.** 10Mbps
- ❍ **B.** 100Mbps
- ❍ **C.** Half-duplex
- ❍ **D.** Full-duplex

20. This communication mode allows for simultaneous two-way data transmissions.

- ❍ **A.** 10Mbps
- ❍ **B.** 100Mbps
- ❍ **C.** Half-duplex
- ❍ **D.** Full-duplex

Answers to Review Questions

1. Token-passing is a Data Link protocol that inserts a three-byte token (or special bit pattern) into a frame and passes it around the network in a single direction from one node to another until it forms a complete loop. The node that has possession of the token is the only one that can send data at any given time on that LAN. Because only one node can send data at a time, collisions are avoided.

2. Standardized by the IEEE 802.5 specification

A token-passing media access technology

Set up as a physical ring or physical star topology

Creates a logical ring topology

Speeds are assigned as either 4Mbps or 16Mbps

Utilizes an MSAU rather than a switch or hub

Provides collision-free data transfer

High overhead

3. Developed by ANSI with the ANSI X3T9.5 specification

A token-passing media access technology

Set up as a dual ring topology

Redundant, fault-tolerant network

Speed is 100Mbps

Runs over fiber-optic cable

Not susceptible to EMI

Provides collision-free data transfer

Fault-detection provided by beaconing

High overhead

4. A unicast address identifies the MAC address of an individual LAN or NIC card.

A multicast address forwards a frame to a subset of devices in the same LAN. IEEE ethernet multicast addresses always begin with 0100.5E in hexadecimal format. The last three bytes can be any combination.

A broadcast address sends a frame to all devices in the same LAN. Broadcast addresses are always the same value, which is FFFF.FFFF.FFFF.

5. CSMA/CD or Carrier Sense Multiple Access Collision Detection is an algorithm that sends a jam signal to notify the devices that there has been a collision. The devices then halt transmission for a random back-off time.

6. The primary tasks performed by both bridges and switches are as follows:

The source MAC address of every inbound frame is examined to learn its MAC address.

You can decide whether to forward or filter a frame based on the destination MAC address.

Eliminate loops that are caused by redundant connections by configuring Spanning Tree Protocol (STP).

7. Half-duplex allows for one-way communication, which means that a device can only send or receive a data transmission at any given time. As a part of a shared collision domain, hubs must use half-duplex.

Full-duplex allows for two-way communication, which means that a device can simultaneously send and receive data transmissions. Full-duplex is available with dedicated switch port connections to a single device. If a switch port connection is configured for full-duplex, the CSMA/CD algorithm must be disabled. Also, an ethernet connection set for full-duplex allows for 100% transmission speeds in both directions.

8. Microsegmentation occurs when a switch creates a dedicated path for sending and receiving transmissions with each connected host. Each host then has a separate collision domain and a dedicated bandwidth.

Answers to Exam Questions

1. **D**. IEEE 802.5 defines token ring. Answers A, B, and C are incorrect because IEEE 802.2 defines LLC, 802.3a defines ethernet, and 802.3u defines Fast Ethernet.

2. **C**. ANSI X3T9.5 defines FDDI. Answers A, B, and D are incorrect because they are all IEEE standards. IEEE 802.5 defines token ring, 802.3u defines Fast Ethernet, and 802.2 defines LLC.

3. **A.** Token-passing inserts a three-byte token (or special bit pattern) into a frame and passes it in a single direction from one node to another until it forms a complete loop. Answers B, C, and D are all incorrect because unicast, multicast, and broadcast are all types of ethernet addresses.

4. **B, D.** Token ring and FDDI use token-passing to send frames. Answers A and C are incorrect because Fast Ethernet and Gigabit Ethernet both use 802.3 MAC and 802.2 LLC headers and trailers for framing.

5. **A.** Unicast addresses identify the MAC address of an individual LAN or NIC card. Answer B is incorrect because multicast addresses send a frame to a group of devices in the same LAN. Answer C is incorrect because broadcast addresses send a frame to all the devices in the same LAN. Answer D is incorrect because a token is a special bit pattern used with token-passing networks.

6. **A, D.** Both 0000.0C12.3456 and 0200.1111.1111 are unicast addresses. 0000.0C is Cisco's OUI. Answers B and C are incorrect because 0100.5E12.3456 is a multicast address and FFFF.FFFF.FFFF is a broadcast address.

7. **B.** Multicast addresses send a frame to a subset of devices in the same LAN. Answer A is incorrect because unicast addresses identify the MAC address of an individual LAN or NIC card. Answer C is incorrect because broadcast addresses send a frame to all the devices in the same LAN. Answer D is incorrect because a token is a special bit pattern used with token-passing networks.

8. **B.** 0100.5E12.3456 is a multicast address. Multicast addresses always start with 0100.5E. Answers A and D are incorrect because both 0000.0C12.3456 and 0200.1111.1111 are unicast addresses. Answer C is incorrect because FFFF.FFFF.FFFF is a broadcast address.

9. **C.** Broadcast addresses send a frame to all the devices in the same LAN. Answer A is incorrect because unicast addresses identify the MAC address of an individual LAN or NIC card. Answer B is incorrect because multicast addresses send a frame to a subset of devices in the same LAN. Answer D is incorrect because a token is a special bit pattern used with token-passing networks.

10. **C.** Broadcast addresses are always represented as FFFF.FFFF.FFFF. Answers A and D are incorrect because both 0000.0C12.3456 and 0200.1111.1111 are unicast addresses. Answer B is incorrect because 0100.5E12.3456 is a multicast address.

11. **B.** Frames are used by the Data Link layer to transport data between the Network and Physical layer. Framing is the process of interpreting data that is either received or sent out across the network. Answers A, C, and D are incorrect because bits are used at the Physical layer, packets are used at the Network layer, and segments are used at the Transport layer of the OSI model.

12. **D.** The frame check sequence (FCS) field of a frame uses a mathematical formula to determine whether any bit errors occurred during data transmission. Answer A is incorrect because Service Access Point (SAP) identifies the upper-layer protocol such as IP. Answer B is incorrect because DSAP is the destination SAP or destination upper-layer protocol. Answer C is incorrect because SSAP is the source SAP or the source upper-layer protocol.

13. **B, C.** IEEE 802.3ab and 802.3z define Gigabit Ethernet standards. Answers A and D are incorrect because 802.3u defines the Fast Ethernet standard, and 802.3ae defines the 10 Gigabit Ethernet standard.

14. **A.** Collision domains are increased with the addition of bridges or switches on a network. Answer B is incorrect because routers create additional broadcast domains. Answers C and D are incorrect because unicast and multicast are both addresses used by ethernet.

15. **C.** The source MAC address of an incoming frame is examined by a bridge or switch to learn the MAC address for the bridge table. Answers A and B are incorrect because multicast and broadcast addresses can never be the source MAC address. Answer D is incorrect because the destination MAC address is not used by a bridge or switch to create the bridge table.

16. **D.** Switches use ASIC hardware chips for frame forwarding. Answers A and B are incorrect because hubs and repeaters do not forward frames because they are Physical layer or Layer 1 devices. Answer C is incorrect because bridges use software for frame forwarding.

17. **A.** 10Mbps is guaranteed with dedicated bandwidth on a 10Mbps ethernet LAN. Answers B, C, and D are incorrect because other speeds of 100, 1000, and 10,000Mbps are all faster speeds that require a different ethernet LAN standard.

18. **D.** Spanning Tree Protocol (STP) is a Data Link protocol that eliminates loops caused by redundant connections on a LAN. Answers A and B are incorrect because cyclical redundancy check (CRC) and frame check sequence (FCS) both provide error detection. Answer C is incorrect because CSMA/CD is an algorithm that is used for arbitration on an ethernet network.

19. **C.** Half-duplex allows for only one-way data transmissions at any time. Answers A and B are incorrect because 10Mbps and 100Mbps are speed classifications primarily associated with ethernet LANs. Answer D is incorrect because full-duplex allows for two-way data transmissions.

20. **D.** Full-duplex allows for simultaneous two-way data transmissions. Answers A and B are incorrect because 10Mbps and 100Mbps are speed classifications primarily associated with ethernet LANs. Answer C is incorrect because half-duplex allows for only one-way data transmissions at any time.

Suggested Readings and Resources

The following are some recommended readings for LAN networking and related terminology:

1. "TechEncyclopedia," www.techweb.com/encyclopedia.
2. "RFC 1700," www.isi.edu/in-notes/rfc1700.txt.

3. "Layer 1 & 2," www.hojmark.net/layer1-2.html#lan.

4. "Cisco Long-Reach Ethernet," www.cisco.com/warp/public/779/servpro/solutions/long_ethernet/.

5. Barnes, David and Sakandar, Basir. *Cisco LAN Switching Fundamentals*. Cisco Press, 2004.

CHAPTER 4

IP at the Network Layer

Objectives

This chapter covers the following Cisco-specified objective for the "Planning and Designing" section of the CCNA exam:

Design an IP addressing scheme to meet design requirements

- To design an IP addressing scheme, you must first understand IP address formats and IP subnetting. Cisco expects a qualified CCNA candidate to determine the best solution for addressing a network when given a set list of design requirements.

Outline

Study Strategies

- List the characteristics of IPv4.
- Make sure you know how to convert binary to decimal.
- Make sure you know how to convert decimal to binary.
- Make sure you know how to convert decimal to hexadecimal.
- Identify IP address classes, including their networks and hosts, and the IP range value of the first octet of each class.
- Define subnet masks and the IP subnet mask format.
- Describe CIDR notations and how to determine the CIDR notation based on the subnet mask.
- Define RFC 1918, NAT, and PAT.
- Make sure you know how to calculate hosts and networks in a subnet.
- Determine the Network ID, Broadcast IP, and valid IP range of a subnet.
- Name the devices that are used at the Network layer and important traits of each device.

Introduction

This chapter elaborates on the fundamental concepts that you learned about the Network layer or Layer 3 of the OSI model in Chapter 1, "Standard Internetworking Models." It reviews the primary functions of the Network layer and then moves right into IP addressing and formats. After you are familiar with address formats and how to convert between them, it reviews subnetting. No matter whether you decide to take the one- or two-test approach to the CCNA certification, you have to know IP address formats and subnetting. They are integral concepts to any Cisco certification. Finally, this chapter discusses network devices that are used at the Network layer, which are routers and Layer 3 switches.

Network Layer Functions

The Network layer of the OSI model serves two primary functions:

- Determines the best path selection for a packet based on a logical or virtual address on the network (routing)
- Handles ICMP, ARP, and Proxy ARP requests

First, best path determination is made at the Network layer for packet delivery across the network. Routed protocols such as IP are used to define logical addressing, which can identify the destination of a packet or datagram. Logical addresses used for routing consist of network and host bits. Routers also must determine the path through the internetwork for packet transmission. This is similar to how switches use a MAC address and interface for frame delivery. Routers also use an interface along with the logical or IP address.

Second, the Network layer also handles ICMP, ARP, and Proxy ARP requests on the internetwork. Remember the function of each protocol for the CCNA exam.

Internet Control Messaging Protocol (ICMP) is used by ping and traceroute utilities. Packet Internet Groper (ping) enables you to validate that an IP address exists and can accept requests.

- Ping is an echo and the response is an echo response.
- Routers send Destination Unreachable messages when they can't reach the destination network and they are forced to drop the packet. The router that drops the packet sends the ICMP DU message.

A traceroute traces the route or path taken from a client to a remote host. Traceroute also reports the IP addresses of the routers at each next hop on the way to the destination. This is especially useful when you suspect that a router on the route to an unreachable network is responsible for dropping the packet.

Address Resolution Protocol (ARP) maps a known IP address to a MAC address by sending a broadcast ARP. When the destination IP address is on another subnet, the sender broadcasts ARP for the router's ethernet port or default gateway, so the MAC address sent back will be that of the router's ethernet port.

Reverse ARP (RARP) maps a known MAC address to an IP address.

Proxy ARP enables a router to respond to an ARP request that has been sent to a remote host. Some Unix machines (especially Solaris) rely on Proxy ARP versus default gateways.

IP Addressing and Formats

Objective:

Design an IP addressing scheme to meet design requirements

Internet Protocol (IP) uses logical or virtual addressing to get a packet from a source to its destination. At the Network layer, routers use IP addresses to make best path forwarding decisions. Public IP addresses are used for packets destined for the outside world, whereas private addresses can be used if the packet needs to traverse only an internal network. The CCNA course focuses on IP version 4 (IPv4). The addresses themselves are assigned by the Internet Assigned Numbers Authority (IANA) to individual organizations based on a request for IP address space. Because the total number of IPv4 addresses is not infinite, strict guidelines are placed on IP space requests to ensure that they are justifiable.

IPv4 addresses

- Consist of 32-bits.
- Are broken down into four octets (8 bits each).
- Use dotted decimal format: for example, 172.16.122.204.
- Have a minimum value (per octet) of 0 and a maximum value of 255.
- Have a Network ID of 0.0.0.0.
- Have a Broadcast IP of 255.255.255.255.

Another IP version was created in the event that the IP space from IPv4 is exhausted. That version is called IP version 6 (IPv6). IPv6 has emerged in the Cisco professional-level exams and may appear on a future CCNA exam. For this reason, IPv6 is introduced in Appendix A, "Future Exam Topics."

Binary

To understand IP addressing, you must first understand binary. Binary is a computer language that is represented by a bit value of 0 or 1. A 32-bit binary address would resemble 10101010101010101010101010101010. Those 32 bits can be grouped into 4 octets, or 10101010 10101010 10101010 10101010, for conversion to decimal format. When the bit value is 1, the bit is considered to be on and you can calculate its binary value depending on its placement within the binary octet. When the bit value is 0, the bit is off and has no corresponding binary value. Figure 4.1 displays the binary value and the calculated decimal value of each bit within an octet. Notice that the binary value increases exponentially.

Binary Value	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal Value	128	64	32	16	8	4	2	1

FIGURE 4.1 A list of binary and decimal conversion values.

Converting Binary to Decimal

By using the value calculated for each bit you can easily convert to decimal format. Line up the binary octet with the decimal value that was calculated in Figure 4.1. To calculate the total decimal value of each octet, you would add up the binary value of each bit that is on (1).

The example in Table 4.1 uses binary octet 00000000.

TABLE 4.1 Example #1 of a Binary-to-Decimal Conversion

Bit Value	0	0	0	0	0	0	0	0
Decimal Value	128	64	32	16	8	4	2	1

In this case, all the bit values are off (0), so there is no corresponding decimal value. The IP address octet value is also 0.

Table 4.2 uses binary octet 00010001.

TABLE 4.2 Example #2 of a Binary-to-Decimal Conversion

Bit Value	0	0	0	**1**	0	0	0	**1**
Decimal Value	128	64	32	**16**	8	4	2	**1**
				16				**1**

In this example, the fourth and last bit values are 1. Add the decimal values to get the total decimal value of that octet. That is, the total decimal value = 17 (16 + 1).

Table 4.3 uses binary octet 11111111.

TABLE 4.3 Example #3 of a Binary-to-Decimal Conversion

Bit Value	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
Decimal Value	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

In Table 4.3, the total decimal value = 255 (128 + 64 + 32 + 16 + 8 + 4 + 2 + 1).

In this case, all the bit values are on (1), so all the decimal values are added together to calculate the IP address octet. The IP address octet value is 255.

Now, you can convert a 32-bit binary address into a dotted decimal address. In this example the binary address is 10101010 01010101 11000011 00111100. Start with the first octet 10110000. Table 4.4 shows the conversion of 10101010 from binary to decimal value.

TABLE 4.4 Binary-to-Decimal Conversion of 10101010

Bit Value	**1**	0	**1**	**1**	0	0	0	0
Decimal Value	**128**	64	**32**	**16**	8	4	2	1
	128		**32**	**16**				

In Table 4.4, the total decimal value = 176 (128 + 32 + 16).

The second octet is 01010101. Table 4.5 shows the conversion of 01010101 from binary to decimal value.

TABLE 4.5 Binary-to-Decimal Conversion of 01010101

Bit Value	0	**1**	0	**1**	0	**1**	0	**1**
Decimal Value	128	**64**	32	**16**	8	**4**	2	**1**
		64		**16**		**4**		**1**

In Table 4.5, the IP octet value = 85 (64 + 16 + 4 + 1).

The third octet is 11000011. Table 4.6 shows the conversion of 11000011 from binary to decimal value.

TABLE 4.6 Binary-to-Decimal Conversion of 11000011

Bit Value	**1**	**1**	0	0	0	0	**1**	**1**
Decimal Value	**128**	**64**	32	16	8	4	**2**	**1**
	128	**64**					**2**	**1**

In Table 4.6, the total decimal value = 195 (128 + 64 + 2 + 1)

The fourth and final octet is 00111100. Table 4.7 shows the conversion of 00111100 from binary to decimal value.

TABLE 4.7 Binary-to-Decimal Conversion of 00111100

Bit Value	0	0	**1**	**1**	**1**	**1**	0	0
Decimal Value	128	64	**32**	**16**	**8**	**4**	2	1
			32	**16**	**8**	**4**		

In Table 4.7, the total decimal value = 60 (32 + 16 + 8 + 4).

Based on these calculations, the IP address in dotted decimal format is 176.85.195.60.

EXAM ALERT

Whenever the last bit is 1, the decimal value is an odd number. Whenever the last bit is 0, the decimal value is an even number. The CCNA exam often uses multiple-choice questions, so you may be able to narrow down the possible correct answers quickly with this hint.

Challenge

In this challenge, you are given a bit value for four octets. You need to fill out the corresponding decimal value and then calculate the total decimal value. After you have converted all four octets, you need to fill out the IP address in dotted decimal format.

Bit Value	1	1	1	0	1	0	1	0
Decimal Value								

Total Decimal Value = _____

Bit Value	0	1	1	0	1	1	0	1
Decimal Value								

Total Decimal Value = _____

Bit Value	0	0	1	0	1	1	0	0
Decimal Value								

Total Decimal Value = _____

Bit Value	1	0	1	0	1	1	1	1
Decimal Value								

Total Decimal Value = _____

The IP Address in dotted decimal format is _____._____._____._____.

Converting Decimal to Binary

You must also be able to convert an IP address from dotted decimal format into binary. It helps to work from left to right when converting to binary.

Example IP address = 206.110.28.62

The first octet of 206 can be broken down as follows:

128	**64**	32	16	**8**	**4**	**2**	1
1	1	0	0	1	1	1	0

The octet value is greater than 128, so the first bit is on. Subtract 128 from 206.

206 – 128 = 78

The remainder 78 is greater than 64, so the second bit is also on.

78 – 64 = 14

The remainder 14 is less than 32 and 16, so the third and fourth bits are off. However, 14 is greater than 8, so the fifth bit is on.

14 – 8 = 6

The remainder 6 is greater than 4, so the sixth bit is on.

6 – 4 = 2

The remainder 2 is equal to the seventh bit value, so that bit is also on.

2 – 2 = 0

The last bit value is off because the remainder is 0. Remember that it is an even number, so the last bit will always be 0!

Challenge

You've already converted the first octet of 206.110.28.62 into binary. Determine the appropriate bit value for the remaining three octets.

Second octet 110:

128	64	32	16	8	4	2	1
___	___	___	___	___	___	___	___

Third octet 28:

128	64	32	16	8	4	2	1
___	___	___	___	___	___	___	___

Fourth octet 62:

128	64	32	16	8	4	2	1
___	___	___	___	___	___	___	___

Now that you all four quartets have been converted, the binary equivalent of 216.110.28.62 is 11001110 _____ _____ _____.

Hexadecimal

Hexadecimal is a numbering system with a base of 16. Numbers 0–9 represent the first 10 decimal digits and the next 6 digits are the letters A–F. Each hexadecimal character is equal to four bits. Hexadecimal format was first introduced in Chapter 1, during the discussion of MAC addresses at the Data Link layer. Figure 4.2 shows the decimal values 0–15 and their equivalent hexadecimal values.

Decimal Value	0-9	10	11	12	13	14	25
Hexadecimal Value	0-9	A	B	C	D	E	F

FIGURE 4.2 Decimal-to-hexadecimal conversions.

Converting Decimal to Hexadecimal

There are two ways to calculate hexadecimal from decimal format. With the first method, the decimal value should first be converted to binary format.

Decimal value = 141

128	64	32	16	8	4	2	1
1	0	0	0	1	1	0	1

Binary value = 10010001

Now break the binary value into two groups of four bits each, which is 1000 and 1101. Then, line up the four bits with the last four decimal values that were calculated in Figure 4.1. Again, add up the binary value of each bit that is on (1).

1	0	0	0	
8	4	2	1	
8				The combined value is 8 so the hexadecimal character = 8
1	**1**	0	**1**	
8	**4**	2	**1**	
8	**4**		**1**	The combined value is 13 so the hexadecimal character = D

The combined hexadecimal address is 0x8D.

The second method for calculating a hexadecimal address is to divide the decimal number by 16 first. So, 141 divided by 16 equals 8 with a remainder of 13, which matches the results from the binary conversion in the first method.

NOTE

Recall how 8 bits for an octet equals one byte. Well, when you divide an octet into two hexadecimal fields of 4 bits each, each 4-bit field is called a *nibble*.

Challenge

Here are several decimal values. Calculate the hexadecimal value, using Figure 4.2 as a guideline.

Decimal Value	Hexadecimal Value
210	
193	
245	
161	

IP Address Classes

As you know, IP addresses are 32 bits long, represented by dotted decimal notation. Each address can be divided into two parts:

- Network
- Host

The number of network octets and host octets determines the IP address class. Table 4.8 shows the three IP defined network classes.

TABLE 4.8 IPv4 Address Classes

	1st Octet	2nd Octet	3rd Octet	4th Octet
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host

TCP/IP defines two additional address classes:

- **Class D**—Used for multicast addresses
- **Class E**—Used for research purposes

Table 4.9 lists the possible values each class network can have in the first octet. With these values you can easily identify what class network is being referenced on the exam.

TABLE 4.9 Address Class Ranges

Class	1st Octet Decimal Range
A	1–126
B	128–191
C	192–223
D	224–239
E	240–255

NOTE

The 127.x.x.x address range is reserved for loopback addresses.

EXAM ALERT

Memorize the decimal range for the first octet of each address class.

The network portion of an address maintains the same value for all the IP addresses that are assigned from a Class A, B, or C network. Remember that one octet is equal to eight bits or

one byte. The Class A network portion is one byte, and the host portion takes up the remaining three bytes. The Class B network portion is two bytes, with the remaining two bytes making up the host portion. The Class C network portion is three bytes, whereas the host portion is one byte. It stands to reason that if fewer bytes are devoted to the network portion of an address, fewer networks are possible for that class of network. With that said, the same is true for the host portion of an address. The fewer host bytes, the fewer total hosts that are available for that class of network.

When calculating the total number of Class A, B, or C networks available, you must subtract two from the total. This is a Cisco standard implemented for the CCNA exam. A host address must be unique for each device or interface on a network. For each Class A, B, or C network, there is always a network identifier (ID) and a broadcast IP address. For this reason, you must also subtract two to calculate the total number of valid hosts per network.

A *network ID* is the first IP address in a network. This may also be referred to as a *subnet ID*. Every host bit for the network ID address is turned off (or all 0s). An example of a Class A network ID is 16.0.0.0.

A *broadcast IP* is the last IP address in a network. Every host bit for the broadcast IP address is turned on (or all 1s). An example of a Class A broadcast IP is 16.255.255.255.

EXAM ALERT

Power of 2 When you enter the exam room, it's helpful to write some things down on the paper or white board that is supplied. I would suggest writing down the powers of 2 for quick reference when calculating networks and hosts.

Here's a calculation for the number of networks for each class:

$2^7 - 2 = 126$ total Class A networks

$2^{14} - 2 = 16{,}382$ total Class B networks

$2^{21} - 2 = 2{,}097{,}150$ total Class C networks

NOTE

When calculating the total number of Class A, B, or C networks, the exponent is a multiple of 7.

Now you can calculate the number of hosts per network:

For any Class A network,

Network = 1 byte (8 bits)
Host = 3 bytes (24 bits)
$2^{24} - 2 = 16{,}777{,}214$ total hosts per network

For any Class B network,

Network = 2 bytes (16 bits)
Host = 2 bytes (16 bits)
$2^{16} - 2 = 65{,}534$ total hosts per network

For any Class C network,

Network = 3 bytes (24 bits)
Host = 1 byte (8 bits)
$2^{8} - 2 = 254$ total hosts per network

NOTE

When calculating the total number of hosts per network, the exponent is equal to the number of host bits.

Challenge

You will see the terms Class A, B, and C on the CCNA exam. In this challenge, I would like you to fill in the corresponding values for each network class.

Network Class	First Octet Range (Decimal)	Total Networks	Total Hosts per Network
A			
B			
C			

Subnet Masks

Sub-networks (subnets) enable you to break a large network of IP addresses down into smaller, manageable address ranges. A smaller address range means fewer hosts on a network. Each subnet becomes a separate broadcast domain. All the devices that are in the same broadcast

domain receive all broadcasts. Think if it were possible to have all 16,777,214 Class A network hosts sharing a broadcast domain and receiving all broadcasts. That would be a huge amount of traffic. Subnets enable you to break this large network into smaller address ranges. In this case, smaller is better.

A subnet mask is used to identify which part of an IP address is the network portion. Like the IP address itself, a subnet mask consists of 32 bits. The network portion is represented by all 1s.

The default subnet masks for Class A, Class B, and Class C networks are as follows:

- **Class A**—255.0.0.0 (11111111 00000000 000000000 000000000)
- **Class B**—255.255.0.0 (111111111 1111111111 000000000 000000000)
- **Class C**—255.255.255.0 (111111111 1111111111 111111111 0000000000)

Now that you know what an IP address and subnet mask are, there is a mathematical operation called Boolean AND that helps to identify some important aspects of an IP network. With Boolean AND you can determine the network ID and broadcast IP given an IP address and subnet mask.

Boolean AND works as follows:

- Determines the binary value of the IP address.
- Determines the binary value of the subnet mask.
- Lines up both binary values one on top of the other.
- If the lined-up bit values in both addresses equal 1, the Boolean bit is also 1.
- If the lined-up bit values in both addresses do not equal 1, the Boolean bit is 0.

Table 4.10 provides a Boolean example. The decimal IP address value = 124.0.0.0, and the subnet mask = 255.0.0.0.

TABLE 4.10 Boolean AND Example #1

IP Address Binary	01111100	00000000	00000000	00000000
Subnet Mask Binary	11111111	00000000	00000000	00000000
Boolean AND	01111100	**00000000**	**00000000**	**00000000**

The network ID in this example is 124.0.0.0. Using Boolean you can see that the host bits in the last three octets are 0 bits, which identifies the network ID. I emphasized the last host octet in Table 4.10. If you turn all of those host bits on, you will get the broadcast IP, which in this case is 124.255.255.255.

For the next example (Table 4.11), the decimal IP address value = 135.252.4.0, and the subnet mask = 255.255.0.0.

TABLE 4.11 Boolean AND Example #2

IP Address Binary	10000111	11111100	00000100	00000000
Subnet Mask Binary	11111111	11111111	00000000	00000000
Boolean AND	10000111	11111100	**00000000**	**00000000**

The network ID in this example is 135.252.0.0. Using Boolean you can see that the host bits in the last two octets are 0 bits, which identify the network ID. I emphasized both host octets in the example. If you were to turn all those host bits on, you would get the broadcast IP, which in this case is 135.252.255.255.

Classless Interdomain Routing (CIDR) notation may also be used to identify the subnet mask. The mask is written in slash notation as follows:

- **Class A**—/8
- **Class B**—/16
- **Class C**—/24

EXAM ALERT

The CIDR notation or prefix notation for each network class can be determined by counting the 1s in binary or the number of bits that make up the network portion of the address.

Challenge

In this challenge, please fill in the appropriate default subnet mask and CIDR notation for each network class.

Network Class	Subnet Mask (Decimal)	CIDR Notation
A		
B		
C		

Private (RFC 1918) Addressing

The previously listed Class A, B, and C addresses are all IANA assigned public IP addresses. Although it originally seemed that there was sufficient public IPv4 address space available,

resources began being consumed quickly. I mentioned that IPv6 was developed in the event that IPv4 address space became exhausted. Other measures were also implemented to alleviate the shortage of IPv4 public IP address space. These measures include RFC1918, Network Address Translation (NAT), and Port Address Translation (PAT). RFC 1918 defines private IP address space. Private address space can be used for traffic that does not need to leave the internal network. Because this traffic is internal to the network, it does not matter if other organizations are using the same address space. Private IP addresses are not routable on the Internet.

IANA Private Address Space Allocations include the following IP address ranges for Class A, Class B, and Class C networks:

- **Class A**—10.0.0.0–10.255.255.255
- **Class B**—172.16.0.0–172.31.255.255
- **Class C**—192.168.0.0–192.168.255.255

NAT translates one IP address to another. Typically this is done between private and public IP addresses. For example, a private IP address can be translated with NAT to a public IP address for outbound transmission to the Internet. NAT can also translate a public IP address to a private IP address for inbound transmission on the internal network. PAT can translate multiple addresses on an internal network to a single public IP address, which is called one-to-many address translation. PAT is available as NAT overloading on Cisco routers.

NOTE

Chapter 14, "Network Address Translation," covers NAT terminology and configurations in detail.

Subnetting IP

So far, we have focused on the network classes and key characteristics of each one. As I mentioned, each network class can also be broken down into smaller groups of IP address ranges or subnets. *Subnetting* is the process of breaking down those larger IP networks into smaller sub-networks. At first, subnetting IP might seem like a daunting task, but it's not that bad after you get the hang of it. In this section you need to pull together all the knowledge that you have learned so far about binary, decimal, and subnets.

First, let's get the easy subnetting out of the way.

For an IP address that has a 255.255.0.0 or 255.255.255.0 subnet mask, you can copy the octets that have a subnet mask value of 255 from the original IP address. For the remaining octets, you will put down a 0. Here's an example:

IP address = 139.42.6.0

Subnet Mask = 255.255.0.0

The Network ID is 139.42.0.0.

To determine the Broadcast IP of this IP address and subnet mask, just replace the 0 octets from the Network ID with 255.

The Broadcast IP is 139.42.255.255.

EXAM ALERT

When a subnet mask has a value of 255.255.0.0 or 255.255.255.0, you can copy the original IP octets that match the 255 value subnet octets and then use 0 for any remaining octets to determine your Network ID. The Broadcast IP is the same original IP octets that match the 255 value subnet octets and the number 255 rather than 0 for the remaining octet(s).

To understand more difficult subnetting, you need to break down an IP address into network bits, host bits, and subnet bits. The network bits are determined by the network class. Class A has 8 network bits, Class B has 16 network bits, and Class C has 24 network bits. The network bits value is a constant. The host bits, on the other hand, must share space with the subnet bits. To determine the subnet bits for a network you need to look at the subnet mask in binary. For example,

IP address = 176.85.195.60/22

Subnet Mask = 255.255.252.0

Subnet Mask in Binary = 11111111 11111111 11111100 00000000

Network bits = 16

Host bits = 10

Subnet bits = 6

The subnet mask in binary has 22 bits with a value of 1, which means the CIDR notation is /22. Based on the first octet of the IP address you know that this is a Class B network. Class B networks have 16 network bits. That leaves 16 bits in the address. The bits that have a value of 0 determine the number of host bits. In this case there are 10 host bits. The rest of the bits are the subnet bits, so there are 6 subnet bits.

Table 4.12 is a conversion table of decimal to binary values that will help you convert addresses more quickly when taking the exam.

TABLE 4.12 Decimal-to-Binary Conversion

Decimal	Binary
0	00000000
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

You can use the chart to figure out more IP address values:

IP address = 100.15.209.0/23
Subnet Mask = 255.255.254.0
Subnet Mask in Binary = 11111111 11111111 11111110 00000000
Network bits = 8
Host bits = 9
Subnet bits = 15
IP address = 128.216.55.0/24
Subnet Mask = 255.255.255.0
Subnet Mask in Binary = 11111111 11111111 11111111 00000000
Network bits = 16
Host bits = 8
Subnet bits = 8
IP address = 222.110.8.61/28
Subnet Mask = 255.255.255.240
Subnet Mask in Binary = 11111111 11111111 11111111 11110000
Network bits = 24
Host bits = 4
Subnet bits = 4

Challenge

In this challenge, I supply you with the IP address and subnet mask. From there, you need to convert the subnet mask to binary and determine the number of network bits, host bits, and subnet bits for each network.

IP address = 193.216.0.0

Subnet Mask = 255.255.248.0

Subnet Mask in Binary = _____ _____ _____ _____

Network bits = _____

Host bits = _____

Subnet bits = _____

IP address = 130.101.2.0

Subnet Mask = 255.255.255.128

Subnet Mask in Binary = _____ _____ _____ _____

Network bits = _____

Host bits = _____

Subnet bits = _____

Calculating Hosts in a Subnet

To calculate the hosts in a subnet, we can use the formula $2^H - 2$. The exponent *H* represents the number of host bits in a network. If you use the subnetting examples, you can determine the hosts in each subnet:

IP address = 176.85.195.60/22

Subnet Mask = 255.255.252.0

Network bits = 16

Host bits = 10

Subnet bits = 6

$2^{10} - 2 = 1022$ Hosts

IP address = 100.15.209.0/23

Subnet Mask = 255.255.254.0

Network bits = 8

Host bits = 9

Subnet bits = 15

$2^9 - 2 = 510$ Hosts

IP address = 128.216.55.0/24

Subnet Mask = 255.255.255.0

Network bits = 16

Host bits = 8

Subnet bits = 8

$2^8 - 2 = 254$ Hosts

IP address = 222.110.8.61/28

Subnet Mask = 255.255.255.240

Network bits = 24

Host bits = 4

Subnet bits = 4

$2^4 - 2 = 14$ Hosts

EXAM ALERT

The formula to calculate the number of hosts created is $2^H - 2$. The *H* represents the host bits in a network.

Challenge

In the last challenge, you figured out the network bits, host bits, and subnet bits for two different IP address subnets. In this challenge, please take that information and calculate the number of hosts in each subnet.

IP address = 193.216.0.0

Subnet Mask = 255.255.248.0

Network bits = _____

Host bits = _____

Subnet bits = _____

Hosts = _____

IP address = 130.101.2.0

Subnet Mask = 255.255.255.128

(continues)

(continued)

Network bits = _____

Host bits = _____

Subnet bits = _____

Hosts = _____

Calculating Networks in a Subnet

To calculate the networks in a subnet, you can use the formula $2^N - 2$. The exponent *N* represents the number of subnet bits in a network. You can figure out the number of networks in each subnet with the formula.

IP address = 176.85.195.60/22

Subnet Mask = 255.255.252.0

Network bits = 16

Host bits = 10

Subnet bits = 6

$2^6 - 2 = 62$ Networks

IP address = 100.15.209.0/23

Subnet Mask = 255.255.254.0

Network bits = 8

Host bits = 9

Subnet bits = 15

$2^{15} - 2 = 32{,}766$ Networks

IP address = 128.216.55.0/24

Subnet Mask = 255.255.255.0

Network bits = 16

Host bits = 8

Subnet bits = 8

$2^8 - 2 = 254$ Networks

IP address = 222.110.8.61/28

Subnet Mask = 255.255.255.240

Network bits = 24

Host bits = 4

Subnet bits = 4

$2^4 - 2 = 14$ Networks

EXAM ALERT

The formula to calculate the number of networks or subnets created is $2^N - 2$. The *N* represents the subnet bits in a network.

Challenge

In this challenge, please use the subnet bit value that you calculated and determine the number of networks in each subnet.

IP address = 193.216.0.0

Subnet Mask = 255.255.248.0

Network bits = _____

Host bits = _____

Subnet bits = _____

Subnets = _____

IP address = 130.101.2.167

Subnet Mask = 255.255.255.224

Network bits = _____

Host bits = _____

Subnet bits = _____

Subnets = _____

Zero Subnet Rule

Zero subnet may also be referred to as *subnet zero*. The zero subnet is the first subnet in a network and has all binary 0s in the subnet field. For the purpose of taking the CCNA exam, you should not include the first subnet when calculating the number of networks in a larger subnet. This is one of the two reserved subnet numbers on a network and one of the reasons why you subtract from the total number of networks to get the correct answer for the test. The other network is the broadcast subnet, which has all 1s in the subnet field.

The Increment

We have been working with the IP address subnet 222.110.8.61/28. After you know how many subnets and hosts are in a subnet, you can determine the network ID for that subnet. So far,

you know that 222.110.8.61/28 has 14 hosts and 14 subnets. Before subtracting 2 for the valid number of hosts/networks, your calculations were for 16 hosts and 16 networks. This means that a subnet with a 255.255.255.240 mask is part of a larger subnet with a 16-host increment. The variable part of this subnet is the last octet. So you can automatically write down the first three octets as follows:

222.110.8.*x* (where the *x* is variable and has a 16-host increment)

Octet values range from 0–255. So the first subnet in the larger network is 222.110.8.0. Now you want to add increments of 16 to the last octet, so you get the following networks:

222.110.8.0 (zero subnet—not valid for the CCNA exam)
222.110.8.16
222.110.8.32
222.110.8.48
222.110.8.64
222.110.8.80
222.110.8.96
222.110.8.112
222.110.8.128
222.110.8.144
222.110.8.160
222.110.8.176
222.110.8.192
222.110.8.208
222.110.8.224
222.110.8.240 (broadcast subnet—not valid for the CCNA exam)

This is a list of the Network IDs in that Class C network with a subnet of 255.255.255.240. The Network ID is always an even number. There are 16 total subnets. According to the zero subnet and broadcast subnet rule, the first and last subnet cannot be used. The IP address 222.110.8.61 is greater than 48 and less than 64, so the Network ID or subnet number for 222.110.8.61/28 is 222.110.8.48 (which is highlighted in the list of networks). To get the broadcast IP, subtract 1 from the next Network ID in your list. In this example, the broadcast IP is 222.110.8.63.

There is another math shortcut that can be used to identify the Network ID, which then helps you determine the Broadcast IP. Take another look at 222.110.8.61/28.

IP address = 222.110.8.61

Subnet Mask = 255.255.255.240

Look at the first subnet mask octet from the left that is not a value of 255 and subtract it from 256.

256 – 240 = 16

You want to find the closest multiple of 16 that is less than the last octet in the IP address, which equals 61. You are using the last octet because that is the same octet used from the subnet mask.

16×3 = 48 and 16×4 = 64

Based on the calculations, the Network ID increments are as follows:

222.110.8.48

222.110.8.64

So you use 48 because it is less than 61, and 64 is the Network ID of the next subnet. You come up with the same answer as before.

Network ID = 222.110.8.48

Broadcast IP = 222.110.8.63 (one less than the next Network ID of the next subnet)

Here's another example:

IP address = 100.15.209.0

Subnet Mask = 255.255.254.0

The first two octets in the subnet mask equal 255, so you need to use the first octet that is not equal to 255, or in this case the third octet from the left. Now you can subtract 254 from 256.

256 – 254 = 2

2×104 = 208

2×105 = 210

You can see that the valid network ID less than 209 is 208. The next network ID equals 210, so you can fill out the third octet with each value to obtain the following network ID increments:

100.15.208.0

100.15.210.0

For IP address 100.15.209.0 with a subnet mask of 255.255.254.0, you now know the Network ID is 100.15.208.0. The next network is 100.15.210.0, so you want to find the last IP address before that network ID to get the Broadcast IP. Because the value of an octet can range from 0–255, the last possible IP before 100.15.210.0 is 100.15.209.255.

Network ID = 100.15.208.0

Broadcast IP = 100.15.209.255

Challenge

Part I:

To help you understand incremental values, make a list of the subnet increments for address 130.101.2.167 with a subnet mask of 255.255.255.224. I will fill in the first and last network ID (neither are valid networks per the CCNA exam).

130.101.2.0

_____

_____

_____

_____

_____

_____

130.101.2.224

What is the Network ID of 130.101.2.167/27? _____

What is the Broadcast IP of 130.101.2.167/27? _____

Part II:

Given the following IP address and subnet mask, use the shortcut method to determine the Network ID and Broadcast IP.

IP address = 176.85.195.60

Subnet Mask = 255.255.252.0

Determining the Range of Valid IPs

The range of valid IP addresses in a subnet is the first IP address after the Network ID and the last IP address before the Broadcast IP address. If you are given the following IP address and subnet mask, you can determine the range of valid IP addresses:

IP Address = 210.189.16.0

Subnet Mask = 255.255.255.0

First, identify the Network ID, which in this case is 210.189.16.0. Then determine the Broadcast address, which is 210.189.16.255. In this case the valid IP range is 210.189.16.1–210.189.16.254.

Here are some more examples where the Network ID and Broadcast IP have already been determined:

IP address = 100.15.209.0

Subnet Mask = 255.255.254.0

CIDR = /23

Network ID = 100.15.208.0

Broadcast IP = 100.15.209.255

Valid IP range = 100.15.208.1–100.15.209.254

IP address = 222.110.8.61

Subnet Mask = 255.255.255.240

CIDR = /28

Network ID = 222.110.8.48

Broadcast IP = 222.110.8.63

Valid IP range = 222.110.8.49–222.110.8.62

EXAM ALERT

The valid range of IP addresses always starts with an odd number and ends with an even number.

Challenge

In this challenge I have supplied the IP address and subnet mask. First, calculate the binary equivalent of the subnet mask. Then determine the CIDR notation. After you have these fields completed, calculate the Network ID and Broadcast IP, using the shortcut provided for subnetting. After you identify the Network ID and Broadcast IP, you can determine the valid IP host range.

IP Address	172.17.8.122
Subnet Mask	255.255.255.224
Binary Subnet Mask	

(continues)

(continued)

CIDR Notation
Network ID
Broadcast IP
Valid IP Range

It is important to understand the general concepts related to IP addressing and subnetting. Figure 4.3 is a chart or quick sheet that will help you check your answers and provide you a guideline for the CCNA exam. I suggested that you memorize the powers of 2. I also suggest that you memorize this chart and write it down on your scrap paper or white board when you start the exam. I found it to be extremely helpful!

Binary Increment	128	64	32	16	8	4	2	1
Subnet Mask	128	192	224	240	248	252	254	255
CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Hosts-2	32768	16384	8192	4096	2048	1024	512	256
Class B Networks-2	2	4	8	16	32	64	128	256
Class C Networks-2								

128	64	32	16	8	4	2	1
128	192	224	240	248	252	254	255
/25	/26	/27	/28	/29	/30	/31	/32
128	64	32	16	8	4	2	0
512	1024	2048	4096	8192	16384	32768	65536
2	4	8	16	32	64	128	256

FIGURE 4.3 Subnetting quick sheet.

Network Layer Devices

The most common network device found at the Network layer is a router; however, Layer 3 switches may also be implemented to create a WAN.

Both routers and Layer 3 switches can carry out these functions:

- Suppress broadcasts or multicasts
- Determine the best path for data transfer (routing)
- Strip down and add to Data Link layer frames
- Implement access lists for packet filtering (permit/deny statements)
- Set up quality of service (QoS) qualifiers to measure network performance

It is important to know that both these devices can be used at the Network layer. However, for the purpose of the CCNA exam, routers are more widely recognized and, therefore, are referred to when discussing Layer 3 functions.

Routers

Routers join a minimum of two networks together to create a WAN. So far, we have discussed devices that are used at the Physical layer (hubs and repeaters) and the Data Link layer (Layer 2 switches and bridges). Layer 2 switches and bridges create a separate collision domain for each segment of the LAN. Routers and Layer 3 switches create a separate broadcast domain for each segment of a WAN. A broadcast domain is a group of nodes that can receive one another's broadcast messages. Figure 4.4 demonstrates how a router creates broadcast domains whereas the connected switches create collision domains.

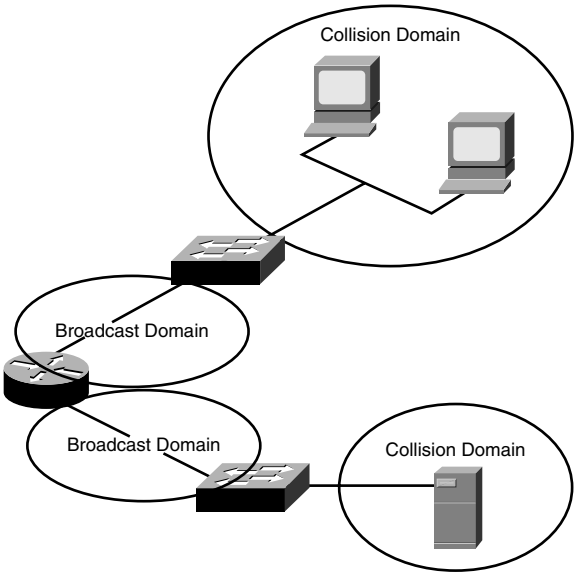


FIGURE 4.4 Broadcast and collision domains.

Figure 4.5 demonstrates a simple LAN with one router and two segments. In this network, any traffic that is generated by Matt's PC has the source MAC and source IP address of that PC. If Matt is sending a frame to the server on the other segment of that WAN, the destination IP address will be that of the server he is trying to reach. Because the server is not on the same segment as Matt, the destination MAC address is that of the router, which is the default gateway. The router takes a look at the frame and at its own routing table. It then decides what

interface to use to forward the frame based on the network portion of the IP address. The router attaches its own MAC address as the source MAC address of the frame before sending the frame to the server.

A routing table on a router contains the following information:

- **Network Address**
- **Interface**—Exit interface used to forward packets
- **Metric**—Distance to reach a remote network

Figure 4.6 exemplifies a WAN with two routers. Each router has a separate routing table to make best path decisions.

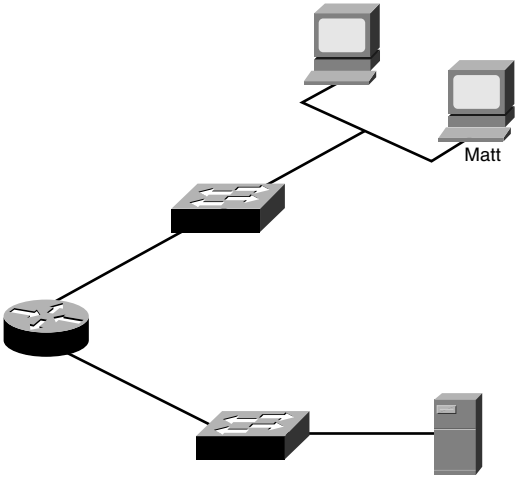
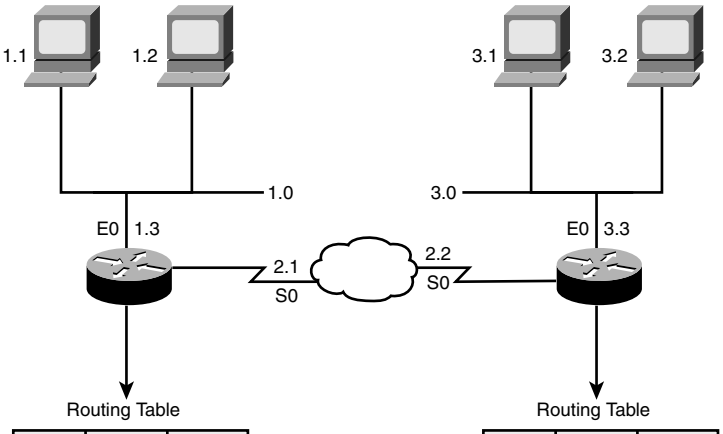


FIGURE 4.5 Frame transmission using a router.

There are two packet types used at Layer 3:

- **Data Packets**—Transport data across the internetwork and are supported by routed protocols such as IP and IPX.
- **Route Update Packets**—Send updates to neighbor routers about all networks connected to that internetwork and are supported by routing protocols such as RIP, EIGRP, and OSPF.



NET	INT	Metric
1	E0	0
2	S0	0
3	S0	1

NET	INT	Metric
1	S0	1
2	S0	0
3	E0	0

FIGURE 4.6 A WAN with routing tables.

NOTE

Specific Cisco router models are reviewed in Chapter 5, "Introduction to Cisco Routers and Switches."

IP configurations are covered in Chapter 7, "Basic Cisco Configurations."

Chapter 10, "Introduction to Routing and Routing Protocols," details routing terminology.

Chapter 11, "Distance Vector Routing Protocols," reviews RIP and IGRP routing protocols.

Chapter 12, "Link-State and Hybrid Routing Protocols," discusses OSPF, RIPv2, and EIGRP routing protocols.

Layer 3 Switches

Layer 3 switches are typically called *multi-layer switches*. I already listed the commonalities between routers and Layer 3 switches. There are also a couple of differences worth mentioning. The number one difference between a router and a Layer 3 switch is packet switching throughput. Whereas a router has evolved over the years to process more than one million packets per second (pps), a Layer 3 switch can process millions of pps. That said, Layer 3 switches process more traffic in a shorter time.

Whereas routers use microprocessor-based engines, Layer 3 switches use ASIC hardware to perform packet switching. Layer 2 switches use ASIC hardware to forward frames.

NOTE

The Cisco Catalyst 8500 series switch is an example of a Layer 3 switch. Layer 3 switches are recommended for Campus networks.

Chapter Summary

Take a deep breath… That was a lot to cover! IP addressing and IP subnetting are vital to studying for the CCNA exam. In fact, they are integral to understanding networking in general. This chapter touched on many of the concepts that are elaborated later in this book. A lot of device configurations are in upcoming chapters. Knowing your IP format and subnet masks is the first big hurdle when working with IP routing protocols such as OSPF and EIGRP. The next chapter introduces Cisco routers and switches as well as other important Cisco network components. You will also be introduced to Cisco IOS, which you will need to understand to configure a Cisco device.

Key Terms

- IPv4 (IP version 4)
- binary
- Network ID
- Broadcast IP
- subnet
- subnetting
- subnet mask
- CIDR (Classless Interdomain Routing)
- Boolean AND
- NAT
- PAT
- zero subnet rule
- broadcast subnet

Apply Your Knowledge

Exercises

4.1 Converting Binary to Decimal

Practice makes perfect! Address conversion is pretty much guaranteed to be on the CCNA exam. I promise you that it is worth your while to go over these exercises until you have the system down pat. I will give you the bit values for four octets. Convert each octet to decimal and fill in the corresponding dotted decimal IP address value.

Keep in mind that the bit values for each octet are

128 64 32 16 8 4 2 1

Estimated Time: 10 minutes

First Octet:

Binary 1 1 0 1 1 0 0 0

Decimal_____

Second Octet:

Binary 0 1 0 1 1 1 1 1

Decimal_____

Third Octet:

Binary 1 0 1 1 1 1 1 1

Decimal_____

Fourth Octet:

Binary 1 1 1 0 0 0 0 0

Decimal_____

IP Address = _____. _____. _____. _____

4.2 Converting Decimal to Binary

Conversions go both ways. Now, I will give you the decimal values for four octets. Convert each octet to binary and fill in the corresponding binary address value.

Estimated Time: 10 minutes

First Octet:

Decimal 224

Binary _____

Second Octet:

Decimal 137

Binary _____

Third Octet:

Decimal 15

Binary _____

Fourth Octet:

Decimal 253

Binary _____

Binary Address = _____ _____ _____ _____

4.3 Converting Decimal to Hexadecimal

You may be asked to determine a hexadecimal value given a decimal value. In this challenge I have given you the decimal value. You need to convert that to binary and then break the binary octet into two 4-bit groups.

Keep in mind that the bit values for each 4-bit group are

8 4 2 1

Also, Figure 4.2 has the decimal-to-hexadecimal values.

Estimated Time: 10 minutes

Decimal = 105

Binary = ____ ____ ____ ____ ____ ____ ____ ____

First 4 bits of the binary octet:

____ ____ ____ ____ = Decimal _____ Hexadecimal_____

Last 4 bits of the binary octet:

____ ____ ____ ____ = Decimal _____ Hexadecimal_____

The combined hexadecimal value is 0x_____.

4.4 Binary Chart

There are several useful memorization tools for the IP subnetting questions on the CCNA exam. Fill in the binary equivalent (one octet) for each of the following decimal values.

Estimated Time: 5 minutes

Decimal	Binary
0	
128	
192	
224	
240	
248	
252	
254	
255	

4.5 Identify the Network ID

In this exercise, please use Boolean AND to determine the Network ID, given the IP address 134.141.7.130 and subnet mask 255.255.255.0.

Estimated Time: 5 minutes

IP Address Binary
Subnet Mask Binary
Boolean AND

Network ID = _____. _____. _____. _____

Review Questions

1. Convert binary 00101010 00111111 11011100 11111111 to decimal format.
2. Convert decimal 150.193.6.100 to binary format.
3. What is hexadecimal 0x5F in decimal format?
4. Perform Boolean AND to define the Network ID of IP address 200.62.183.26 255.255.255.0.
5. Given the IP address 32.116.5.0 and subnet mask 255.255.255.0, what is the Network ID?
6. Given the IP address 213.50.201.0 and subnet mask 255.255.255.0, what is the Broadcast IP?
7. What is the valid IP range for 220.9.3.0/24?
8. Define the zero subnet and broadcast subnet rules.
9. Describe the process of routing.
10. List the functions performed by a router or Layer 3 switch.

Exam Questions

1. What is the decimal equivalent of 10010111 00000110 10101100 01110111?
   - ❍ **A.** 151.6.172.119
   - ❍ **B.** 151.6.172.120
   - ❍ **C.** 151.6.172.121
   - ❍ **D.** 151.6.172.122

2. What is the first octet range for Class B addresses?
   - ❍ **A.** 1–126
   - ❍ **B.** 128–191
   - ❍ **C.** 192–223
   - ❍ **D.** 224–239

3. What is the first octet range for Class C addresses?

- ❍ **A.** 1–126
- ❍ **B.** 128–191
- ❍ **C.** 192–223
- ❍ **D.** 224–239

4. How many hosts are available with a Class C network?

- ❍ **A.** 253
- ❍ **B.** 254
- ❍ **C.** 255
- ❍ **D.** 256

5. What is the network ID for a host with the IP address 124.199.7.18/28?

- ❍ **A.** 124.199.7.0
- ❍ **B.** 124.199.7.16
- ❍ **C.** 124.199.7.32
- ❍ **D.** 124.199.7.48

6. You have been assigned a Class C network address. A coworker has requested that you create 10 networks that can support 10 hosts per network. What subnet mask should you use?

- ❍ **A.** 255.255.255.0
- ❍ **B.** 255.255.255.224
- ❍ **C.** 255.255.255.240
- ❍ **D.** 255.255.255.248

7. Which of the following are valid host addresses in the 208.62.15.0 network with a 255.255.255.224 subnet mask? (Choose the 2 best answers.)

- ❍ **A.** 208.62.15.0
- ❍ **B.** 208.62.15.1
- ❍ **C.** 208.62.15.30
- ❍ **D.** 208.62.15.32

8. Given the network address 192.131.10.0 and subnet mask 255.255.255.0, what is the total number of networks and the total number of hosts per network?

- ❍ **A.** 1 network / 255 hosts
- ❍ **B.** 1 network / 254 hosts
- ❍ **C.** 2 networks / 62 hosts
- ❍ **D.** 6 networks / 30 hosts

9. How many valid host IP addresses are available with a network address of 218.41.99.24 and a subnet mask of 255.255.255.252?

- ❍ **A.** 2
- ❍ **B.** 6
- ❍ **C.** 14
- ❍ **D.** 30

10. If you need at least five subnetworks with a Class C network and you want to have as many hosts as possible on each network, what subnet mask would you use?

- ❍ **A.** 255.255.255.252
- ❍ **B.** 255.255.255.240
- ❍ **C.** 255.255.255.248
- ❍ **D.** 255.255.255.224

11. How many hosts are available with a Class B network?

- ❍ **A.** 254
- ❍ **B.** 64,000
- ❍ **C.** 65,534
- ❍ **D.** 16,777,214

12. What is the Broadcast IP for 196.23.250.32/27?

- ❍ **A.** 196.23.250.32
- ❍ **B.** 196.23.250.33
- ❍ **C.** 196.23.250.63
- ❍ **D.** 196.23.250.64

13. What subnet mask would you use if you had a Class B address and you would like 250 networks?

- ❍ **A.** 255.255.255.0
- ❍ **B.** 255.255.254.0
- ❍ **C.** 255.255.252.0
- ❍ **D.** 255.255.248.0

14. How many subnets can you have with subnet mask of 255.255.240 on a Class B network?

- ❍ **A.** 6
- ❍ **B.** 14
- ❍ **C.** 16
- ❍ **D.** 30

15. How many hosts are available if you have a Class B network with a subnet mask of 255.255.255.128?

- ❍ **A.** 254
- ❍ **B.** 256
- ❍ **C.** 128
- ❍ **D.** 126

16. Which of the following are considered private addresses per RFC 1918? (Choose the 3 best answers.)

- ❍ **A.** 1.0.0.0
- ❍ **B.** 10.10.10.20
- ❍ **C.** 172.30.255.10
- ❍ **D.** 192.168.128.128

17. What is the CIDR notation for the 128.250.62.0 network with a subnet mask of 255.255.255.0?

- ❍ **A.** /23
- ❍ **B.** /24
- ❍ **C.** /25
- ❍ **D.** /26

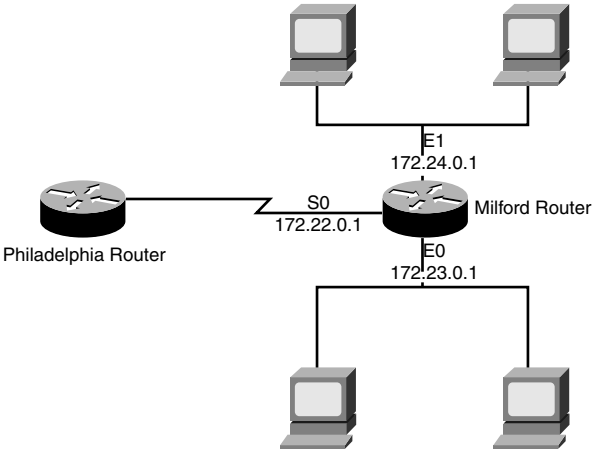
18. Which of the following network classes do not define public IP address space? (Choose the 2 best answers.)

- ❍ **A.** Class B
- ❍ **B.** Class C
- ❍ **C.** Class D
- ❍ **D.** Class E

19. What is the valid IP host range for 160.254.101.167/27?

- ❍ **A.** 160.254.101.128–160.254.101.254
- ❍ **B.** 160.254.101.129–160.254.101.254
- ❍ **C.** 160.254.101.160–160.254.101.191
- ❍ **D.** 160.254.101.161–160.254.101.190

20. Given this network diagram, if the Philadelphia router sends a packet to 172.23.0.51, what interface will the Milford router use to forward the packet?



- ❍ **A.** E0
- ❍ **B.** E1
- ❍ **C.** S0
- ❍ **D.** S1

Answers to Review Questions

1. 128 64 32 16 8 4 2 1

0 0 1 0 1 0 1 0

32+8+2 = 42

128 64 32 16 8 4 2 1

0 0 1 1 1 1 1 1

32+16+8+4+2+1 = 63

128 64 32 16 8 4 2 1

1 1 0 1 1 1 0 0

128+64+16+8+4 = 220

128 64 32 16 8 4 2 1

1 1 1 1 1 1 1 1

128+64+32+16+8+4+2+1 = 255

The correct answer is 42.63.220.255.

2. 128 64 32 16 8 4 2 1

1 0 0 1 0 1 1 0

128 64 32 16 8 4 2 1

1 1 0 0 0 0 0 1

128 64 32 16 8 4 2 1

0 0 0 0 0 1 1 0

128 64 32 16 8 4 2 1

0 1 1 0 0 1 0 0

The correct answer is 10010110 11000001 00000110 01100100.

3. The first hexadecimal character is 5, which is the same as the decimal value.

   8 4 2 1

   0 1 0 1

   The second hexadecimal character is F, which is 15 in decimal.

   8 4 2 1

   1 1 1 1

   Now you can combine the two 4-bit groups to get 01011111, which converts to 95 in decimal.

4. IP Address Binary = 11001000 00111110 10110111 00011010

   Subnet Mask Binary= 11111111 11111111 11111111 00000000

   Boolean AND = 11001000 00111110 10110111 **00000000**

   The correct answer is 200.62.183.0.

5. This is considered an easy mask. You just write down the original octets with a subnet mask value of 255 and a 0 for each octet with a 0 value in the subnet mask.

   The correct answer is 32.116.5.0.

6. Because this has an easy subnet mask, you can copy the first three octets and then replace the last octet with 255.

   The correct answer is 213.50.201.255.

7. This IP address subnet mask is 255.255.255.0, so the network ID is 220.9.3.0. The broadcast IP is 220.9.3.255.

   The correct answer is 220.9.3.1–220.9.3.254.

8. Zero subnet may also be referred to as subnet zero. The zero subnet is the first subnet in a network and has all binary 0s in the subnet field. For the purpose of taking the CCNA exam, you should not include the first subnet when calculating the number of networks in a larger subnet. This is one of the two reserved subnet numbers on a network and one of the reasons why you subtract from the total number of networks to get the correct answer for the test. The other network is the broadcast subnet, which has all 1s in the subnet field.

9. Traffic that is generated by a device has the source MAC and source IP address of that device. If a frame is sent to a server on another segment of a WAN, the destination IP address is that of the server the frame is trying to reach. Because the server is not on the same segment, the destination MAC address is that of the router, which is the default gateway. The router takes a look at the frame and at its own routing table. It then decides what interface to use to forward the frame, based on the network portion of the IP address. The router attaches its own MAC address as the source MAC address of the frame before the frame is sent to the server.

10. Suppress broadcasts or multicasts.

    Determine the best path for data transfer (routing).

    Strip down and add to Data Link layer frames.

    Implement access lists for packet filtering (permit/deny statements).

    Set up quality of service (QoS) qualifiers to measure network performance.

Answers to Exam Questions

1. **A.** The decimal equivalent of 10010111 00000110 10101100 01110111 is 151.6.172.119. Answers B and D can be eliminated right away because both IP addresses end with an even number.

2. **B.** The first octet range for Class B addresses is 128–191. Answers A, C, and D are incorrect because the range of 1–126 is Class A, 192–223 is Class C, and 224–239 is reserved for multicast.

3. **C.** Answer C is correct because the first octet range for Class C addresses is 192–223. Answers A, B, and D are incorrect because the first octet range for Class A addresses is 1–126, for Class B is 128–191, and 224–239 is reserved for multicast.

4. **B.** There are 254 hosts per Class C network. For any Class C network there are 24 network bits and 8 host bits: $2^8 - 2 = 254$.

5. **B.** The Network ID of 124.199.7.18/28 is 124.199.7.16. If you write out the subnet mask it is 255.255.255.240. Subtract 240 from 256 and you have 16; $16 \times 1 = 16$, which is the first valid increment that can be the network ID. The next network ID is 124.199.7.32.

6. **C.** Subnet mask 255.255.255.240 allows for 14 networks and 14 hosts. Answer A is incorrect because subnet mask 255.255.255.0 allows for only one network with 254 hosts. Answer B is incorrect because subnet mask 255.255.255.224 allows for 6 networks and 30 hosts, and answer D is incorrect because subnet mask 255.255.255.248 allows for 30 networks and 6 hosts.

7. **B, C.** 208.62.15.1 and 208.62.15.30 are valid host addresses in the 208.62.15.0 network with a 255.255.255.224 subnet mask. Answer A is incorrect because 208.62.15.0 is the network ID and therefore is not a valid host address. Answer D is incorrect because 208.62.15.32 is the network ID of the next network and is not valid.

8. **B.** The network address 192.131.10.0 and subnet mask 255.255.255.0 has one network with 254 hosts.

9. **A.** With a network address of 218.41.99.24 and a subnet mask of 255.255.255.252, 2 valid host addresses are available. Answer B is incorrect because subnet mask 255.255.255.248 has 6 available hosts. Answers C and D are incorrect because subnet mask 255.255.255.240 has 14 available hosts, and subnet mask 255.255.255.224 has 30 available hosts.

10. **D.** Subnet mask 255.255.255.224 would allow for 6 networks with 30 available hosts per network. Answer A is incorrect because subnet mask 255.255.255.252 allows for 62 networks but only 2 hosts per network. Answers B and C are incorrect because subnet mask 255.255.255.240 allows for 14 networks with only 14 hosts per network, and subnet mask 255.255.255.248 allows for 30 networks with only 8 hosts per network.

11. **C.** There are 65,534 hosts available for a Class B network. Answers A and D are incorrect because a Class C network has 254 possible hosts, and a Class A has 16,777,214 possible hosts.

12. **C.** The broadcast IP for 196.23.250.32/27 is 196.23.250.63. Answer A is incorrect because 196.23.250.32 is the Network ID of 196.23.250.32/27. Answers B and D are incorrect because 196.23.250.33 is the first valid IP in the /27 network and 196.23.250.64 is the Network ID of the next network.

13. **A.** The only subnet that allows for 250 networks is 255.255.255.0. Subnet mask 255.255.255.0 can create 254 subnets. Answer B is incorrect because subnet mask 255.255.254.0 can create 126 subnets. Answer C is incorrect because subnet mask 255.255.252.0 can create 62 subnets. Answer D is incorrect because subnet mask 255.255.248.0 can create 30 subnets.

14. **B.** You can have 14 subnetworks with a Class B network that has a subnet mask of 255.255.240.0.

15. **D.** Answer D is correct because there are 126 possible hosts for a Class B network with a subnet mask of 255.255.255.128. Answer A is incorrect because a Class B network with a subnet mask of 255.255.255.0 has 254 possible hosts. Answers B and C are incorrect because the Network ID and Broadcast IP addresses were not subtracted from the total number of IPs in each subnet.

16. **B, C, D.** RFC 1918 defines the following private IP address ranges: 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, and 192.168.0.0–192.168.255.255. Answer A is incorrect because the address 1.0.0.0 is a Class A public address.

17. **B.** 24 is the correct CIDR notation for the 128.250.62.0 network with a subnet mask of 255.255.255.0. Answer A is incorrect because /23 is the CIDR notation for 255.255.254.0. Answer C is incorrect because /25 is the CIDR notation for 255.255.255.128, and answer D is incorrect because /26 is the CIDR notation for 255.255.255.192.

18. **C, D.** Class D defines multicast address space and Class E defines IP address space reserved for research. Answers A and B are incorrect because Classes B and C are both defined for public use.

19. **D.** The valid host range for 160.254.101.167/27 is 160.254.101.161–160.254.101.190. Answers A and B are incorrect because both 160.254.101.128–160.254.101.254 and 160.254.101.129–160.254.101.254 are part of a 255.255.255.128 subnet. Answer C is incorrect because with the range 160.254.101.160–160.254.101.191, the first IP is the Network ID and it is not a valid host IP address.

20. **A**. The Milford router forwards the packet through the E0 interface because the network matches the 172.23.0.0 network. Answer B is incorrect because interface E1 is going to the 172.24.0.0 network, and answer C is incorrect because interface S0 is going to the Philadelphia router via the 172.22.0.0 network. Answer D is incorrect because interface S1 does not exist in this scenario.

Suggested Readings and Resources

The following are some recommended readings on IPv4, private and public IP addressing, subnetting, and routing:

1. "IPv4," http://en.wikipedia.org/wiki/IPv4.
2. "RFC 1918," http://www.faqs.org/rfcs/rfc1918.html.
3. "IP Addressing and Subnetting for New Users," http://www.cisco.com/warp/public/701/3.html.
4. "IP Address Subnetting Tutorial," http://www.ralphb.net/IPSubnet/.
5. "Network Calculators," http://www.subnetmask.info/.
6. Colton, Andrew. *Cisco IOS for IP Routing*. Rocket Science Pr Inc, 2002.

5

CHAPTER FIVE

Introduction to Cisco Routers and Switches

Objectives

This chapter covers the following Cisco-specified objective for the "Technology" section of the CCNA exam:

Describe the components of network devices

- A network device may use various components to achieve connectivity and increase functionality. These components are fundamental to internetworking.

Outline

Study Strategies

- Identify the interfaces and modules used with Cisco devices.
- Describe the Cisco memory components ROM, Flash, RAM, and NVRAM.
- Familiarize yourself with Cisco Internetworking Operating System (IOS) feature sets.
- Review the IOS image file structure.
- Identify the Cisco Router models and their features.
- Identify the Cisco Switch models and their features.

Introduction

Up to this point, we have discussed general internetworking technologies and devices to provide a background of the material relevant to the CCNA exam. Now the scope of the discussion widens to include Cisco technology. This chapter reviews internetworking devices (routers and switches) that were developed by Cisco for network implementations. It also discusses the individual hardware components that make up a router and switch, which you must thoroughly understand before the configuration of these devices is explained. This introduction to Cisco technology leads up to Chapter 6, "Initial Cisco IOS Operations," where you will delve into hands-on device operations and configurations.

Interfaces and Modules

Objective:

Describe the components of network devices

Networks can be connected to Cisco hardware in a variety of ways. Communication lines can be terminated to a Cisco device via hardware interfaces and modules. Interfaces provide a physical point of interaction between two networks. That hardware interface includes the cable, plug, socket, and signal that sync up together to communicate among devices.

Certain Cisco routers are built as fixed-port routers or fixed configuration routers and do not allow for additional network module installations. Cisco also offers modular-port routers. Modular-port routers allow for future system upgrades by mounting network modules in available spaces to accommodate changing network environments. A module is a self-contained component. A Cisco network module has built-in hardware interfaces to add alternate connection options on a network. Because they are modular components, Cisco routers can be upgraded easily and with minimal expense to the company. This chapter reviews the variety of physical connection types on LAN and WAN devices.

LAN Interfaces

Local area network (LAN) interfaces are used to provide a point of interconnection between Cisco switches and other network devices. Cisco provides a wide selection of switches that can be implemented on a LAN and offer end-user connectivity. In Chapter 3, "Data Link Networking Concepts," Layer 2 switches were introduced. The Cisco 2950 series switch family includes various models with different interface options, such as the Cisco 2950-12 and the Cisco 2950-24. The 2950-12 has 12 built-in ethernet ports, whereas the 2950-24 has 24 built-in ethernet ports. Certain models also have Gigabit Ethernet slots.

If Gigabit Ethernet ports are included, the front panel of a 2950 model has 10/100 ethernet ports on the left side of the switch and 2 Gigabit Ethernet slots that accommodate LAN

interface modules on the right. The 10/100 ports allow for either a 10Mbps or 100Mbps connection speed. Media connects to an ethernet switch port via an RJ-45 connector. As far as the switch is concerned, each ethernet port is designated as a numbered interface for identification. The top left port is labeled `1` by the switch. Each interface begins with a `0/#`, where the `#` sign equals the port number on the switch. The top left port is then named 0/1 on that switch. Given this formula, the bottom left port is labeled 0/2.

EXAM ALERT

For the CCNA exam, know how the interfaces are labeled for an ethernet port. This information is necessary for any switch configuration exercises.

The Gigabit Ethernet slots are available for Gigabit Interface Converters (GBICs). A GBIC interface module can be inserted into the Gigabit Ethernet slot to allow for different media connections to that port. The physical media can range from copper to single-mode fiber. A GBIC is also hot swappable, so you can remove and replace it without shutting off power to the switch. This helps to avoid interruption of service to that switch.

The back panel of the 2950 includes power input and the switch's console port. The console port has an RJ-45 connector and is connected to a terminal with a rollover cable for initial switch configuration.

WAN Interfaces

Wide area network (WAN) interfaces are also used to provide a point of interconnection between Cisco routers and other network devices. Types of WAN interfaces include

- Basic Rate Interface (BRI)
- Synchronous Serial
- Asynchronous Serial
- High-Speed Serial Interface (HSSI)
- T1 Controller Card

BRI

BRI is an Integrated Services Digital Network (ISDN) service that consists of two 64Kbps bearer (B) channels and one 16Kbps data (D) channel. Voice, video, and data traffic can be carried over the B-channels. Signals between telephone company switches use the D-channel. Cisco offers an 8-port ISDN-BRI with a built-in Network Termination Type 1 (NT-1) Network Module for router installation.

EXAM ALERT

For the exam you should know that BRI is an ISDN line that consists of two 64Kbps bearer (B) channels and one 16Kbps data (D) channel.

The NT-1 is a telephone company requirement for an ISDN line connection. This network module has a BRI U interface, which means that the NT-1 is built in on the network module and does not require a separate NT-1 device.

Synchronous Serial

A synchronous serial interface synchronizes clocks for the bit stream of both the sending and receiving end of a serial link. This allows for the data rate to be adjusted if necessary to ensure that both ends of a serial link are functioning at the same speed.

Asynchronous Serial

An asynchronous serial interface does the opposite of a synchronous serial interface. It does not synchronize the clocks for the bit stream of the sending and receiving end of a serial link. Cisco offers a 4-port asynchronous/synchronous serial network module.

With the asynchronous/synchronous serial network module, each port can be configured individually as either asynchronous or synchronous, depending on your network setup.

HSSI

High-speed serial interfaces offer up to 52Mbps transmission rates to the WAN from a Cisco router. The higher speed capacity is relevant if the corporate backbone requires high-speed Internet access and VPN connectivity. Cisco offers a 2-port HSSI port adapter.

T1 Controller Card

Also referred to as a *digital signal level 1* (DS1) service, a T1 is a connecting line that offers a 1.544Mbps data transmission speed. A single T1 line consists of 24 digital signal level 0 (DS0) channels that are 64Kbps each and an additional 8Kbps that is reserved for management overhead. A T1 controller card can be installed in a router's T1 slot to communicate with and control the 24 DS0 channels.

Data Communications Equipment (DCE)

Data Communications Equipment (DCE) or Data Circuit-Terminating Equipment (DCE) is the term used to identify a device that connects the Data Terminal Equipment (DTE) to a service provider's communications line. The DCE side of a connection sets the clock speed for a serial connection.

DCE equipment may consist of a

- Modem
- Channel Service Unit/Data Service Unit (CSU/DSU)
- Basic Rate Interface Network Termination Type 1 (BRI NT-1)

Modems convert a digital signal into an analog signal for transmission over a telephone line. The signal is converted back into a digital format when it reaches the device on the other end of that telephone line.

A Channel Service Unit/Data Service Unit (CSU/DSU) serves as the intermediary between the service provider and the WAN router. In most cases, the CSU/DSU provides the clock speed for the router. A CSU/DSU may be a separate unit or it could be incorporated into a WAN interface card (WIC).

If it is not built in on a Cisco router via a BRI-U (Basic Rate Interface-User) interface, the service provider requires separate BRI NT-1 hardware as a termination point for the communications line. The BRI NT-1 then connects to the Cisco router.

Data Terminal Equipment (DTE)

Data Terminal Equipment is the term used to identify a device at the user end of a network and is connected to the service provider via the DCE device.

DTE equipment may consist of a

- Router
- PC
- Server

In Figure 5.1, the service provider, whom you will most likely hear called a telco, brings a communication line from its central office (CO) to the customer and terminates its line to the CSU/DSU. The CSU/DSU is then connected to the customer router. The point at which the telco terminates its line to the customer is called a *demarcation point* or *demarc*. Customer-owned equipment, such as the router and typically the CSU/DSU, is referred to as *customer premise equipment (CPE)*.

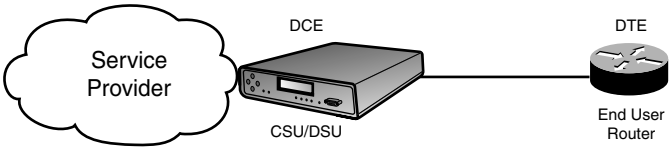


FIGURE 5.1 An overview of a service provider connection to an end user.

Cabling between the CSU/DSU and router is decided by the type of CSU/DSU that is deployed on that network. If a WIC functions as a CSU/DSU, then the CPE is a telco jack and a Category 5 or Category 6 cable is used with an RJ-45 connector. If a WIC does not function as the CSU/DSU, there are several types of connections possible between a CSU/DSU and the DTE device. With routers, typically a DB-60 connector is used to connect to the router while one of the following connectors is used to connect to the CSU/DSU:

- EIA/TIA-232
- EIA/TIA-449
- EIA/TIA-530
- V.35
- X.21

The Electronic Industries Association/Telecommunications Industry Association (EIA/TIA) formed a standards body, which developed the 232, 449, and 530 cables. The V.35 and X.21 cables were developed by the International Telecommunication Union (ITU).

Your best bet is to position the CSU/DSU as close to the router as possible. This requires the shortest amount of cable and therefore ensures maximum speeds.

EXAM ALERT

For the exam you should know the difference between DCE and DTE equipment. Also, know that the DCE side of a connection must provide the clocking for the serial connection.

Cisco Memory Components

Four memory components are used by Cisco devices. Those components include ROM, Flash, RAM, and NVRAM.

ROM

Read-only memory (ROM) contains the basic code for booting a device and maintaining Power on Self Test (POST), ROM Monitor (ROMmon), bootstrap, and RXBOOT. Because this type of memory is read-only, it cannot be changed by any configuration done at the networking device. ROM is nonvolatile, so data is not lost when the device is powered off.

Flash

Flash is installed on either an electrically erasable, programmable, read-only memory (EEPROM) or Personal Computer Memory Card International Association (PCMCIA) card. Flash memory contains the Cisco Internetworking Operating System (IOS) image. The router uses

Flash by default to locate the IOS when it is booted. Configuration files may also be stored on a Flash card. Like ROM, Flash is also nonvolatile memory.

RAM

Random-access memory (RAM) is used for short-term storage of a machine's running IOS and running configuration. The IOS is copied from Flash to RAM. This is the only type of system memory that is not permanent. At times, you may hear RAM also referred to as dynamic random-access memory (DRAM). Because this type of memory is volatile, it is lost whenever the machine is shut down.

EXAM ALERT

RAM contains the running IOS, with the exception of Run-From-Flash (RFF) routers. RAM also contains the running configuration or the active configuration that is used after a machine is booted.

NVRAM

Nonvolatile random-access memory (NVRAM) stores the startup configuration. This is the configuration that is loaded when the machine is booted.

Cisco Internetworking Operating System

Cisco IOS software is developed and maintained by Cisco to support a full array of system functions, applications (including Internet applications), and network hardware in a single software package. IOS software is installed on each Cisco router or switch and can accommodate network growth and provide for secure data transfers. The command-line interface (CLI) for routers and switches defines the commands that are used to communicate with the IOS. Future chapters demonstrate the use of CLI commands on both network devices.

NOTE

A Cisco Catalyst switch may use either a Cat OS or Cisco IOS. The major difference with Cat OS is the CLI commands that are used in conjunction with the operating system software.

Cisco releases IOS software using what they call trains. Each release can be further defined by train identifiers. A train identifier determines whether a release is a Technology (T), Enterprise (E), or Service Provider (SP) release. When the IOS version has no train identifier, it is the mainline train. With so many features and applications being offered with each

release, a train identifier can further define a specific subset of features. For example, if you have a release named 12.3(1)T, the IOS version number breaks down as follows:

- 12.3 refers to the mainline train that will not be added to but will be subject to IOS bug fixes.
- (1) represents the release number, which increments with each new release of the mainline train.
- T identifies the type of train release where T stands for Technology. This may also be an S (Service Provider) or E (Enterprise) train.

Feature Sets

A feature set is a package of the features that is offered in addition to the basic IOS functions of an IOS software release. You can select more than one feature set per release. Feature sets may be identified as standard, enhanced, or advanced, depending on the services that are supported. To give you an idea of the latest features available with Cisco IOS, current releases offer the following software functionality:

- IP Base—The base IOS image.
- IP Voice—Features include Voice over IP (VoIP), and Voice over Frame (VoFR).
- Advanced Security—Offers advanced protection via firewall, Intrusion Detection System (IDS), Secure Shell (SSH), and IP Security (IPSec).
- SP Services—Includes service provider services such as IPv6, Netflow SSH, ATM, Voice over ATM (VoATM), and Frame Relay.
- Enterprise Base—Consists of Enterprise Layer 3 routed protocols, and IBM support.
- Advanced IP Services—Offers a combination of the Advanced Security and Service Provider Services feature sets.
- Enterprise Services—Combines the Enterprise Base and Service Provider Services feature sets with full IBM support.
- Advanced Enterprise Services—Incorporates all the Cisco IOS feature sets.

IOS Image File Naming

The IOS image file represents the name of the system image on a Cisco router or switch. The hardware platform, feature set, compression format, IOS version, and train information are all

found in the name of an IOS image file. An IOS image filename can be broken out to identify more specific information about the IOS in use by a device. This is helpful if you are troubleshooting a system issue and need to verify what version is currently in use. Cisco may be aware of an IOS bug, or the version may simply be outdated and an IOS upgrade might be the solution to your trouble. To find the IOS image filename, use the `show version` command from the command prompt.

Given the example filename `c2600-ipbase-1.122-1.T.bin` (`.bin` indicates binary format), from left to right, each portion of the filename represents the following:

- `c2600`—Hardware platform (Cisco 2600 router)
- `ipbase`—Feature set
- `1`—File format (compressed re-locatable)
- `122`—IOS version number
- `1`—Maintenance release number
- `T`—Train identifier

EXAM ALERT

Remember the IOS image file structure. If given a filename, you should be able to break down each part of the file and what it represents.

Challenge

Understanding Cisco IOS is necessary for the maintenance and troubleshooting of Cisco routers and switches. I will provide an IOS image filename and would like you to identify the hardware platform, feature set, compression format, IOS version, and train information for that file.

IOS Image filename—c1700-entbase-1.121-1.E.bin

Maintenance Release Number _____

File Format _____

Hardware Platform _____

Train Identifier _____

Feature Set _____

IOS version number _____

Cisco Router Models and Features

Cisco offers a wide selection of router models for network implementations. The Cisco family of routers can accommodate networks that range in size and require various network interfaces for WAN connectivity. As mentioned, some router models are fixed port and fixed configuration, whereas others are modular-port routers. To help you prepare for the CCNA exam, a Cisco 2500 series router model can perform a broad range of the basic routing functions. This router can provide you with sufficient functionality to practice initial router setup and configurations.

The 2500 series hardware can support CSU/DSU, ethernet, token ring, asynchronous or synchronous serial, and ISDN connections. The 2500 series routers coupled with Cisco IOS software can support routed protocols such as IP, Novell IPX, and AppleTalk. They can also support a wide array of routing protocols. Although most of the 2500 family routers are fixed port, the 2524 and 2525 models are both modular-port routers.

In addition to the 2500 series routers, Cisco also offers the following router series:

- **800 Series**—Fixed-port and fixed-configuration routers that support Asymmetric Digital Subscriber Line (ADSL), ADSL over ISDN, Single-pair High-Speed DSL (G.SHDSL), Serial, and ethernet to an external cable modem or DSL connections. They can also support a small office or a home office for a telecommuter.
- **1600 Series**—Fixed-port routers that support ISDN, asynchronous serial, or synchronous serial connections and can support a small- to moderately-sized business.
- **1700 Series**—Modular-port routers that support built-in Fast Ethernet LAN ports and WAN/Voice modular slots, and can support a small- to moderately-sized business.
- **1800 Series**—Fixed-port and modular-port routers that build on the 1700 Series router functionality with integrated services such as IPSec VPN, firewall security, inline intrusion prevention (IPS), Network Admission Control (NAC), and URL filtering to small offices.
- **2600 Series**—Modular multiservice access routers that support built-in ethernet LAN ports, built-in Fast Ethernet LAN ports, and WAN/voice modular slots. They can support a small to medium office.
- **2800 Series**—Integrated service routers that support built-in Fast Ethernet LAN ports, built-in Gigabit Ethernet LAN ports, and WAN/voice modular slots. They can support a small to medium office, its telecommuters, and Wi-Fi connections.
- **3600 Series**—Modular multiservice access routers that support data, voice, video, and VPN. They can support a medium to large office or a small Internet Service Provider (ISP).
- **3700 Series**—Modular multiservice access routers that support built-in Fast Ethernet LAN ports and WAN/voice modular slots. They can support branch offices.

- **3800 Series**—Modular multiservice access routers that support built-in dual Gigabit Ethernet LAN ports and enhanced network module slots. They can support a medium to large business with integrated services.
- **7200 Series**—Can be used with an Enterprise Edge or Service Provider Edge environment and support links that range in size from a DS0 (64Kbps) all the way up to an OC12 (655Mbps). They can support Fast Ethernet, Gigabit Ethernet, and Packet over Sonet connections. Chassis slots are open for installation of more than 70 network interfaces.
- **7600 Series**—Are likely to be found in a main office of an enterprise business or at a small service provider's point-of-presence (POP) site. Each chassis can support a maximum of 4 slots. Each slot has either a 40Gbps or 720Gbps capacity with advanced optical service modules.

Cisco Switch Models and Features

The Cisco family of switches includes the Catalyst switch models, which as you learned earlier in this chapter might use the Cat OS rather than the IOS. As with Cisco routers, the switch model numbers increase as they are upgraded for enhanced overall operability. Various switches have been developed over the years to accommodate the size and functionality requirements of LANs around the world. You may have a Cisco 1900, 2800, 2900, or 2924 switch to help you study for the Cisco Certified Network Associate. These models should be easy to find and affordable, and they cover all the features necessary for the exam when coupled with Cisco IOS.

In addition to the 1900, 2800, 2900, and 2924 series switches, Cisco also offers the following switch series:

- **2950 Series**—Includes a fixed-configuration switch that can support both Fast Ethernet and Gigabit Ethernet connections.
- **3500 Series**—Are stackable switches that can employ Cisco Switch Clustering technology and GigaStack GBICs, and support Layer 3 functionality.
- **4000 Series**—Can support high-density copper, fiber-based interfaces, Fast Ethernet, Gigabit Ethernet connections, and Layer 3 functionality.
- **6500 Series**—Can support Power over Ethernet (PoE) devices, 10/100Mbps ethernet ports, 10/100/1000Mbps ethernet ports, 10Gbps ethernet ports, and Layer 3 functionality.

Cisco switches may also support PoE. PoE enables an end device to receive power over a copper ethernet cable. End devices that might use PoE include IP telephones, video cameras, and card scanners. This technology was originally developed by Cisco and called "inline power." IEEE has since standardized PoE with 802.3af.

Chapter Summary

A general knowledge of Cisco hardware and IOS is integral to your preparation for the CCNA exam. Chapter 6 shows you how to correctly navigate through the Cisco IOS. Also, Cisco router and switch configurations are presented throughout the remainder of this book.

Key Terms

- interface
- module
- GBIC
- BRI
- synchronous
- asynchronous
- HSSI
- T1 controller card
- DS0
- DS1
- T1
- BRI
- ISDN
- NT-1
- HSSI
- DTE
- modem
- CSU/DSU
- CO
- demarc
- CPE
- ROM
- Flash
- RAM
- NVRAM
- IOS
- train
- CLI
- PoE

Apply Your Knowledge

Exercises

5.1 Cisco Memory Components

You may be asked to identify the memory components that are used on Cisco devices. In this exercise, please list the four types of memory and their respective functions.

Estimated Time: 10 minutes

Memory Component	Memory Component Functionality

Review Questions

1. Describe a GBIC.
2. List the WAN interfaces and their descriptions.
3. Define DCE and DTE.
4. What is the Cisco IOS?
5. Define PoE.

Exam Questions

1. Which WAN interface is an ISDN line that consists of two 64Kbps bearer (B) channels and one 16Kbps data (D) channel?

   - ❍ **A.** BRI
   - ❍ **B.** Synchronous serial
   - ❍ **C.** Asynchronous serial
   - ❍ **D.** HSSI

2. Which WAN interface synchronizes clocks for the bit stream of both the sending and receiving end of a serial link?

   - ❍ **A.** BRI
   - ❍ **B.** Synchronous serial
   - ❍ **C.** Asynchronous serial
   - ❍ **D.** HSSI

3. Which WAN interface offers up to 52Mbps transmission rates to the WAN from a Cisco router?

   - ❍ **A.** BRI
   - ❍ **B.** Synchronous serial
   - ❍ **C.** Asynchronous serial
   - ❍ **D.** HSSI

4. Which of the following devices can be labeled Data Circuit-Terminating Equipment (DCE)? (Choose the 3 best answers.)

- ❍ **A.** Router
- ❍ **B.** Modem
- ❍ **C.** CSU/DSU
- ❍ **D.** BRI NT-1

5. Which of the following devices can be labeled Data Terminal Equipment (DTE)? (Choose the 3 best answers.)

- ❍ **A.** Router
- ❍ **B.** Modem
- ❍ **C.** PC
- ❍ **D.** Server

6. What type of memory contains the basic code for booting a device and maintaining POST, ROMmon, bootstrap, and RXBOOT?

- ❍ **A.** ROM
- ❍ **B.** Flash
- ❍ **C.** RAM
- ❍ **D.** NVRAM

7. What type of memory is nonvolatile and contains the Cisco IOS image?

- ❍ **A.** ROM
- ❍ **B.** Flash
- ❍ **C.** RAM
- ❍ **D.** NVRAM

8. This type of memory contains the running IOS and the running configuration (active configuration) that is used after a machine is booted.

- ❍ **A.** ROM
- ❍ **B.** Flash
- ❍ **C.** RAM
- ❍ **D.** NVRAM

9. This type of memory stores the startup configuration.

   - ❍ **A.** ROM
   - ❍ **B.** Flash
   - ❍ **C.** RAM
   - ❍ **D.** NVRAM

10. What does the ipbase portion of the Cisco IOS file named c2600-ipbase-1.122-1.T.bin represent?

    - ❍ **A.** Hardware platform
    - ❍ **B.** Feature set
    - ❍ **C.** Train identifier
    - ❍ **D.** IOS version

Answers to Review Questions

1. A GBIC interface module can be inserted into the Gigabit Ethernet slot to allow for different media connections to that port. The physical media can range from copper to single-mode fiber. A GBIC is also hot swappable, so it can be installed without interrupting service to that switch.

2. Basic Rate Interface (BRI)

   BRI is an ISDN line that consists of two 64Kbps bearer (B) channels and one 16Kbps data (D) channel. Voice, video, and data traffic can be carried over the B-channels. Signals between telephone company switches use the D-channel.

   Synchronous serial

   A synchronous serial interface synchronizes clocks for the bit stream of both the sending and receiving end of a serial link. This enables the data rate to be adjusted if necessary to ensure that both ends of a serial link are functioning at the same speed.

   Asynchronous serial

   An asynchronous serial interface does the opposite of a synchronous serial interface. It does not synchronize the clocks for the bit stream of the sending and receiving end of a serial link.

   High-Speed Serial Interface (HSSI)

   High Speed Serial Interfaces offer up to 52Mbps transmission rates to the WAN from a Cisco router.

   T1 controller card

   A T1 controller card can be installed in a router's T1 slot to communicate with and control the 24 DS0 channels.

3. Data Circuit-Terminating Equipment (DCE) or Data Communications Equipment is the term used to identify a device that connects the Data Terminal Equipment (DTE) to a service provider's communications line. DCE equipment may consist of a modem, CSU/DSU, or BRI NT-1.

   DTE is the term used to identify a device at the user end of a network and is connected to the service provider via the DCE device. DTE equipment may consist of a router, PC, or server.

4. Cisco IOS software is developed and maintained by Cisco to support a full array of system functions, applications (including Internet applications), and network hardware in a single software package. IOS software is installed on each Cisco router or switch and can accommodate network growth and provide for secure data transfers. The command-line interface (CLI) for routers and switches defines the commands that are used to communicate with the IOS.

5. Power over Ethernet (PoE) enables an end device to receive power over a copper ethernet cable. End devices that might use PoE include IP telephones, video cameras, and card scanners. This technology was originally developed by Cisco and called "inline power." IEEE has since standardized PoE with 802.3af.

Answers to Exam Questions

1. **A.** BRI consists of two 64Kbps B channels and one 16Kbps D channel. Answer B is incorrect because synchronous serial synchronizes clocks for the bit stream of both the sending and receiving end of a serial link. Answer C is incorrect because asynchronous serial does not synchronize the clocks for the bit stream of the sending and receiving end of a serial link. Answer D is incorrect because HSSI offers up to 52Mbps transmission rates to the WAN from a Cisco router.

2. **B.** Synchronous serial synchronizes clocks for the bit stream of both the sending and receiving end of a serial link. Answer A is incorrect because BRI consists of two 64Kbps B channels and one 16Kbps D channel. Answer C is incorrect because asynchronous serial does not synchronize the clocks for the bit stream of the sending and receiving end of a serial link. Answer D is incorrect because HSSI offers up to 52Mbps transmission rates to the WAN from a Cisco router.

3. **D.** HSSI offers up to 52Mbps transmission rates to the WAN from a Cisco router. Answer A is incorrect because BRI consists of two 64Kbps B channels and one 16Kbps D channel. Answer B is incorrect because synchronous serial synchronizes clocks for the bit stream of both the sending and receiving end of a serial link. Answer C is incorrect because asynchronous serial does not synchronize the clocks for the bit stream of the sending and receiving end of a serial link.

4. **B, C, D.** Modems, CSU/DSUs, and BRI NT-1s are all Data Circuit-Terminating Equipment. Answer A is incorrect because routers are considered Data Terminal Equipment.

5. **A, C, D.** Answers A, C, and D are correct because routers, PCs, and servers are all Data Terminal Equipment. Answer B is incorrect because modems are Data Circuit-Terminating Equipment.

6. **A.** ROM contains the basic code for booting a device and maintaining POST, ROMmon, bootstrap, and RXBOOT. Answer B is incorrect because Flash memory contains the Cisco IOS image. Answer C is incorrect because RAM is used for short-term storage of a machine's running IOS and running configuration. Answer D is incorrect because NVRAM stores the startup configuration.

7. **B.** Flash memory is nonvolatile and contains the Cisco IOS image. Answer A is incorrect because ROM contains the basic code for booting a device and maintaining POST, ROMmon, bootstrap, and RXBOOT. Answer C is incorrect because RAM is used for short-term storage of a machine's running IOS and running configuration. Answer D is incorrect because NVRAM stores the startup configuration.

8. **C.** RAM contains the running IOS and the running configuration (active configuration) that is used after a machine is booted. Answer A is incorrect because ROM contains the basic code for booting a device and maintaining POST, ROMmon, bootstrap, and RXBOOT. Answer B is incorrect because Flash memory contains the Cisco IOS image. Answer D is incorrect because NVRAM stores the startup configuration.

9. **D.** NVRAM stores the startup configuration. Answer A is incorrect because ROM contains the basic code for booting a device and maintaining POST, ROMmon, bootstrap, and RXBOOT. Answer B is incorrect because Flash memory contains the Cisco IOS image. Answer C is incorrect because RAM is used for short-term storage of a machine's running IOS and running configuration.

10. **B.** The term *ipbase* refers to the IP Base feature set. Answer A is incorrect because the hardware platform is c2600 or the Cisco 2600 router. Answer C is incorrect because the train identifier is T for Technical. Answer D is incorrect because the IOS version is represented by 122 or version 12.2.

Suggested Readings and Resources

The following are some recommended readings on network components, Cisco devices, and terminology:

1. "Serial Connectivity Network Modules," http://www.cisco.com/en/US/products/hw/routers/ps274/products_data_sheet09186a0080091b8b.html.

2. "White Paper: Cisco IOS Reference Guide," http://www.cisco.com/warp/public/620/1.html.

3. Boney, James. *Cisco IOS in a Nutshell*, first edition. O'Reilly, 2001.

4. "Loading and Maintaining System Images," http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/1026071.

5. "Cisco Router Guide," http://www.cisco.com/application/pdf/en/us/guest/products/ps5855/c1031/cdccont_0900aecd8019dc1f.pdf.

CHAPTER 6

Initial Cisco IOS Operations

Objectives

This chapter covers the following Cisco-specified objectives for the "Technology," "Implementation and Operation," and "Troubleshooting" sections of the CCNA exam:

Establish communication between a terminal device and the router IOS, and use IOS for system analysis

Describe the purpose and fundamental operation of the internetwork operating system (IOS)

Identify the major internal and external components of a router, and describe the associated functionality

Identify and describe the stages of the router boot-up sequence

Describe how the configuration register and `boot system` commands modify the router boot-up sequence

- One of the primary steps in configuring a Cisco device is to establish a terminal session using the proper cabling, protocols, and parameters.
- Comprehending the command hierarchy of the IOS is an integral stepping stone in understanding its fundamental operations.
- By scrutinizing the individual steps of a router or switch boot-up sequence, you formulate a detailed perspective of the internal components of that device.
- From turning on the power of a Cisco device all the way to the configuration being loaded, a CCNA candidate is expected to thoroughly comprehend each stage of a router boot-up and the implications when that boot-up fails at any stage.
- Changing the default configuration register and utilizing `boot system` commands will alter the normal boot-up process for Cisco devices.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- This chapter serves as a foundation for all configurations that are to come. It is not enough to just grasp these concepts. You should feel completely comfortable with the navigation of the IOS before tackling advanced configurations in future chapters.
- If possible, practice the syntax of every command discussed throughout this chapter (and book) with real or simulated Cisco equipment.
- Complete the Challenge Exercises and the Exercises at the end of the chapter. These exercises are designed to give you practical experience using the utilities discussed.
- Complete the Exam Questions at the end of the chapter. They are designed to simulate the type of questions you will be asked in the CCNA exam.

Introduction

Unfortunately, Cisco devices are not yet at the point where they can automatically configure themselves. With that being said, each Cisco device that contains an IOS (internetwork operating system) must have some interface in which you, the expert Cisco administrator, can interact with the operating system to perform any administration, configuration, and troubleshooting services.

This chapter explores the options available for interacting with the Cisco IOS. In addition, it looks into the multiple boot-up steps that occur when a Cisco router or switch is powered on, and how you can manipulate that startup sequence. Finally, it explores the command hierarchy of the IOS and shows you how to accurately navigate your way around to achieve your administrative goal.

Terminal Options

Objective:

Establish communication between a terminal device and the router IOS, and use IOS for system analysis

You can choose from among several options to gain access to the Cisco IOS. These access methodologies are commonly referred to as EXEC sessions. Assuming that the device model and IOS supports them, certain Cisco devices can support up to five means of gaining an EXEC session to the IOS, which are discussed in the following subsections.

Console Port

The majority of Cisco devices do not have a default IP address that can be utilized to gain access to the IOS. Therefore, most Cisco devices gain initial out-of-band terminal access via the console port. After an EXEC access is gained, you can configure the device via the CLI (command-line interface) of the IOS.

NOTE

The term *out-of-band* simply refers to the fact that the console is a management port that is separate from interfaces that are used for networking data transmissions. Adversely, *in-band* management signals traverse over the same networking paths and interfaces as the data stream. This implies that you have IP connectivity to the devices that you are managing.

To connect to a console port, Cisco supplies you with a flat rollover cable. As illustrated in Figure 6.1, the pins in a rollover cable are reverse images of each other when the cable is viewed with both sides of the tabs down. Cisco console cables either come with a two RJ-45 connectors in which a DB-9 adapter is required for connection to the PC, or come with the DB-9 connector attached to one end of the cable. The 9-pin connector of the console cable connects to your terminal PC's COM port. Keep in mind that this management connection is for initial terminal access only and should not be confused with an actual networking Ethernet cable of any sort.

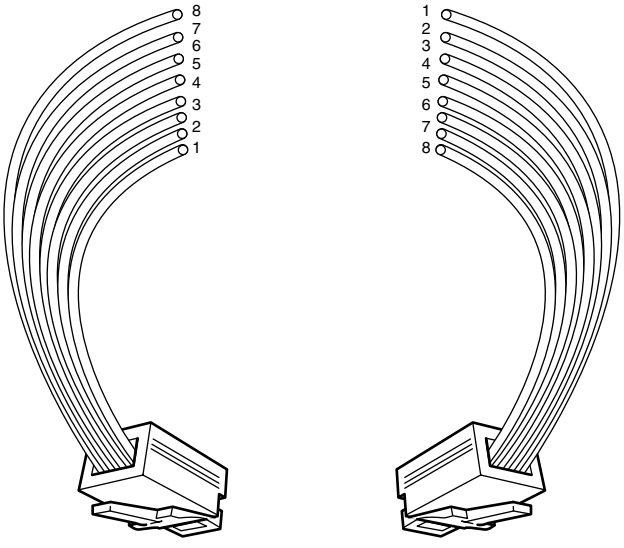


FIGURE 6.1 Cisco console cable pinouts.

EXAM ALERT

It is important to be able to recognize and differentiate between the pin configurations of a straight-through ethernet cable versus a cross-over ethernet cable versus a rollover console cable.

An ASCII terminal emulation software program must be running on your management PC if it is to interact with the Cisco IOS. There are several different terminal programs available, such as HyperTerminal, TeraTerm, SecureCRT, and others. The terminal setup of the COM port connected to the rollover console cable must be set to the following default console parameters: 9600 baud, 8 data bits, no parity bits, 1 stop bit, and no flow control. After the terminal is set up correctly and you have powered on the Cisco device, you should see the output from your console EXEC session in the terminal window.

Auxiliary Port

Certain Cisco models may contain another out-of-band management port called an auxiliary (AUX) port. This port is very similar to the console port in that it uses a rollover cable and has an RJ-45 connection to the Cisco device. The difference between the auxiliary and the console port is that the auxiliary port has flow control capability, which is useful for analog modem connectivity. By connecting an external modem to this management port, you can dial into the modem remotely and gain an EXEC session without being physically next to the Cisco device.

Telnet

As discussed in Chapter 1, "Standard Internetworking Models," Telnet is an Application layer protocol of the TCP/IP protocol suite that uses TCP port 23 to gain virtual terminal emulation to a device. Telnet is considered in-band management because it is required to have IP connectivity to the Cisco device into which you are trying to Telnet. Most Cisco devices allow at least 5 Telnet EXEC sessions to be connected for remote terminal access. For the sake of security, there is some configuration involved to allow Telnet access into the Cisco devices. Telnet is discussed in further detail in Chapter 7, "Basic Cisco Configurations."

EXAM ALERT

Initiating a Telnet session to a Cisco device is an excellent way to test that you have Application layer connectivity to that device.

HTTP

Similar to Telnet, HTTP is also an Application layer protocol of the TCP/IP protocol suite. It uses TCP port 80 to establish a management connection to the Cisco device. In addition, this EXEC option also requires IP connectivity to the Cisco device, making it an in-band management communication methodology. The key difference between HTTP and Telnet is that when you HTTP, you can have a graphical interface to the configuration and administration features of the Cisco IOS.

NOTE

Although the navigation of this management connection contains a graphical user interface (GUI), you will still be required to know the CLI syntax for most of the IOS functions.

The HTTP EXEC session is made possible by a HTTP server service that can run if configured on the Cisco device. For security purposes, Cisco routers do not have this functionality

enabled by default. Cisco Catalyst switches, however, typically have this functionality enabled for ease of administration. If this functionality is not going to be utilized, it is recommended that you disable this service to avoid any security vulnerabilities.

SSH

Imagine you have Telntetted into a Cisco device and you decide to change the password. If an attacker has the capability to eavesdrop on that Telnet terminal session, he could very well detect the password change because the Telnet communications are in clear text.

With SSH (Secure Shell), you are provided a secure terminal EXEC connection through the use of encrypted communications between your terminal client and the Cisco device. Your terminal application must support SSH to connect securely to your Cisco device. Some terminal programs that support SSH are SecureCRT and Putty. In addition, the version and feature set of the Cisco IOS must support SSH. Similar to its brother in-band protocols, Telnet and HTTP, SSH also requires initial configurations before gaining access to an EXEC session.

REVIEW BREAK

Table 6.1 quickly reviews the five means of gaining EXEC sessions to Cisco Devices.

TABLE 6.1 Cisco EXEC Session Summary

	In-band Versus Out-of-band	Cabling	Configuration Required	Notes
Console	Out-of-band	Rollover	No	Requires physical connectivity.
Auxiliary	Out-of-band	Rollover	No	Requires external modem for remote connectivity.
Telnet	In-band	None	Yes	Can support at least five connections to most Cisco devices.
HTTP	In-band	None	Yes	Must be enabled on Cisco routers. Should be disabled if not utilized.
SSH	In-band	None	Yes	Requires SSH-compliant terminal emulation program and specific Cisco IOS version and feature set.

Router/Switch Startup Procedures

Objective:

Identify and describe the stages of the router boot-up sequence

Now that you have an understanding of how to connect to the Cisco IOS, you can now look at the startup procedures for a Cisco router or switch to determine how the IOS is loaded and running in the first place when you power on those devices. Additionally, these devices would be doing us a huge administrative injustice if they did not load the configurations that you have toiled over in previous EXEC sessions (despite the obvious level of job security). Thus, you also need to look into how a saved configuration is applied after the IOS is loaded. As you will see, each of the memory components that was discussed in Chapter 5, "Introduction to Cisco Routers and Switches," performs a pivotal part in the storing, loading, and running of the IOS and the configuration.

Router and switch startup procedures are extremely similar to a computer's boot-up process. For instance, when you turn on a computer, the computer utilizes ROM (read-only memory) chips to perform a POST (power-on self-test) to check the critical hardware initially for start-up. Then it consults the BIOS (basic input/output system) settings to determine the order in which to search the hard drives, floppy drives, or CD drives to locate the operating system. After the operating system is loaded, it applies any custom configurations you have made in the past and utilizes those settings toward its normal operation.

Similarly, when you turn on a Cisco router and a switch, ROM chips perform a POST and then load the IOS process. You can manipulate the location sources of the IOS similar to specifying the boot drive in the BIOS settings on a computer. After the IOS is loaded, your saved configuration is loaded and applied to the device's operating functions. The next sections delve further into the specific processes that are occurring at each stage.

POST

Objective:

Identify the major internal and external components of a router, and describe the associated functionality

When you first apply power to a Cisco router or switch, a specialized ROM performs a series of tests of the critical hardware components that are pertinent for startup and basic operation such as Flash memory, CPU, and interfaces. It makes sense to utilize ROM chips for this service because they are already hard-coded with their programs and they do not require constant power to keep those programs stored in the memory. If a failure occurs during this stage of the startup process, you may encounter one of several outcomes, ranging from a non-functioning

interface all the way to complete device failure. In any case, your equipment should be under warranty or you have an active support contract in place to fix the failing hardware.

Bootstrap

After the hardware passes all its tests (if only the CCNA was that easy), another ROM seeks out the operating system in accordance to its programming routines. The code that is run in the ROM is commonly referred to as the bootstrap code. If a failure occurs at this stage of the boot-up process, your Cisco device could very likely enter what is known as ROM Monitor or commonly called ROMmon.

ROMmon

In your travels, if you or someone else has ever coined the phrase "hit rock bottom" you have a general idea of what purpose ROMmon serves. The ROM Monitor is a very limited codeset that enables you to perform elementary functions to manually get the router or switch back to a functioning state. You can perform low-level diagnostics and even copy a new IOS file to the Cisco device over the console port.

TIP

Keep in mind that your default console speed is 9600bps, and a typical IOS file exceeds 16 megabits. If you need to re-copy a working IOS to the Cisco device in ROMmon mode over the console, I recommend changing the default console speed in ROMmon to a higher speed or taking a long lunch or dinner break.

ROMmon is also utilized during password recovery on a Cisco router to make it possible to tell the device manually to ignore any saved configurations (including the passwords). It is possible to force your Cisco device to go directly to ROMmon on boot by sending a break sequence in your terminal session in the first 60 seconds of bootup. You can tell you are in ROMmon mode if you are presented with a command prompt that looks like `rommon 1 >`. Any time you type a command in ROMmon, the number at the prompt increments by one (`rommon 2 >`, `rommon 3 >`, and so on).

IOS Loading

Objective:

Describe how the configuration register and `boot system` commands modify the router boot-up sequence

Up to this point, the Cisco router or switch has performed only initial diagnostics. With that being said, the IOS itself still has not been located or loaded. The bootstrap's programming

has a specific search order in which it typically follows to locate and load the IOS. I say "typically" because you can alter the natural order of things with the router or switch's startup process if you manipulate something called the configuration register.

Located in NVRAM, the configuration register is a 16-bit (4 hexadecimal characters) value that specifies how the router or switch should operate during initialization. For instance, 0x2102 (0x signifies all characters that follow are hexadecimal) is a common configuration register that specifies that the router or switch should boot in its typical fashion. However, if you manipulate certain characters in the configuration register, you can manually modify the startup process to load the IOS from locations other than the default. Specifically, the last hexadecimal character in the configuration register, known as the boot field, is the value that dictates where the bootstrap code can find the IOS. The possible boot field values are as follows:

- **0x2100**—When the boot field is a zero, the configuration register instructs the bootstrap to boot directly into ROM and load ROMmon.
- **0x2101**—If the boot field has a value of one, the router or switch boots into a mini IOS located in ROM and commonly referred to as RxBoot. RxBoot looks very similar to the normal IOS; however, it does not provide the majority of the IOS's services. This mini IOS provides just enough functionality to reach a TFTP server and download a working IOS to the Cisco device. You can easily determine you are in RxBoot if the prompt looks like **`Router(boot)>`** in a router or **`Switch(boot)>`** in a switch.
- **0x2102-0x210F**—When the last field in the configuration register is 2-F, the router or switch boots normally.

Assuming the configuration register is 0x2102 (meaning it has not been modified and the boot field value is 2-F), the next step for initialization is to have the bootstrap search the configuration located in NVRAM to see whether the Cisco administrator has placed a command telling the router or switch specifically where to boot. The tools to do this are known as `boot system` commands. For example, if you have previously configured your device and put in the `boot system tftp c2600-do3s-mz.120-5.T1 172.16.1.1` command, you have instructed the bootstrap to load the IOS file c2600-do3s-mz.120-5.T1 from a TFTP server located at 172.16.1.1.

NOTE

Do not confuse this step with loading the configuration. This is just a step in the IOS loading process that enables the bootstrap code to implement any configuration specifications you previously saved that told the device where to boot. The configuration itself is not loaded until after the IOS is located and running.

If the default configuration register is utilized and you have not configured the device with any `boot system` commands, the default action of the bootstrap is to load the first IOS file in Flash memory. After the file is found, it is decompressed and loaded into RAM. At this point, the IOS is successfully loaded and running on your Cisco device.

What would happen if the IOS image were corrupted or missing? As with many functions of Cisco devices, a couple of failsafes are put in place to keep the device in an operating state or a mode in which you can get it back to an operating state. Specifically, if the Cisco router or switch cannot locate a working IOS file, it broadcasts out all interfaces in the hopes that a backup IOS file is stored on a TFTP server on its connected segments. If there isn't a TFTP server or the TFTP server does not contain a valid IOS file, the next failsafe for the IOS is to go to RxBoot so you can manually locate a valid IOS and copy it to Flash for the next reboot. If RxBoot becomes corrupted, the device inevitably boots to ROMmon.

EXAM ALERT

If the IOS is corrupt or missing from Flash and there is no network connectivity to reach a TFTP server, RxBoot in ROM is loaded. If RxBoot is missing or corrupt, the router or switch boots to ROMmon.

Configuration Loading

With the IOS loaded, the router or switch is now able to apply any saved configuration parameters. NVRAM is the first location where the device searches for the configuration. Here, a file called `startup-config` contains all the previous configurations that were present the last time an administrator saved the configuration. As the name states, this is the configuration that is loaded each time the Cisco device starts up. Similar to the IOS, after this configuration file is found, it is loaded into RAM as well. After the configuration is loaded and running at this point, it is conveniently referred to as `running-config`.

EXAM ALERT

The running-config is the active configuration running in RAM.

Cisco devices do not ship with a stored startup configuration, which is why you have to initially configure Cisco devices through some means of out-of-band management such as the console or auxiliary port. So the question begs, what happens when you initially turn on a new Cisco router or switch, or if someone erases the `startup-config`?

Many Cisco devices attempt to do an autoinstall by downloading a configuration file from an active TFTP server (similarly to the IOS) when they detect that the `startup-config` is not

located in NVRAM. Typically, these files contain enough configuration parameters (such as IP addresses for interfaces) for you to Telnet into the device and configure the remaining parameters. If the Cisco device finds an autoinstall configuration file from a TFTP server, the device loads the file and makes that the `running-config`. On the chance that you were not proactive enough to have an autoinstall configuration on your TFTP server, the router or switch prompts you for something called *Setup Mode*.

EXAM ALERT

It is imperative that you can identify the steps that a switch or router follows during initialization, the memory or device architectures where these steps occur, and the fallback sequences when a failure has occurred in the boot-up sequence.

Setup Mode

With non-CCNA technicians in mind, Cisco created Setup Mode so you can build a working configuration on a device without having to memorize the nuances of the CLI of the IOS. Setup Mode is a friendly interactive dialog in which the IOS asks the administrator questions about common configuration parameters that enable the Cisco device to have basic operations. Illustrated in Figure 6.2, the Setup Mode dialog initially asks you whether you wish to continue with Setup Mode. If you answer "no" to this question, you exit out of Setup Mode and are brought immediately to a CLI EXEC session. In addition, if you want to cancel at any point in the Setup Mode and get to the command prompt, you can use Ctrl+C to terminate the setup dialog. After you complete all questions, Setup Mode displays the parameters that you specified and asks you whether you want to use this configuration. If you answer "yes," the Cisco device saves your configuration and applies the settings to the device's operations.

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: CCNA
```

FIGURE 6.2 Setup Mode dialog.

EXAM ALERT

Remember that there are several ways to exit out of Setup Mode. You can answer "no" to the setup dialog prompt or use Ctrl+C at any point while in Setup Mode.

TIP

Throughout the configuration with the IOS, you may encounter several different types of interactive dialogs similar to Setup Mode. To save yourself from unnecessary typing, you can use the default value that is located in the brackets to answer any single-answer question by simply hitting the Enter key. For example, notice in Figure 6.2, the `Enter host name` prompt contains the word `Router` in brackets. If you were to press the Enter key at that prompt, this Cisco router would have a host name of Router.

Password Recovery

As the next chapter explains, you can secure access to your Cisco devices in several ways. In times where you inherit a pre-configured device or accidentally forgot or mis-configured a password, you need some loophole in the boot-up process that enables you to regain access to the device. Once again, the configuration register plays a pivotal part in the quest to manipulate the natural order of Cisco device initialization.

The third character in the configuration register enables you to tell the device to ignore any configurations that might be saved in NVRAM. If this field is changed from a 0 to a 4, the device inevitably boots into Setup Mode because the router or switch is fooled that there is no startup configuration. Now, with the configuration register changed to 0x2142, you can reconfigure the Cisco device creating your own unique passwords and save that configuration for future device startups.

CAUTION

Don't Forget the Natural Order Do not forget when performing password recovery to set your configuration register back to 0x2102. Failing to do so enforces your router to constantly ignore your configurations, causing your router or switch to repeatedly enter Setup Mode.

EXAM ALERT

Be sure to recognize that a configuration register of 0x2142 is a typical setting for performing password recovery.

REVIEW BREAK

To solidify the startup process, the following is a recap of the stages of the boot-up, any fallback procedures, and the memory locations involved:

1. POST, located in ROM, tests hardware.
2. Bootstrap, located in ROM, looks at the boot field in the configuration register to locate IOS. 0x2100 boots to ROMMON located in ROM. 0x2101 boots to RxBoot, located in ROM.

3. 0x2102-0x210F prompts bootstrap to parse startup-config in NVRAM for any boot system commands. If it finds any commands, it does what they say.
4. If no boot system commands are found, the first file in Flash is loaded. If no file is found in Flash, TFTP boots. If no IOS file is found from TFTP, the device goes to RxBoot in ROM. If no RxBoot is found, the device goes to ROMmon mode.
5. After IOS is loaded, the configuration register is checked. If it is 0x21**4**2, ignore `startup-config` in NVRAM. If it is 0x2102, load `startup-config` in NVRAM. If there is no `startup-config`, TFTP autoinstall. If no TFTP autoinstall configuration is found, enter Setup Mode.

Challenge

As you read in this chapter, be aware that many operations are occurring behind the scenes when you gain access to a Cisco device and turn it on. In this challenge, I want you to logically think through what is occurring at each stage of the boot-up process and identify the memory architectures that are involved given the following scenario:

Your night administrator planned to upgrade the IOS on your company's router last night. When you came in to work the next morning, you saw a written note from the night admin frantically explaining how he began the IOS upgrade, but he accidentally kicked out the power cord mid-upgrade and does not know what to do. Unfortunately, the IOS upgrade had to erase the IOS image file in Flash memory to make room for the new IOS. You do not have any TFTP servers on your network.

1. You must initially gain access to the device. Because the IOS cannot be loaded, what is the most logical way to gain an EXEC session?
2. When you turn on the device, what is the first thing your router will do and what memory is involved?
3. The default configuration register is configured, so where will the bootstrap look first to locate the IOS?
4. If you have not made any previous configurations telling the router how to boot, where will it look next?
5. Because the file isn't complete here, what is the first fallback failsafe?
6. Knowing that will fail, in what mode will you be and in what part of memory is that located?
7. What will the prompt look like?

Challenge Answer

To gain access to a non-functioning device, you will need to use some means of out-of-band management such as the console or the auxiliary port. When the device is powered on, the POST in ROM tests the hardware. Because the configuration register is 0x2102 (the default), the router searches for `boot system` commands in the startup-config. Because there are no configurations stating where to boot, the router looks into Flash. Unfortunately, the Flash memory does not have a complete IOS because the upgrade process was interrupted. With that being said, the router tries to locate an IOS file on a TFTP server. Because the scenario mentioned that there are no TFTP servers on the network, the router falls back to RxBoot in ROM, which displays a prompt similar to `Router(boot)>`.

Navigating the IOS

Objective:

Describe the purpose and fundamental operation of the internetwork operating system (IOS)

By now, you have a new-found love and respect for your Cisco equipment after knowing all the work that occurs when you turn on your router or switch. What better way to prove that love and respect but by mastering the IOS that the Cisco devices have so painstakingly found and loaded for your administration and configuration pleasure? This section looks at the hierarchical levels of the IOS and what type of interactivity you can encounter at each level.

EXAM ALERT

You will be able to eliminate several distracting incorrect answers in the exam by recognizing the level of the IOS hierarchy the commands will be found.

User EXEC

At your organization, you may have Level 1 technicians who are not strong in Cisco fundamentals; thus, you want to ensure only that they have access to basic troubleshooting and statistics without worrying that they might change the configuration or cause some other network catastrophe. Because a multitude of administrators might need to gain access to these Cisco devices, it makes sense to ensure that the first level of IOS hierarchy they encounter is somewhat limited in the extent of what can be done. This is the nature of User EXEC.

In User EXEC, you are limited in the number and type of commands that are available to you. For instance, the majority of `show` commands are available at this level of the IOS hierarchy because they do not detrimentally affect the router or the switch to perform these commands.

In addition, you can test IP connectivity to other devices with `ping` as well as remotely administer other devices or troubleshoot all the way up to Layer 7 with Telnet. The Cisco IOS prompt for User EXEC is signified by the greater than sign (>) following the hostname of the Cisco device. For example, a Cisco router and switch with their default hostnames would look like `Router>` and `Switch>`, respectively. Figure 6.3 displays the commands that you have available at User EXEC.

```
Router>?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  mrinfo           Request neighbor and version information from a multicast
                   router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  set              Set system parameter (not config)
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  where            List active connections
  x28              Become an X.28 PAD
```

FIGURE 6.3 User EXEC command display.

Privileged EXEC

Assuming you need to acquire more functionality from your Cisco devices beyond basic troubleshooting and statistical displays, you have to have another layer of the Cisco IOS hierarchy in which you have access to all commands. Happily named, Privileged EXEC is the next level of the IOS, in which you have the same commands as you do in User EXEC, as well as some commands that can alter the Cisco device's functionality.

For example, in Privileged EXEC, you can perform `debug` commands that can show you hundreds of real-time routing and switching functions and report them to the console. Because this can cause quite a processing strain on the device, these commands are reserved for only those who can access Privileged EXEC. Additionally, some `show` commands such as `show startup-config` and `show running-config` can be seen only by those who should be able (privileged) to see the configuration of the devices (including passwords). Some other new and dangerous commands available in Privileged EXEC include `delete`, `clear`, `erase`, `configure`, `copy`, and `reload` (reboots the device), to name a few.

To gain access to Privileged EXEC, type the command **`enable`** from User EXEC. After you press Enter, the prompt changes from > to #, signifying that you are now in Privileged EXEC mode. Because anybody can read this section and learn how to get to these commands, it makes sense to have some way for the IOS to prompt for a password to authorize those who

truly should be granted access. The next chapter discusses how to apply these passwords to restrict who gains access from User EXEC to Privileged EXEC. To return back to User EXEC, the reverse command is `disable`.

Global Configuration

One of the commands that you can access through Privileged EXEC is `configure`. This means that we have to enter yet another level of the Cisco IOS to make any configuration changes to the Cisco device. By typing the **`configure terminal`** command, you are telling the Cisco IOS that you are going to configure the Cisco device via your terminal window. The new level you enter after you complete this command is called Global Configuration. You can recognize it by looking at the command prompt, which will reflect `Router(config)#` for routers and `Switch(config)#` for switches.

Figure 6.4 displays a partial output of just some of the commands that are available in Global Configuration. Note that the commands `delete`, `debug`, `clear`, `configure`, and `copy` do not show up in the list of commands. You have a different set of commands available to you at this level of the IOS versus Privileged and User EXEC. This means that you must exit Global Configuration to use these commands as well as `show`, `reload`, and other Privileged EXEC-specific commands.

Of equal note, after you enter a command in the IOS, it is immediately applied to `running-config` and applied to the device's operation. The configurations are not listed and then applied later like batch files or executed compiled programs. Configuration help is shown in Figure 6.4.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#?
Configure commands:
  aaa                     Authentication, Authorization and Accounting.
  access-list             Add an access list entry
  alias                   Create command alias
  alps                    Configure Airline Protocol Support
  arp                     Set a static ARP entry
  async-bootp             Modify system bootp parameters
  autonomous-system       Specify local AS number to which we belong
  banner                  Define a login banner
  boot                    Modify system boot parameters
  bridge                  Bridge Group.
  bstun                   BSTUN global configuration commands
  buffers                 Adjust system buffer pool parameters
  busy-message            Display message when connection to host fails
  call-history-mib        Define call history mib parameters
  cdp                     Global CDP configuration subcommands
  chat-script             Define a modem chat script
  clock                   Configure time-of-day clock
  config-register         Define the configuration register
  controller              Configure a specific controller
  default                 Set a command to its defaults
  default-value           Default character-bits values
  dial-control-mib        Define Dial Control Mib parameters
  dial-peer               Dial Map (Peer) configuration commands
  dialer                  Dialer watch commands
  dialer-list             Create a dialer list entry
  dlsw                    Data Link Switching global configuration commands
  dnsix-dmdp              Provide DMDP service for DNSIX
  dnsix-nat               Provide DNSIX service for audit trails
```

FIGURE 6.4 Partial Global Configuration command display.

EXAM ALERT

Newer releases of Cisco IOS are making it possible to utilize some of these commands across the levels of the Cisco IOS hierarchies. However, for exam purposes, put on a pair of Cisco horse blinders to this new functionality and focus on the original levels and syntaxes described throughout this book.

As the name states, any configuration that is applied in this level applies globally to the Cisco router or switch. Here we can perform configuration tasks such as changing the hostname of the router or switch, creating a login banner, creating a password to prompt users trying to gain access to Privileged EXEC, and many others. It is also at this level of the Cisco IOS hierarchy that you can enter several different sub-configuration modes to apply specific configurations for things such as interfaces, routing protocols, and EXEC lines (which are discussed throughout this book).

Interface Configuration

Directly from Global Configuration, you can configure interface-specific commands that apply only to interfaces specified in the configuration. Now you can enable the interfaces, assign IP addresses, set speeds, and configure other interface commands. Once again, the commands that are available at this sub-configuration level of the IOS are not applicable at Global Configuration or Privileged EXEC and User EXEC.

To configure an interface, you must specify the interface you want to configure. If the device has fixed (non-modular) interfaces, you simply specify the type of interface followed by the interface number (and remember Cisco routers start their numbering schema with 0). For example, the 1600 series router has a fixed ethernet interface that cannot be removed from the router. To configure that interface, you type **`interface Ethernet 0`** from Global Configuration. In modular devices, you may have to specify the module number as well as the interface number because these devices can change functionality depending on the type of module inserted into them. For example, to configure the second WAN serial interface on the first module on a 3600 series router, you would input **`interface serial 0/1`** where `0` is the module number (first module starts with 0) and `1` is the interface. The prompt in Interface Configuration Mode is displayed as `Router(config-if)#`, regardless of the interface type. This means you must keep track of what interface you are configuring because the prompt does not specify the type.

Line Configuration

Also accessed from Global Configuration, line configurations are specific to those EXEC lines through which a user can gain access to the Cisco device. Specifically, you can configure options such as logins and passwords for a user trying to gain User EXEC access to the console and auxiliary ports, as well as the 5 vty (virtual teletype) Telnet lines into a router or switch. From Global Configuration, you must utilize the keyword, `line`, followed by the

EXEC line you want to configure. For example, to configure console-specific commands, you would type **`line console 0`** from Global Configuration. The prompt changes to `Router(config-line)#`, regardless of the line you are configuring.

Context-Sensitive Help

Even though the Cisco IOS is a command-line interface, it is not without its help features to help you through your navigation of the IOS. Specifically, to see what commands are available at any level of the IOS, you can use the help feature of the IOS, the question mark. By typing **`?`** (no Enter keystroke necessary) at any level of the IOS, you get a listing of all the commands available and a brief description of the command, such as you saw in Figures 6.3 and 6.4.

Quite often, the list of available commands may extend beyond one terminal screen. This is apparent because the string `--More--` is displayed at the bottom of the list on the screen. To see the next page of listed commands, you can press the space bar and the command list scrolls another terminal screen's length. If you prefer to see the commands line by line, you can keep hitting the Enter key and it displays only the next command each time you press it. On the chance that you have found the command you were looking for in the list, you can hit any key (pause for inevitable "where's the any key?" joke) to get back to the command prompt.

In some instances, you may not recall the command that you are looking for, but you do remember the first letter of the command. Let's say, for example, the command is in Global Configuration and starts with the letter *l*. You could use the question mark and scroll through all the commands; however, the IOS enables you to see the commands starting with *l* if you type the letter, followed immediately by the question mark (no space in between), as illustrated in Figure 6.5. Similarly, if you remembered that the command started with *log*, you can type those characters, followed immediately by the question mark, to see the commands `logging` and `login-string`.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#l?
lane     line          lnm  locaddr-priority-list  location
logging  login-string

Router(config)#l
```

FIGURE 6.5 Global Configuration commands output starting with *l*.

Keep in mind that many commands in the IOS require a string of keywords to comprehend what you are trying to achieve with the command. For instance, if I was searching for the command `logging` and hit the Enter key, the IOS would report back an error to the terminal screen that the command was incomplete because it does not understand where I want to send my logging information. If you are unsure of the commands available, once again, you use the question mark for command help. In this case, you must put a space after the first keyword followed by the question mark. The IOS then displays a list of commands that are valid after the keyword `logging`, as displayed in Figure 6.6.

```
Router(config)#logging ?
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  console              Set console logging level
  facility             Facility parameter for syslog messages
  history              Configure syslog history table
  monitor              Set terminal line (monitor) logging level
  on                   Enable logging to all supported destinations
  source-interface     Specify interface for source address in logging
                       transactions
  trap                 Set syslog server logging level

Router(config)#logging
```

FIGURE 6.6 Valid commands following the keyword `logging`.

EXAM ALERT

In the simulations on the Cisco exam, you can use ? for help when configuring or troubleshooting the Cisco device. If you get stuck in a simulation, utilize the help feature extensively because you do not get docked points for using this feature.

Abbreviations

To make things easy for administration, the Cisco IOS enables you to abbreviate commands as long as you type enough characters for the IOS to interpret the command that you want to input. For instance, the previous example involved trying to locate the command that started with *l* in Global Configuration. Because there were several commands that started with *l*, you would need to type in more characters to find the `logging` command. Specifically, you would need to type **`logg`**, which is just enough characters for the IOS to understand that you want to use the `logging` command. If you want the IOS to complete typing the command for you, you can hit the Tab key and it autocompletes the command when you provide enough characters.

EXAM ALERT

The simulations on the exam support some of the abbreviations; however, not all of them are supported. With that being said, it is a good idea to be able to type the entire command in case it is not supported for abbreviation. The Tab autocomplete, however, is not supported on the exam simulations.

EXAM ALERT

Some multiple-choice questions and answers may show you the completed command, whereas others may show you the abbreviated one. Do not discount a valid answer if the full command syntax is not used.

Shortcut Keys

To make terminal editing simpler and faster, Cisco has created several shortcut keystrokes that can speed up IOS navigation. The most useful of these shortcuts enables you to cycle through your command history to re-use or edit previously typed commands. You can use both the up and down arrow keys or Ctrl+N and Ctrl+P (if arrow keys are not supported at your terminal) to cycle through the last 10 commands in the history buffer relative to the level of the IOS you

are currently located. Table 6.2 lists some other useful terminal editing keystrokes that will help you navigate within a command line.

TABLE 6.2 Cisco IOS Terminal Editing Keystrokes

Keystroke	Function
Ctrl+A	Move the cursor to the beginning of the command line.
Ctrl+E	Move the cursor to the end of the command line.
Ctrl+B	Move the cursor back one character.
Ctrl+F	Move the cursor forward one character.
Esc+B	Move the cursor back one word.
Esc+F	Move the cursor forward one word.

The terminal editing keys discussed so far are very useful for moving within a particular level of the IOS. However, you need to know how to navigate back from those different levels of the Cisco IOS. Namely, if you need to go back one level of the IOS, simply type the command `exit`. For instance, if you are in the Interface Configuration mode of the IOS and you need to go back to Global Configuration, just type **`exit`**, and your prompt display should change from `Router(config-if)#` to `Router(config)#`.

Suppose you are back in the interface configuration and you need to ping or traceroute to your neighbor or do a `show` command to verify that the interface is working. Recall that this variety of commands can be performed only in Privileged EXEC or User EXEC. To return to these levels of the IOS hierarchy, you can type **`exit`** until you are all the way back. You can also use the keystroke Ctrl+Z or the keyword `end`, which will automatically take you back to Privileged EXEC, regardless of how deep in the configuration levels you happen to be.

Common Syntax Errors

As mentioned before, the IOS reports back error messages if you have not provided the correct syntax for a command. The three syntax error messages that you may encounter are as follows:

- **Ambiguous Command**—This error is displayed when you have not typed enough characters for the IOS to distinguish which command you want to use. In other words, several commands start with those same characters, so you must type more letters of the command for the IOS to recognize your particular command.
- **Incomplete Command**—The IOS has recognized your keyword syntax with this error message; however, you need to add more keywords to tell the IOS what you want to do with this command.
- **Invalid Input**—Also known as the "fat finger" error, this console error message is displayed when you mistype a command. The IOS displays a caret mark (^) at the point up to which the IOS could understand your command.

Figure 6.7 displays an example for each of these three error console messages. Also notice that this configuration snapshot now includes abbreviations to get into Privileged EXEC and Global Configuration.

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#l
% Ambiguous command:  "l"
Router(config)#logging
% Incomplete command.

Router(config)#loggning
                   ^
% Invalid input detected at '^' marker.
```

FIGURE 6.7 Error console messages.

STEP BY STEP

6.1 Navigating the IOS

1. Go into Privileged EXEC by typing **`enable`** or **`en`** (or any abbreviation you feel comfortable with). Use Figure 6.8 as a loose reference of what the output might look like.
2. Enter Global Configuration by typing **`configure terminal`** or **`config t`**.
3. Enter the Line Configuration mode for the console by typing **`line console 0`** or **`line con 0`**.
4. Look at the list of commands available by using **`?`**.
5. Press the space bar to cycle page by page or Enter to cycle line by line.
6. Return back to Global Configuration by typing **`exit`**.
7. Enter the interface configuration for serial 0/0 by typing **`interface serial 0/0`** or **`int ser 0/0`**.
8. Exit back to Privileged EXEC by typing **`Ctrl+Z`** or **`end`**.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line con 0
Router(config-line)#?
Line configuration commands:
  absolute-timeout        Set absolute timeout for line disconnection
  access-class            Filter connections based on an IP access list
  activation-character    Define the activation character
  autocommand             Automatically execute an EXEC command
  autocommand-options     Autocommand options
  autohangup              Automatically hangup when last connection closes
  autoselect              Set line to autoselect
  data-character-bits     Size of characters being handled
  databits                Set number of data bits per character
  default                 Set a command to its defaults
  disconnect-character    Define the disconnect character
  dispatch-character      Define the dispatch character
  dispatch-machine        Reference a TCP dispatch state machine
  dispatch-timeout        Set the dispatch timer
  domain-lookup           Enable domain lookups in show commands
  editing                 Enable command line editing
  escape-character        Change the current line's escape character
  exec                    Start an EXEC process
  exec-banner             Enable the display of the EXEC banner
  exec-character-bits     Size of characters to the command exec
  exec-timeout            Set the EXEC timeout

Router(config-line)#exit
Router(config)#int serial 0/0
Router(config-if)#^Z
Router#
03:47:27: %SYS-5-CONFIG_I: Configured from console by console
```

FIGURE 6.8 IOS navigation step-by-step output.

Chapter Summary

This chapter delved into the many intricacies surrounding the Cisco internetwork operating system. Specifically, you learned at least five ways to gain access to the IOS. The two out-of-band methods are through the console and auxiliary interface. In-band methods such as Telnet, HTTP, and SSH require some level on configuration of the Cisco devices before you can remotely manage them.

To load the IOS, Cisco routers and switches have to complete a series of systematic stages. Initially, the device tests the hardware and loads the bootstrap code, both located in ROM. If the configuration register boot field has not been manipulated (values 0x2-0xF), then the bootstrap queries the `startup-config` in NVRAM for any `boot system` commands. If no commands are present, the first file in Flash memory is loaded into RAM. If the file in Flash is missing or corrupt, the Cisco router or switch broadcasts for help to any local TFTP servers. If that fallback fails, the router or switch returns back to ROM and loads RxBoot. After the IOS is loaded, the Cisco device can load the startup configuration in NVRAM (assuming you didn't change the configuration register to 0x2142 for password recovery). If the startup configuration is not present, the router or switch tries to autoinstall from a TFTP server. If that fails, the device enters the configuration dialog, Setup Mode.

If you were to cancel out of Setup Mode by answering "no" or typing Ctrl+C, you would give yourself the opportunity to conquer the mighty mountain of the Cisco IOS navigation hierarchy because you would immediately enter into User EXEC mode. In User EXEC, you have limited functionality (the majority of `show` commands, `ping`, `traceroute`, `Telnet`, and so on) and would need to use the command `enable` to enter Privileged EXEC to gain access to all the commands at that particular level. From here, you can enter Global Configuration by typing **`configure terminal`** to configure parameters that apply to the entire device. Global Configuration can then be utilized as a jumping-off point to enter sub-configuration modes, such as for interfaces, EXEC lines, routing protocols, and many other sub-configuration modes.

At any point in the IOS, you can see the commands available by using `?` at the command prompt. If you were to get an ambiguous command error, the IOS requires that you enter more characters to a keyword because multiple commands might share those beginning characters. You can easily discover the commands that start with certain character by immediately typing **`?`** after those letters. Incomplete Command errors signify that the command string required more keywords to know what to do with the command keyword. To see the commands available after a specific keyword, you can also use the `?` preceded by a space to see what commands are valid. Invalid input errors indicate that the command was mistyped somewhere. In these situations, you can cycle through the previous commands by using the up and down

arrows or Ctrl+P and Ctrl+N. After you find the mistyped command, you can use other terminal editing keys to navigate the cursor to the point where the mistake was made. To exit configuration modes, you can type **`exit`** to go back a level at a time. To go directly to Privileged EXEC, type Ctrl+Z or **`end`**.

Key Terms

- configuration register
- boot field
- POST
- ROMmon
- RxBoot
- console port
- auxiliary port
- SSH
- bootstrap
- User EXEC
- Privileged EXEC
- Setup Mode
- `running-config`
- `startup-config`
- interface configuration
- line configuration
- terminal editing keys
- in-band
- out-of-band

Apply Your Knowledge

Exercises

6.1 Navigating a New Router

You have just received a new router that you will have to install at a customer's location in two days. To ensure you appear confident in your installation, you decide to take the router out for a test drive so you can be comfortable with the IOS navigation before arriving onsite.

This exercise assumes you have a router to utilize that is not in production.

NOTE

If you do not have an actual router, you can always follow along by using simulated software such as SemSim (www.semsim.com) or Boson's NetSim (www.boson.com). If your budget is tight, open up Notepad and type the commands as you would if you were in the router itself. Practicing these commands and understanding the level of IOS at which they should be typed are critical to your success in the CCNA exam and as a CCNA technician.

Estimated Time: 15 minutes

1. Plug the router into the power outlet and connect your console cable between your PC's COM port and the console port on the router.
2. Open your terminal program and set the settings for 9600 baud, 8 data bits, no parity bits, 1 stop bit, and no flow control.
3. Power on the router and notice bootstrap and IOS decompression from Flash output similar to Figure 6.9.

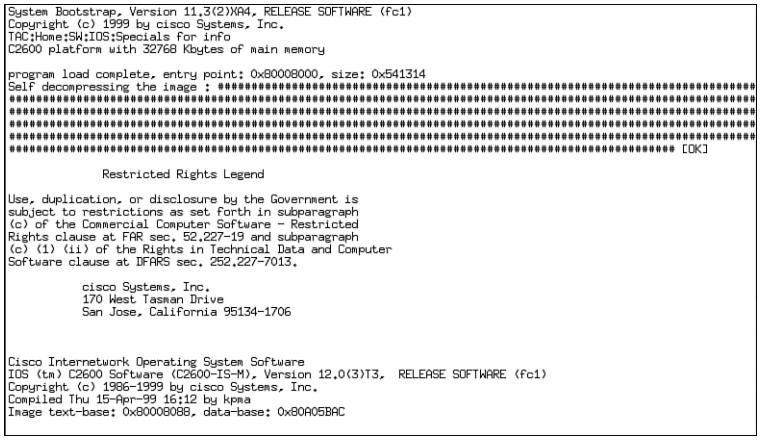


FIGURE 6.9 IOS bootstrap and IOS decompression.

4. Because this is the first time the router has been turned on, a startup-config is not present in NVRAM, so you will inevitably go to Setup Mode. Exit Setup Mode by answering "no" to the question, `Would you like to enter the initial configuration dialog? [yes/no]:`
5. In User EXEC, type **`enable`** to enter into Privileged EXEC.
6. Enter Global Configuration by typing **`configure terminal`**.
7. See what commands are available in this mode by using the question mark for help.
8. Type **`l`** and press Enter to see the ambiguous command error.
9. Type **`li`** to see the incomplete command error.
10. Type **`line consoul 0`**, purposely misspelling the word *console* to see the invalid command error.
11. Press the up arrow or Ctrl+P to cycle to the previous command.
12. Enter Ctrl+A to go to the beginning of the command.
13. Enter Esc+F to move the cursor forward one word.
14. Move the cursor forward, using Ctrl+F, until you are at a point where you can correct the spelling to *console*.

15. Exit back to Privileged EXEC by entering Ctrl+Z or type the command **end**.
16. Exit out of Privileged EXEC by typing **disable** or the keyword **exit**.

Review Questions

1. What is the effect of changing the configuration register?
2. Why would a Cisco administrator use `boot system` commands?
3. What are the memory components in a router and what purpose do they have in the booting process?
4. What cabling and terminal settings are required for out-of-band management?
5. What is the significance of having User EXEC mode in addition to Privileged EXEC mode?

Exam Questions

1. What type of cable would you connect to manage your Cisco device from the COM port of your PC?
   - ❍ **A.** Cross-over cable
   - ❍ **B.** Straight-through cable
   - ❍ **C.** Patch cable
   - ❍ **D.** Rollover cable

2. Which are two methods of exiting out of Setup Mode? (Choose 2.)
   - ❍ **A.** Ctrl+C
   - ❍ **B.** Ctrl+Z
   - ❍ **C.** Answer no
   - ❍ **D.** Type `end`

3. You have just been given a router that will not save its configuration. As you boot up the router, you confirm that despite saving the configurations several times, the router enters Setup Mode consistently. What might be a possible cause?
   - ❍ **A.** Flash memory is corrupt.
   - ❍ **B.** TFTP Server is down.
   - ❍ **C.** The configuration register is 0x2100.
   - ❍ **D.** The configuration register is 0x2142.

4. What and where are the commands that can alter the location for the bootstrap IOS process?

- ❍ **A.** `boot system` command, NVRAM memory
- ❍ **B.** `boot enable` command, NVRAM memory
- ❍ **C.** `boot strap` command, Flash memory
- ❍ **D.** `boot system` command, Flash memory

5. Assuming no boot commands, what is the default location of the IOS and what is the order of the two fallbacks?

- ❍ **A.** NVRAM, TFTP then ROM
- ❍ **B.** Flash, TFTP then ROM
- ❍ **C.** ROM, Flash then TFTP
- ❍ **D.** TFTP, Flash then ROM

6. Which of the following is considered a typical default configuration register?

- ❍ **A.** 0x2100
- ❍ **B.** 0x2142
- ❍ **C.** 0x2101
- ❍ **D.** 0x2102

7. Which of the following are in-band management EXEC methods? (Choose 2.)

- ❍ **A.** SSH
- ❍ **B.** FTP
- ❍ **C.** Console
- ❍ **D.** Telnet
- ❍ **E.** Auxilliary

8. Which of the following valid commands assign an IP address to an interface from Interface Configuration mode?

- ❍ **A.** `Router(config)#ip address 192.168.1.1 255.255.255.0`
- ❍ **B.** `Router(config-if)#ip address 192.168.1.1 255.255.255.0`
- ❍ **C.** `Router#ip address 192.168.1.1 255.255.255.0`
- ❍ **D.** `Router>ip address 192.168.1.1 255.255.255.0`
- ❍ **E.** `Router(config-line)#ip address 192.168.1.1 255.255.255.0`

9. If your network does not have a TFTP server and your router's configuration was erased, what will the prompt look like when you reboot?

   - ❍ **A.** `rommon 1 >`
   - ❍ **B.** `Router(boot)>`
   - ❍ **C.** `Would you like to enter the initial configuration dialog? [yes/no]:`
   - ❍ **D.** The router would not be able to boot.

10. Which two commands will return you to Privileged EXEC? (Choose 2.)

    - ❍ **A.** Ctrl+Z
    - ❍ **B.** `end`
    - ❍ **C.** `disable`
    - ❍ **D.** Ctrl+C

11. Which four components are located in ROM? (Choose 4.)

    - ❍ **A.** bootstrap
    - ❍ **B.** POST
    - ❍ **C.** `startup-config`
    - ❍ **D.** IOS file
    - ❍ **E.** ROMmon
    - ❍ **F.** `running-config`
    - ❍ **G.** RxBoot

Answers to Review Questions

1. By changing any of the values in the configuration register from its default value of 0x2102, you are altering how the router or switch operates during initialization. The last hexadecimal field in the configuration register is the boot field. This value determines whether the device boots to ROM and loads the ROMmon (0x0) or RxBoot (0x1) program. Values of 0x2-0xF indicate that the device parses the startup configuration in NVRAM for any `boot system` commands. If the *third* hexadecimal character in the configuration register is a 0x4, the device ignores the startup configuration in NVRAM and enters the Setup Mode dialog.
2. The `boot system` commands provide flexible means of specifying from where to load an IOS. This is especially useful if you require specifying a specific IOS file to load in Flash (if multiple files exist) or on a TFTP server.

3. ROM contains the POST program and the bootstrap code for the initial stages of the booting process. ROM also contains the RxBoot mini-IOS for IOS failure fallback and ROMmon for RxBoot failure. Flash memory stores the IOS files. The configuration register is stored in NVRAM along with the startup configuration that contains any `boot system` commands.
4. The console and AUX ports both use the rollover cable. The terminal settings should reflect the following parameters: 9600 baud, 8 data bits, no parity bits, 1 stop bit, and no flow control.
5. User EXEC is useful if you have to give access to technicians who need rights to basic verification commands. Privileged EXEC enables access to the remaining command modes, including those commands that can affect the router or switch's operations.

Answers to Exam Questions

1. **D**. The cable to connect your terminal to the Cisco device's console or auxiliary port is a rollover cable. Answers A, B, and C are cables that are used for ethernet networking.
2. **A, C**. To exit out of Setup Mode, you must answer "no" to the `Would you like to enter the initial configuration dialog? [yes/no]:` question, or enter Ctrl+C at any prompt. Ctrl+Z and the End key are shortcuts to exit back to Privileged EXEC.
3. **D**. When the third hexadecimal character in the configuration register is a 4, the `startup-config` is ignored. This is a useful utility if you are doing password recovery; however, it is important that you remember to change it back to 0x2102. A is incorrect because the configuration is not stored in Flash. B is not viable because the Cisco device looks for a config on the TFTP only if the `startup-config` is missing. C will force the router or switch into ROMMON mode, which means the configuration never gets loaded because the IOS needs to be loaded first.
4. **A.** The `boot system` commands located in the `startup-config` in NVRAM can manually force the router or switch to boot the IOS from somewhere other than its default locations.
5. **B**. When no `boot system` commands are used, the bootstrap loads the first file in Flash memory. If that file is missing or corrupt, it tries to load an IOS from a TFTP server first. If there is no network connectivity or TFTP server present, the device enters RxBoot in ROM.
6. **D**. A normal configuration register is 0x2102. A forces the router or switch into ROMmon. B ignores the `startup-config`. C forces the router into Rx Boot.
7. **A, D.** The three in-band management session methods are SSH, Telnet, and HTTP. Answers C and E are out-of-band; B is not a management session method.
8. **B**. Without even discussing the actual configuration of the command, the question stated that it must be in Interface Configuration mode, which means the command prompt will look like `Router(config-if)#` or `Switch(config-if)#`.
9. **C**. Without a TFTP for autoinstall and with the startup-config missing, the router or switch enters Setup mode, which prompts you with `Would you like to enter the initial configuration dialog? [yes/no]:`. Answer A is the ROMmon prompt, and B is the prompt for RxBoot.

10. **A, B.** Ctrl+Z and End returns you to Privileged EXEC, no matter in which level of the configuration hierarchy you are. C returns you to User EXEC from Privileged EXEC mode. D is used to exit out of Setup Mode.

11. **A, B, E, G.** POST, bootstrap code, ROMmon, and RxBoot all reside in ROM. Startup-config is located in NVRAM, and running-config is located in RAM. The IOS file is typically located in Flash memory.

Suggested Readings and Resources

1. Valentine, Michael and Whitaker, Andrew. *CCNA Exam Cram 2*. Que Publishing, 2005.

2. Boney, James. *Cisco IOS in a Nutshell*. O'Reilly Publishing, 2001.

3. "Using the Command-Line Interface," www.cisco.com.

4. "Rebooting" for an explanation of the booting process, www.cisco.com.

7

CHAPTER SEVEN

Basic Cisco Configurations

Objectives

This chapter covers the following Cisco-specified objectives for the "Technology," "Implementation and Operation," and "Troubleshooting" sections of the CCNA exam:

Configure a router for additional administrative functionality

Assign IP addresses

Manage system image and device configuration files

Perform an initial configuration on a router and save the resultant configuration file

Perform an initial configuration on a switch

Use a subset of Cisco IOS commands to analyze and report network problems

Use embedded Layer 3 through Layer 7 protocols to establish, test, suspend, or disconnect connectivity to remote devices from the router console

Use embedded Data Link layer functionality to perform network neighbor discovery and analysis from the router

Determine IP addresses

- Passwords and banners add administrative functionality and security to the configuration.
- Configuring IP addresses is a routine responsibility of the administrator.
- A TFTP server allows back up and restoration of the IOS and configurations.
- Router configuration and saving configurations are other routine tasks.
- Configuration parameters enhance Layer 2 functionality.
- The `show` commands are essential troubleshooting tools.
- Telnetting between devices confirms Layer 4 and Layer 7 functionality.
- Cisco Discovery Protocol (CDP) gathers statistics about neighboring devices.
- CDP discovers the IP addresses of neighboring devices.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- As you are reading through each section, keep in mind on which level of the Cisco IOS these commands exist.
- If possible, practice the syntax of every command discussed throughout this chapter (and book) with real or simulated Cisco equipment.
- Pay close attention to the functionality associated with these commands. It is tempting to focus too hard on the command syntax itself, which ultimately makes you lose focus on the reason you are learning about the command in the first place. The CCNA exam tests you on both why you are typing the command and how to type it.
- Complete the Challenge Exercises throughout the chapter and the Exercises at the end of the chapter. The exercises will solidify the concepts that you have learned in the previous sections.
- Complete the Exam Questions at the end of the chapter. They are designed to simulate the type of questions you will be asked in the CCNA exam.

Introduction

Now that you have a firm understanding how to navigate the Cisco IOS, it is time to put that knowledge to the test by exposing yourself to the huge number of commands that are available for configuration and verification. This chapter is specifically arranged to ensure that you understand on which layer of the Cisco IOS navigation hierarchy each command resides. With the chapter divided into these sections, you will learn to apply these commands correctly if presented with a Cisco configuration objective for the exam and the real world. Additionally, you should notice similarities and form an association between the syntax and functionality of the commands and the level of IOS to which they can be applied and utilized. Having this knowledge at your fingertips will prove invaluable when configuring simulations or eliminating distracting answers on the CCNA exam.

Global Configuration

As mentioned in the previous chapter, Global Configuration commands affect the entire router or switch's operations. Recall also that you enter Global Configuration by typing **`configure terminal`** from Privileged EXEC, which changes the prompt to `Router(config)#` or `Switch(config)#`. This section looks at the syntax and functions of some basic Global Configuration parameters that you can configure in a switch or a router.

NOTE

Any configuration command discussed throughout this entire book can be negated or removed if you type the keyword `no`, followed by the command again. The same syntax rules must apply when removing the command (you must type the command correctly and you must be in the correct level of the IOS hierarchy where the original command exists).

Altering the Boot Sequence

The previous chapter discussed two means of altering the default boot sequence of a switch or a router. Namely, you learned that by changing certain fields in the configuration register, you can force the Cisco device to perform actions such as booting from ROM and ignoring the startup configuration. In Global Configuration, the `config-register` command enables you to manipulate those fields and ultimately change the normal default operations of the router or switch.

For example, if you wanted to manipulate the configuration register to enter RxBoot on the next reboot, the Global Configuration command would look like this on a router:

```
Router(config)#config-register 0x2101
```

On the next boot, this router instructs the bootstrap to immediately boot into RxBoot in ROM. The prompt displays `Router(boot)>`, signifying that the manipulation was successful and you are indeed in the mini-IOS.

CAUTION

Don't Change Configuration Register Fields Unless Necessary In this book, we mention only a couple of the boot field values and the configuration field values. Do not randomly experiment with the configuration register to see the outcome. You could very well change a configuration parameter that will cause the router or switch to boot abnormally, change the console speed (leaving you guessing what speed you need to use to get terminal connectivity), or not boot at all.

If you accidentally change these settings, you can try to change the configuration register back by forcing the device to go directly to ROMmon mode on boot-up. From a console connection, turn on the device and send a break sequence (Ctrl+Break Key in HyperTerminal) from your terminal window in the first 60 seconds. You see the `rommon 1 >` prompt, indicating that you are in ROM Monitor. From here, enter the following command:

```
rommon 1 >confreg 0x2102
```

You should see a response similar to the following:

```
You must reset or power cycle for new config to take effect
rommon 2 >
```

At this point, you can recycle the power on the device or type the ROMmon-specific command, `reset`, to reboot the device because you have restored the default configuration register to ensure normal operations.

The second Global Configuration command to globally affect the startup sequence that was mentioned in the previous chapter is the `boot system` command. With this command, you can optionally instruct the bootstrap to boot from specific locations, and even tell it which file to load if there are multiple IOS files at that location. Three different examples of the boot system commands are as follows:

```
Router(config)#boot system tftp c2600-do3s-mz.120-5.T1 172.16.1.1
Router(config)#boot system flash c2600-do3s-mz.120-5.T1
Router(config)#boot system rom
```

The first command instructs the bootstrap to locate the IOS on the TFTP server located at 172.16.1.1. The second `boot system` command configures the bootstrap to specifically load the IOS file `c2600-do3s-mz.120-5.T1` in the possible event that Flash has multiple IOS image files on it. The last `boot system` command forces the router to boot directly into ROM upon initialization. In examples where you have multiple boot system commands in a sequence, such as the example just given, the bootstrap tests each command in successive order until it successfully locates and loads an IOS.

Changing the Hostname

Objective:

Configure a router for additional administrative functionality

Throughout this and the last chapter, you saw that the default prompt for a router starts with the hostname `Router`, and the hostname `Switch` for a Catalyst switch. You should change the hostname to uniquely identify the Cisco device in your internetwork. This is especially useful if you are using Telnet to remotely manage multiple devices and you need to identify to which device you are connected. The syntax for the command to change the hostname of the Cisco device is `hostname`, followed by the name you have chosen (up to 25 characters) as illustrated here:

```
Router(config)#hostname CCNA2621
CCNA2621(config)#
```

Creating a Login Banner

Objective:

Configure a router for additional administrative functionality

It is advisable to display a login banner as a means to provide notice of acceptable use or as a warning to anyone attempting to gain unauthorized access to your Cisco device. In Cisco terms, this is known as the message of the day. This message is displayed to any user attempting to gain an EXEC session on all terminal lines in the IOS. An example configuration for the message of the day is as follows:

```
CCNA2621(config)#banner motd # This is a private system and may be accessed only by
➥ authorized users.  Unauthorized access is strictly prohibited and will be
➥ enforced to the full extent of the law.#
```

Notice that the `banner motd` (message of the day) command example contains a # character before and after the message. This is known as a delimiting character and is used to inform the IOS where your banner begins and ends. This can be any character, so it makes sense to use a character that is not present in the banner itself. For instance, if the delimiting character were "v", the banner would be displayed as `This is a pri`.

EXAM ALERT

Remember that the command to configure a login banner is `banner motd`.

CAUTION

No Need for a Warm Welcome Be extremely careful of the message that you choose in your login banner. A login banner can be useful if you need to seek legal action against an intruder to your Cisco device. On the flip side, however, the wrong login banner can work against you. For example, if your login contains the word "welcome" or similar inviting words, this can be used as grounds for defense for an unauthorized user to gain access because it can be considered as invitation to your device.

Assigning a Password for Privileged EXEC Mode

Objective:

Configure a router for additional administrative functionality

Gaining access to Privileged EXEC essentially means you have access to all the functionality of the IOS, including those commands that can detrimentally affect the router or switch. With that being said, it makes sense to secure access to Privileged EXEC to ensure those who gain access are indeed skilled and authorized to do so. This is achieved in Global Configuration with the creation of an enable password, which prompts anyone attempting to access Privileged EXEC with a password that is known only by those who truly are privileged.

The command to assign a password to gain access to Privileged EXEC can be achieved with one of the following two commands:

```
CCNA2621(config)#enable password myenablepassword
CCNA2621(config)#enable secret mysecretpassword
```

TIP

Be careful not to accidentally put the additional keyword `password` after the `enable secret` command. Otherwise, your secret password would be "password," followed by your actual password. In addition, the commands are case sensitive, so make sure you don't accidentally put the wrong case in the command.

So what is the difference between the two commands? The `enable secret` password is secure because it utilizes a non-reversible one-way MD5 (Message Digest 5) cryptographic hash of the password so it cannot be deciphered by anybody who can see the configuration. On the other hand, the `enable password` command is in clear text and can be seen by anyone that gains access to that configuration. In practice, it is customary to utilize the `enable secret` command for the security that it provides over the `enable password` command. Figure 7.1 demonstrates a secure `enable password` configuration, and the resulting prompt that occurs when you try to re-enter Privileged EXEC.

```
CCNA2610>enable
CCNA2610#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CCNA2610(config)#enable secret giforgot
CCNA2610(config)#end
CCNA2610#
00:07:41: %SYS-5-CONFIG_I: Configured from console by console
CCNA2610#disable
CCNA2610>
CCNA2610>enable
Password:
```

FIGURE 7.1 Secure `enable password` example and output.

EXAM ALERT

When the `enable password` command and the `enable secret password` command are used in the same configuration, the `enable secret` command overrides the `enable password` command. For example, using the preceding configuration examples above, the password would be "mysecretpassword" to enter Privileged EXEC.

It is possible to encrypt the password used in the `enable password` command by using the following Global Configuration command:

```
CCNA2621(config)#service password-encryption
```

This command actually encrypts all clear text passwords in your configuration, including passwords you assign to the EXEC lines (discussed later). This is useful in case anyone happens to actually see your configuration because the password cannot be distinguished visually upon initial sight. Be advised, however, that the encryption used is a Cisco proprietary encryption, which is easily broken to reveal the actual password. When choosing between this method and the `enable secret` method for secure Privileged EXEC, use `enable secret` because its encryption is exponentially stronger.

EXAM ALERT

The `service password-encryption` command encrypts all clear text passwords in the configuration with a Cisco proprietary encryption.

Domain Name–Specific Commands

Quite often, you have to test connectivity or connect to a multitude of devices from your router or switch. Unless you have all their IP addresses memorized or you have a trusty topology map with you wherever you go, you might find it difficult to accurately recall their IP address information. To assist you when such challenges arise, the Cisco IOS can statically or dynamically support domain name resolution on the Cisco device. This way, you can refer to the devices by a recognizable hostname versus an IP address.

The command to create a static entry in the IOS configuration file is `ip host`. For example, given the following command:

```
CCNA2621(config)#ip host corerouter 172.16.1.1
```

The IOS automatically forms a name-to-IP association in a host table so that every time you refer to `corerouter`, it translates that hostname to the IP of 172.16.1.1.

In instances where there are far too many devices to create individual static host entries, you might be better suited to have a DNS server keep the hostname-to-IP records. With that infrastructure in place, you can have your Cisco device use these servers for the name translation. The command to specify the DNS sever(s) (up to 6) is the following:

```
CCNA2621(config)#ip name-server 172.16.1.254 172.16.1.100 172.16.1.2
```

Domain resolution is automatically enabled on your Cisco device. If you have not configured a DNS server, it tries to resolve hostnames by sending a broadcast out all its active interfaces. This can be irksome when you accidentally type a command in User or Privileged EXEC and the IOS attempts to resolve the command thinking that it is a hostname. To disable this feature, use the following command:

```
CCNA2621(config)#no ip domain-lookup
```

NOTE

If you happen to have IOS version 12.2 or later, the command was changed to the non-hyphenated command `no ip domain lookup`.

Line Configurations

Objective:

Configure a router for additional administrative functionality

This chapter previously discussed how to secure access to Privileged EXEC by using the `enable password` or `enable secret` command. However, this assumes that any administrators can still gain User EXEC to the Cisco device. The problem with this configuration is that you can send excessive pings or Telnet to another device from your router or switch in User EXEC. Because the ping and Telnet traffic are coming from your private router or switch, they might not be blocked by a security device such as a firewall. This section looks into how to secure access to the User EXEC by assigning a password on the EXEC lines into the Cisco device.

Securing Console Access to User EXEC

Console access necessitates that an admin have physical access to the device itself. If your Cisco router or switch is physically accessible to non-authorized personnel (not highly recommended), you should take preventative measures to add another level of security by having the devices prompt anybody trying to get to User EXEC via the console port for a password. The following three commands ultimately achieve that goal:

```
CCNA2621(config)#line console 0
CCNA2621(config-line)#login
CCNA2621(config-line)#password myconsolepassword
```

The first command navigates the IOS to a sub-configuration mode for the console port. The second command instructs the IOS to prompt anybody connecting to this EXEC line for a login, using the password chosen in the third command.

TIP

It does not matter if you type the `password` command before the `login` command. The important factor is that both commands are configured.

To add yet another additional level of security comfort, it is also advisable to have the IOS close the console session after so much time of inactivity (no typing) in the session. After the EXEC session is closed, the admin has to enter the console password (assuming the above console configuration was in place) to get into User EXEC again. This is generally useful for those emergency bathroom breaks that arise after a couple cups of coffee or those unscheduled fire drills.

By default, the console session closes after 10 minutes of inactivity which, unfortunately, is plenty of time for someone to jump on to your terminal and change passwords and lock you out if you are not present. To change that setting, use the `exec-timeout` command followed by the number of minutes and seconds the IOS should wait to time out. For example, if you want the console to close after 1 minute and 30 seconds of inactivity, the command should reflect the following:

```
CCNA2621(config-line)#exec-timeout 1 30
```

EXAM ALERT

The `exec-timeout` command identifies how long the EXEC terminal session will remain active when no commands are being typed. The syntax specifies the minutes followed by the seconds.

TIP

The IOS sends all alerts and notification messages to the console port by default. Unfortunately, this sometimes interrupts the command you are typing. To make your Cisco device more polite and stop interrupting you, use the logging synchronous command. After it is configured, the IOS waits until user input is returned before sending notifications to the terminal session.

Securing Auxiliary Access to User EXEC

If your organization has decided to allow remote terminal access to your Cisco device through an external modem or terminal server connected to the auxiliary port, you have added another means of getting to User EXEC that you must secure. The auxiliary port is slightly easier to connect than the console port because physical access is no longer a mandate. As long as you know the phone number to dial into the modem, you can gain access to a User EXEC session. This ease of access should be counterbalanced with security measures to ensure authorized users are connecting to this EXEC line.

Conveniently, the commands are practically identical to those used to secure a console connection. The only major difference is the navigation to the auxiliary port as opposed to the console:

```
CCNA2621(config)#line auxiliary 0
CCNA2621(config-line)#login
CCNA2621(config-line)#password myauxpassword
CCNA2621(config-line)#exec-timeout 1 30
```

Securing Telnet Access to User EXEC

Telnet is by far one of the most insecure methods of establishing an EXEC session because any user with IP connectivity to the device can initiate a Telnet session to it. For this reason, the default state of these lines is to require that a vty password be set for anyone to achieve access to User EXEC. Otherwise, you will receive an error similar to the following:

```
Password required, but none set
```

In addition, if you do not have an enable password set on the device, you are not able to enter Privileged EXEC mode. The error you receive in this situation is the following:

```
% No password set
```

EXAM ALERT

Remember, by default a password must be set on the vty lines to give Telnet access to this device. An enable password must be set to access Privileged EXEC over a Telnet session.

Once again, the configuration is similar to those of the console and the auxiliary port; however, the navigation of the Telnet lines is slightly different than what you find with the rest. To assign a login password to all the Telnet lines into the device, you must specify the range of those vty lines in your navigation. For instance, most routers allow five Telnet sessions into them. To encompass all the vty lines, you have to identify them starting with the first line (remembering that numbering begins with 0), followed by the last (0-4 is a total of 5 lines), as shown here:

```
CCNA2621(config)#line vty 0 4
CCNA2621(config-line)#login
CCNA2621(config-line)#password mytelnetpassword
CCNA2621(config-line)#exec-timeout 1 30
```

The question usually begs, "What would happen if you configured only `line vty 0` or you put a different password on each vty line?" To answer the first part of the question, if you configure only `line vty 0`, the router prompts the first user for a password. If another user tries to connect with that first Telnet session still running, he cannot log in to the router (remembering that the default state is that a password must be set as mentioned in the earlier Exam Tip).

On the other hand, if you assign different passwords to each of the vty lines, you can connect on all the lines; however, you have no means of choosing or knowing to which vty line you are connected. You would have to guess the password within three tries (IOS only allows three attempts).

EXAM ALERT

Be sure you are easily able to supply a configuration to any number of the EXEC lines depending on the scenario given.

Challenge

Securing access to your router or switch is an inevitable challenge that you will face on the exam as well as throughout your Cisco career. In this challenge, you apply the configurations you just learned to ensure that you also secure access from User EXEC to Privileged EXEC.

1. Through your console, connect an EXEC session and enter into Privileged EXEC, followed by Global Configuration.
2. Configure your console port to prompt for a login and use the password *captnstubing*.
3. Reduce the default inactivity console session timeout to 2 minutes and 10 seconds.
4. Configure your auxiliary port to prompt for a login and use the password *bartenderisaac*.

(continues)

(continued)

5. Reduce the default inactivity console session timeout to 3 minutes.
6. Configure all five Telnet lines to prompt for a login and use the password *yeomangopher*.
7. Secure Privileged EXEC by using a command that displays the password *theloveboat* in clear text.
8. Secure Privileged EXEC by using a command that performs the strongest encryption on the enable password, *something4every1*.
9. Which command will allow you to enter Privileged EXEC with them both configured?
10. Encrypt all the clear text passwords in the configuration using a Cisco proprietary encryption.

Your configuration should look like the following (with possible variation on the abbreviation of the commands):

```
Router>enable
Router#configure terminal
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password captnstubing
Router(config-line)#exec-timeout 2 10
Router(config-line)#exit
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password bartenderisaac
Router(config-line)#exec-timeout 3 0
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password yeomangopher
Router(config-line)#exit
Router(config)#enable password theloveboat
Router(config)#enable secret something4every1
Router(config)#service password-encryption
```

In this configuration, anyone connecting to the console port needs to enter the password *captnstubing* before gaining an EXEC session via the console port. After 2 minutes and 10 seconds of inactivity, the sessions close and users have to enter in the password again to return to User EXEC. Likewise, anyone accessing the router from the auxiliary port needs to enter the password *bartenderisaac* at the login prompt and has to re-enter that password after 3 minutes of inactivity. Up to five administrators can Telnet into this router, at which point they all have to enter the password *yeomangopher* at the login prompt.

Beacuase the `enable password` command and the `enable secret` command are used in this configuration, the password *something4every1* inevitably will be used to enter Privileged EXEC because the `enable secret` command overrides the `enable password`. The final command, `service password-encryption`, encrypts the enable, vty, aux, and console passwords so they are not visible to anyone who can see the configuration.

Router Interface Configurations

Because a primary purpose of Cisco routers and switches is to transfer data between their interfaces, the configuration parameters that you apply to these interfaces dramatically affect how these devices operate in an internetwork. These interface configurations vary depending on the type of interface you are configuring and even which Layer 2 frame encapsulation you are utilizing for WAN interfaces. This section looks specifically at some of the basic configurations that you can apply to LAN and WAN interfaces on a router.

Assigning an IP Address

Objective:

Assign IP addresses

Recall from Chapter 1, "Standard Internetworking Models," that the basic functionality of a router is to forward packets from one network to another, using logical addressing. If you configure an IP address on an interface, that router systematically assumes that all packets that are destined for that IP address's network should be routed out that specific interface. For instance, if you assign the IP address of 192.168.1.1 with a subnet mask of 255.255.255.0 on a serial interface, the router automatically assumes when that interface is enabled that all packets destined for 192.168.1.x are to be sent out the WAN serial interface.

As you can see, assigning an IP address to an interface plays a pivotal role in a router's primary routing operation. The command to help fulfill that role on a given interface is `ip address`, followed by the assigned IP address for that interface and the subnet mask. For instance, if you wanted to assign the IP address of 192.168.1.1 with a subnet mask of 255.255.255.0 to the serial 0/0 interface of the 2600 modular router, the configuration would look like this:

```
Router(config)#interface serial 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

NOTE

Remember, if this was a router with a fixed interface (not modular), the command might look something like this:

```
Router(config)#interface serial 0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

The first line in the configuration navigates you to the appropriate interface that you wish to configure. In this case, it is the first serial interface in the first module on the 2600 router (serial 0/0). The second command assigns the IP address of 192.168.1.1 to this interface. After this interface is enabled (discussed in next section), this router forwards any packets destined for 192.168.1.x 255.255.255.0 out its serial 0/0 interface.

TIP

Because a router needs to forward packets between networks, you cannot configure two interfaces with IP addresses that are part of the same subnet. For example, you cannot configure serial 0 for 192.168.1.1 255.255.255.0 and interface ethernet 0 with an IP of 192.168.1.2 255.255.255.0. Because both IPs exist on the 192.168.1.0 network, the router cannot distinguish to which interface to send packets destined for 192.168.1.x. When a configuration error such as this is attempted, the router informs you that the IP network overlaps with another interface and does not let you assign the second IP address.

For documentation and reference, you can assign a description to this interface by using the `description` command on the interface:

```
Router(config-if)#description This is my first interface description.
```

EXAM ALERT

The `description` interface command assigns a description to a specific interface.

Enabling the Interface

All router interfaces are in a disabled (`shutdown`) state by default. It is the duty of the configuring administrator to enable the interface by using the `no shutdown` command. If properly configured and connected to the network, the interface comes up and begins routing data in and out that interface. An example of administratively enabling the interface with the `no shutdown` command is as follows:

```
Router(config)#interface serial 0/0
Router(config-if)#no shutdown
```

EXAM ALERT

You should be able to seamlessly assign an IP address on any interface and administratively enable it for the exam.

TIP

If your interface is not connected to any other devices to communicate at Layer 2, you can use the `no keepalives` command on the interface to keep your interface active. A keepalive is a mechanism that the IOS uses to send messages to itself or to the other end to ensure a network interface is alive.

LAN-Specific Commands

Many of the LAN interfaces on a router have auto-sensing capabilities such as duplex and speed. For instance, a Fast Ethernet interface can run at speeds of 10mbps or 100mbps at half- or full-duplex. It is generally a good idea to manually assign an interface's duplex in case your connected device does not support auto negotiation. The configuration to manually set the duplex on an interface is fairly straightforward, as follows:

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#full-duplex
```

WAN-Specific Commands

When configuring synchronous serial interfaces, you may discover that you have to configure some additional parameters to ensure proper functionality of your Wide Area Network (WAN) interfaces. For instance, when you have a serial cross-over cable between two routers' serial interfaces in a lab environment, the serial interface with the DCE cable attached to it has to provide timing for the network for data to be recognized on this link. The command to provide this synchronous timing on the network is `clock rate`, followed by the speed in bits per second.

Additionally, WAN serial interfaces automatically assume that the circuit connected to them is of T1 speed (1.54mbps). In instances where you have set a lower clock rate or you are connecting to a WAN service that is using sub-T1 speeds or virtual circuits (discussed later in Chapter 15, "Wide Area Networks"), it is imperative to redefine the bandwidth that is connected to the interface for accurate operation of routing decisions. You can achieve this redefinition by using the `bandwidth` command followed by the speed of the circuit in kilobits per second.

The following configuration demonstrates both of these commands in action for a router in a lab simulating a 64kbps circuit:

```
Router(config)#interface Serial 0/0
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
```

Switch-Specific Commands

Objective:

Perform an initial configuration on a switch

Catalyst switches, for the most part, are designed so that the default state of switch allows for basic Layer 2 functionality without requiring any configuration from the administrator. For example, the physical interfaces on the switch are already enabled, which means that you can plug a cable in the switch and the interface operates without requiring you to perform a `no shutdown` on that interface. Does that mean you don't have to learn about Catalyst switch commands? No such luck.

NOTE

Switch ethernet interfaces are commonly referred to as *ports*.

These next sections look at a few commands that cover some of the basic administrative functions within the switch. In Chapter 8, "Bridging and Switching Operations," and Chapter 9, "Virtual LANs," you will explore some of the more advanced functions and commands that you can perform on the Catalyst switch.

Assigning a Management IP Address to a Switch

Objective:

Assign IP addresses

Cisco Layer 2 switches forward frames solely based upon MAC addresses. On the other hand, Layer 3 switches and routers use IP addresses in their data forwarding decisions. So why assign an IP address to a Layer 2 switch?

Chapter 6, "Initial Cisco IOS Operations," mentioned that to remotely manage a device via SSH, Telnet, or HTTP, you need to have IP connectivity to the switch. Likewise, if you were to manage the switch using SNMP, you would also have to program your management server to use its IP address to gather statistics from the switch. All these management functions assume that an IP address is assigned to the device, which in the Catalyst switch's case does not have an IP address in its default configuration.

Unlike Cisco routers, Layer 2 switches do not assign IP addresses on all the physical interfaces. In fact, the interface to which you assign an IP address on a Layer 2 Catalyst switch is actually a virtual interface called VLAN 1 (Chapter 9 discusses the significance of VLAN 1).

To assign an IP address to the entire switch, you use exactly the same syntax as a router's physical interface to configure the VLAN 1 interface:

```
Switch(config)#interface VLAN1
Switch(config-if)#ip address 172.16.1.100 255.255.0.0
```

Defining a Default Gateway

If you were to Telnet into the switch from the terminal on the far network, the Telnet traffic would traverse through the local router, across the WAN link, through the remote router, and finally to the switch. To return the Telnet traffic back to the terminal, the switch would have to send it to a routing device because the terminal is on another network. To instruct the switch to send any traffic destined for another network to that router, you have to define a default gateway (also known as a gateway of last resort) as required in Figure 7.2.

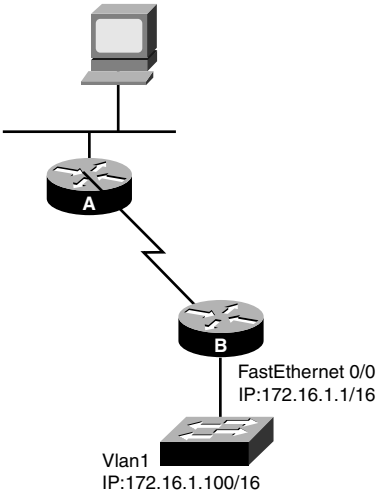


FIGURE 7.2 Remote management requirement for default gateway.

The command to configure a default gateway is `ip default-gateway`, followed by the IP address of the router that is on the switch's segment in Global Configuration. Using the example in Figure 7.2, the configuration would look like the following:

```
Switch(config)#ip default-gateway 172.16.1.1
```

EXAM ALERT

It is essential that you understand the syntax and purpose behind the `ip default-gateway` command in a switch before taking the exam.

Configuring Multiple Switch Interfaces

By design, switches may have a plethora of interfaces that may require a similar configuration. For instance, if the first 20 ports of your switch need to be set to a speed of 100mbs and full duplex, you would be undertaking quite an administrative task of typing the same commands into each interface configuration for all 20 interfaces. To save time, the Catalyst switch's IOS contains a navigation and configuration command shortcut called `interface range` that enables you to define a range of switch ports and configure them simultaneously. The configuration can be condensed to something like this:

```
Switch(config)#interface range FastEthernet 0/1 - 20
Switch(config-if)#speed 100
Switch(config-if)#duplex full
```

TIP

Note that the syntax of the `interface range` command requires you to put a space between the starting and ending interfaces in the range separated by a hyphen.

NOTE

You can manually override the default auto-negotiating speed and duplex settings for each interface as demonstrated. Note the syntax is slightly different for changing the duplex on a switch port versus a router interface.

Saving Configurations

Objective:

Perform an initial configuration on a router and save the resultant configuration file

If you are like me, you like living on the edge by configuring your devices during scheduled brown-outs in a room full of people with size 15 feet who are prone to accidentally kick the power cord out of your Cisco device. The problem with that lifestyle is that when the power returns to your router or switch, the hard work you put into your configuration is gone because all your configurations were made to the running configuration stored in volatile RAM. This is unfortunately true, unless of course, you save your configuration file into NVRAM and make that your startup configuration.

The versatile command that deserves all this credit for saving your hides is the `copy` command. With this command, you are telling the IOS to copy a file from one file system to another. Some options you have after the `copy` command are `running-config`, `startup-`

config, flash, and tftp. The last two are discussed later in this chapter; the Global Configuration command to save the configuration in a switch or router IOS is as follows:

```
Router(config)#copy running-config startup-config
```

EXAM ALERT

Although a source of debate these days, it is rumored that you do not need to save the configuration in a simulation. Despite my danger-seeking lifestyle, I highly recommend you err on the safe side by saving your configuration.

TIP

After performing the `copy running-config startup-config`, later IOSs ask you for the filename that you want to call the configuration file with `[startup-config]` in brackets. If you hit the Enter key, it saves it as the startup-config that will be loaded on next reboot. Saving it with a different filename saves the configuration, but that configuration will not be the one that is loaded.

EXAM ALERT

If you want to return your router or switch to its default configuration, you can use the Privileged EXEC command, `erase startup-config`, and reboot the device with the `reload` command. After the router or switch reboots, you should enter into Setup Mode because the configuration in NVRAM was erased.

STEP BY STEP

7.1 Configuring Router Interfaces

1. Go into Privileged EXEC by typing **`enable`**.
2. Enter Global Configuration by typing **`configure terminal`**.
3. Go into the Fast Ethernet interface 0/0 and configure the IP address of 172.16.1.1 /16 by typing **`ip address 172.16.1.1 255.255.0.0`**.
4. Enable the interface using the `no shutdown` command.
5. Type **`exit`** and go into the Serial interface 0/0 and configure the IP address of 192.168.1.1 /24 by typing **`ip address 192.168.1.1 255.255.255.0`**.
6. Enable the interface by using the `no shutdown` command.
7. Type **`end`** or press Ctrl+Z to go back to Privileged EXEC, and save the configuration by using `copy running-config startup-config`.

The result should look similar to Figure 7.3.

```
CCNA2621>enable
CCNA2621#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CCNA2621(config)#interface fastethernet 0/0
CCNA2621(config-if)#ip address 172.16.1.1 255.255.0.0
CCNA2621(config-if)#no shutdown
CCNA2621(config-if)#exit
CCNA2621(config)#interface serial 0/0
CCNA2621(config-if)#ip address 192.168.1.1 255.255.255.0
CCNA2621(config-if)#no shutdown
CCNA2621(config-if)#^Z
CCNA2621#
00:04:58: %SYS-5-CONFIG_I: Configured from console by console
CCNA2621#copy running-config startup-config
Destination filename [startup-config]?
```

FIGURE 7.3 Step-by-step configuration.

Using the show Command to Get Information

Objective:

Use a subset of Cisco IOS commands to analyze and report network problems

As an administrator of Cisco routers and switches, it is inevitable that you will have to get information and statistics to verify the functionality of those devices and the networks that are connected to them. The crux of every command to view these statistics is the `show` keyword. This section explains what information you can gain from several of these `show` commands and tells you how to interpret outputs of those commands.

Verifying Your Configurations

Without a doubt, verifying your configurations is one of the most widely used `show` functions in the Cisco IOS. What better way to double-check or troubleshoot your configuration could there be seeing it displayed right in front of you? One caveat to these particular `show` commands, however, is that you must be in Privileged EXEC to see the configurations. This makes logical sense because you don't want anybody from User EXEC to see your passwords in the configurations.

To see the active configuration that is running in RAM (that is, `running-config`), simply type **`show running-config`**. Similarly, the command `show startup-config` displays the configuration that will be loaded after you reboot the router or switch. The following example shows the `show running-config` command, and the output of some of the router configurations discussed in this chapter, performed on a 1601 router with fixed interfaces:

```
CCNA1601#show running-config
Building configuration...
Current configuration:
```

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname CCNA1601
!
enable secret 5 $1$nLCr$gNidpLSZvMnm2wFW6ACLm0
enable password 7 14120A0A0107382A29
!
ip subnet-zero
ip host corerouter 172.16.1.1
ip name-server 172.16.1.254
!
interface Ethernet0
 ip address 172.16.1.1 255.255.0.0
 no ip directed-broadcast
 full-duplex
!
interface Serial0
 bandwidth 64
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
 no fair-queue
!
ip classless
no ip http server
!
banner motd ^C This is a private system and may be accessed only by authorized users.
➥Unauthorized access is strictly prohibited and will be enforced to the full
➥ extent of the law.^C
!
line con 0
 exec-timeout 1 30
 password 7 045802150C2E
 login
line vty 0 4
 exec-timeout 1 30
 password 7 02050D480809
 login
!
End
```

NOTE

Notice that in the output of the `show running-config` command there are commands such as `service timestamps debug uptime`, `ip subnet-zero`, and so on that have not been discussed. These are all configurations that are created by default by the IOS, and may vary depending on the version of the IOS that is loaded. On that same note, some configurations do not even show up in the IOS configuration even though they are configured on the router or switch. For instance, both interfaces were administratively enabled in this configuration despite the lack of the command `no shutdown` being displayed on each interface configuration.

EXAM ALERT

One of your best resources on a simulation that has a troubleshooting scenario is the `show running-config` command. By looking at the configuration and recognizing incorrect or missing entries, you can determine what items must be fixed in a particular device to regain connectivity in the simulated network.

Viewing Interface Statuses and Statistics

Beyond a doubt, the next four `show` commands will serve as the most useful tools in determining interface functionality and the performance of the network connected to those interfaces. Some of the outputs for these interface-specific `show` commands display similar statistics; nevertheless, each command serves a unique purpose depending on what facet of the interfaces you are trying to investigate.

Show Interfaces

The most detailed `show` command that displays statistics about the status of the interfaces and the network traffic for that interface is the `show interfaces` command. This command shows you statistics for all interfaces on the router or switch; however, if you wish to view information about only a single interface, you can specify that interface in the command (for example, `show interfaces serial 0/0`). Figure 7.4 illustrates the `show interface` output for a fast ethernet interface.

A common statistic of most of the interface `show` commands is the actual status of the interface itself. This is identified in the first line of output of the `show interfaces` commands. The first part of the status identifies the Layer 1 information of the interface, followed by the Layer 2 line protocol status.

If you understand the interface statuses you are ultimately building a solid foundation to accurately troubleshoot any malfunctioning interface. For example, if your interface is in an "up/line protocol up" state, you have eliminated Layer 1 and Layer 2 malfunctions for that interface. From this point, you can determine whether the problem on the interface is perhaps a Layer 3 problem (IP addressing, routing, and so on). Table 7.1 lists the possible values of this command.

```
Router#show interfaces FastEthernet 0/0
FastEthernet0/0 is up, line protocol is down
  Hardware is AmdFE, address is 0003.e32a.4080 (bia 0003.e32a.4080)
  Internet address is 172.16.1.1/16
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP timeout 04:00:00
  Last input never, output 03:12:26, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 40/40, 922 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     288 packets output, 21024 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

FIGURE 7.4 FastEthernet `show interfaces` output.

TABLE 7.1 Interface Status Values

Layer 1	Layer 2 (line protocol)	Possible Symptoms
Up	Up	None. Interface is functional.
Up	Down	Encapsulation mismatch, lack of clocking on serial interfaces, missing keepalives.
Down	Down	Cable is disconnected or attached to a shut down interface on the far-end device.
Administratively Down	Down	Local interface was not enabled with the **`no shutdown`** command.

EXAM ALERT

Be able to recognize the interface status meanings and determine the possible reasons for that status.

The rest of the output of the `show interfaces` command is also extremely useful for gaining information about the interface and the network. Of course, you won't be expected to know all the elements listed in this output; however, Table 7.2 displays some of the valuable common statistics descriptions.

TABLE 7.2 Show Interface Output Descriptions

Output	Description
`Hardware is AmdFE, address is 0003.e32a.4080`	The MAC address of the ethernet interface.
`Internet address`	Assigned IP address.

(continues)

TABLE 7.2 *Continued*

Output	Description
`MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255`	The Maximum Transmission Unit (frame size) for this interface, logical bandwidth (default or set with bandwidth command), cumulative delay, interface reliability, inbound and outbound load.
`Encapsulation ARPA`	Layer 2 frame encapsulation on interface.
`Half-duplex, 100Mb/s, 100BaseTX/FX`	Duplex and speed of interface.
`Received 0 broadcasts, 0 runts, 0 giants`	The number of broadcasts, runts (below minimum frame size), and giants (above maximum frame size).
`0 collisions`	The number of collisions that occurred on that segment.
`0 late collision`	Late collisions occur when your interface is set for half-duplex and you are connected to a full-duplex interface.

EXAM ALERT

You may be presented with the output of a `show interface` command with the intention of testing your knowledge of being able to identify problematic elements in the output. For instance, a high load value is evidence of a saturated link, a large number of late collisions is a duplex mismatch, excessive collisions might be indicative of being plugged into a hub, and so on.

Show IP Interface Brief

If the goal of your `show` command is to get a condensed output of the interfaces' status and their IP addresses, the `show ip interface brief` command conveniently shows you a minimal display of these statistics as illustrated in Figure 7.5.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.16.1.1      YES manual up                    up
Serial0/0              192.168.1.1     YES manual down                  down
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/1              unassigned      YES unset  administratively down down
Router#
```

FIGURE 7.5 `show ip interfaces brief` output.

Show Controller

Although the output of the `show controller` command is unintelligible to everyone except for the Cisco TAC (Technical Assistance Center), one particularly useful extract from this output is in the `show controller serial` command. The needle in this haystack of statistics is

the line of output that identifies whether a DTE or a DCE cable is attached to the serial interface. This is useful if you are connecting to your router remotely and you are not sure whether your router should be providing the clocking (if you are the DCE interface). The following excerpt example illustrates this useful output:

```
Router>show controller serial 0/1
Interface Serial0/1
Hardware is PowerQUICC MPC860
V.35 DCE cable, clockrate 64000
...output omitted...
```

IOS File Version Show Commands

The following section discusses how to back up your IOS to a TFTP server or download a new version of the IOS to your router or switch. Tasks of this magnitude, however, cannot be performed unless you do some initial legwork. Namely, you must perform some essential steps such as identifying the amount of Flash memory, the IOS filename located in Flash, and the current IOS version that is running on the device.

Different Cisco IOS versions and feature sets will ultimately dictate the size of the IOS file and the amount of Flash and DRAM memory required to run the IOS. If you are planning to upgrade to a new IOS, you must make sure that you have enough memory (the more, the better) in your device. To see the amount of Flash you have and the current IOS file stored in Flash memory, utilize the `show flash` command as follows:

```
Router>show flash
System flash directory:
File  Length   Name/status
  1   5510192  c2600-is-mz.120-3.T3.bin
[5510256 bytes used, 2878352 available, 8388608 total]
8192K bytes of processor board System flash (Read/Write)
```

Typically, the filename of the IOS file in Flash correctly reflects the actual IOS version running currently on the device. However, an administrator can easily change the filename to his or her own purposes, or there could be multiple IOS files stored on the Flash and you are not sure which one is running currently. To ensure the correct version of IOS, use the widely practical `show version` command.

Demonstrated in Figure 7.6, the `show version` command displays a plethora of information well beyond the version of the IOS running. Table 7.3 explains some of the useful output of this multifaceted command.

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(3)T3,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 15-Apr-99 16:12 by kpma
Image text-base: 0x80008088, data-base: 0x80A05BAC

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

Router uptime is 8 hours, 8 minutes
System restarted by reload
System image file is "flash:c2600-is-mz.120-3.T3.bin"

cisco 2621 (MPC860) processor (revision 0x102) with 28672K/4096K bytes of memory.
Processor board ID JAD043804AF (1311100426)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

FIGURE 7.6 `show version` output.

TABLE 7.3 `show version` Output Descriptions

Output	Description
`IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(3)T3,  RELEASE SOFTWARE (fc1)`	The IOS feature set, version, and release.
`ROM: System Bootstrap, Version 11.3(2)XA4`	The version of the bootstrap code in ROM.
`Router uptime is 8 hours, 8 minutes`	The length of time the device has been running.
`System restarted by reload`	How the device was started.
`System image file is "flash:c2600-is-mz.120-3.T3.bin"`	The name of the IOS file that was loaded and the location of that file.
`with 28672K/4096K bytes of memory`	The amount of RAM in the system allocated to the devices processor, followed by memory allocated for packets. The total RAM is calculated by adding the two values together (`28672K+4096K=32858K, or 32MB`).
`32K bytes of non-volatile configuration memory.`	The amount of NVRAM for the startup-config.
`8192K bytes of processor board System flash (Read/Write)`	Total amount of Flash memory.
`Configuration register is 0x2102`	The current configuration register.

EXAM ALERT

Be able to rattle off all the information that you can extract from the `show version` command, including the current loaded IOS version, configuration register, and total memory of RAM, NVRAM, and Flash.

REVIEW BREAK

Table 7.4 reviews the `show` commands discussed in this chapter, including their functions and whether they are in User EXEC or both User EXEC and Privileged EXEC.

TABLE 7.4 `show` Command Review

Command	User EXEC/ Privileged EXEC	Output
`show running-config`	Privileged EXEC	Current configuration in RAM.
`show startup-config`	Privileged EXEC	Configuration in NVRAM to be loaded at next boot.
`show interfaces`	Both	Interface status, IP address, encapsulation, bandwidth, reliability, load, MTU, duplex, network statistics.
`show ip interface brief`	Both	IP address and status of interfaces.
`show controller serial`	Both	Microcode of interface, including whether DTE or DCE cable is attached.
`show flash`	Both	IOS filename and amount of used and available Flash memory.
`show version`	Both	IOS version, IOS filename, uptime, memory amounts, configuration register.

Troubleshooting Commands

Objective:

Use embedded Layer 3 through Layer 7 protocols to establish, test, suspend, or disconnect connectivity to remote devices from the router console

Troubleshooting a Cisco device and the networks to which it is connected is an integral part of being a Cisco administrator. Most of your troubleshooting can be solved by verifying your configurations and the device's operations, using the `show` commands mentioned in the previous section. However, at times you may need to use additional commands to help identify and troubleshoot faults in the network.

Specifically, the `clear` command in Privileged EXEC resets statistical information that is being stored for the outputs of your `show` commands. For example, if you saw that the output of the `show interfaces serial 0/0` command and noticed excessive late collisions, how do you know whether those are recent statistics or collisions that occurred last week? Using the `clear counters` command resets those statistics so you can view up-to-date information from the `show interfaces` output.

One of the most widely utilized commands for troubleshooting is the `ping` command. `ping` uses ICMP echo and echo reply messages to verify connectivity to IP devices. To ping a specific device from User EXEC or Privileged EXEC, enter **`ping`** followed by the IP address or hostname of the device you are trying to verify, as follows:

```
Router#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5)
```

Notice that the ping response contains a period (`.`) followed by four exclamation marks (`!`). An exclamation mark character is indicative of a successful receipt of a reply to the ping. The period character indicates that a timeout has occurred for that particular ICMP echo packet. In some instances, you may receive a `U` character, which signifies a Destination Unreachable ICMP message. These messages are indicative that a router along the packet's path to the destination did not know how to reach the destination network. When this occurs, the router sends a Destination Unreachable message back to the packet's source.

EXAM ALERT

ICMP Destination Unreachable messages are sent by a routing device when it does not know how to reach the destination network. The router sends this ICMP message back to the packet's source.

NOTE

Notice that in the output of the `ping` command, the first ping packet timed out. This actually is quite normal when pinging a device on a LAN because the router or switch might have to resolve the MAC address on the data link segment with an ARP request. Any successive pings shortly after should receive 100% of replies.

Similar to other operating systems, you can manipulate some of the options in a ping echo request, such as the datagram size and the timeout period in the Cisco IOS. To specify these options, you need to use an extended `ping` command. This command requires you to be in Privileged EXEC and is used by typing **`ping`** followed by the Enter key (no IP address). From there, you can change the default parameters such as the datagram sizes, timeout, and the number of packets sent, as shown in the following example:

```
Router#ping
Target IP address: 192.168.1.1
Repeat count [5]: 10
Datagram size [100]: 200
Timeout in seconds [2]: 5
Extended commands [n]: y
```

```
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort 192.168.1.1, timeout is 5 seconds:
!!!!!!!!!
Success rate is 100 percent (10/10)
```

EXAM ALERT

The extended `ping` must be entered in Privileged EXEC. The command is `ping` followed by the Enter key.

Another useful ICMP utility is the `traceroute` command. As the name states, `traceroute` sends ICMP messages and receives a reply from every routing device along the path to the destination. This is useful in situations where you suspect a router on the route to an unreachable network is failing. The command syntax for `traceroute` is similar to the `ping` command. In fact, you can also perform an extended `traceroute` by using the `traceroute` command in lieu of the `ping` keyword.

```
Router#trace 192.168.1.1
Tracing the route to 192.168.1.1
1 192.168.100.1 4 msec 0 msec 4 msec
2 10.1.1.3 4 msec 4 msec 0 msec
3 192.168.1.1 0 msec 0 msec 4 msec
```

EXAM ALERT

`traceroute` is an ICMP utility that tests the connectivity to a device by receiving responses from each routing device along the path to the destination. It is especially useful when you suspect a router on the route to an unreachable network is failing.

The final troubleshooting command (for now) is another exclusive Privileged EXEC command that should be used only when all other troubleshooting has failed. The `debug` command displays real-time information on such things as routing updates, packet forwarding, and interface keepalives, to name a few. The reason behind the cautionary tone of this explanation is because the `debug` command is very processor intensive and can generate a lot of information on your terminal screen. For this reason, it is highly recommended that you use

these commands only in emergency situations or in a lab environment. If you must troubleshoot on a production router, be sure to issue the `show processes` command as follows:

```
RouterA#show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
...Output Omitted...
```

The majority of the output will not make sense; however, the top of the output lists the CPU utilization up to the last 5 minutes. If any of these values exceeds 60%, do not use the `debug` commands. If you do, your router is likely to seize up from over-utilization.

EXAM ALERT

It is recommended to use the `show processes` command before using any debug commands to verify the router's current CPU utilization.

When you are finished troubleshooting, you can turn off debugging by putting a `no` in front of the command, or you can turn off all debugging by typing `no debug all` or `undebug all`. Specific debugging commands are discussed throughout the course of this book.

EXAM ALERT

If your device is seizing up from too much `debug` processing, turn it off by using the `no debug all` or `undebug all` commands.

TIP

To see accurate timestamps for your `debug` messages, it is highly recommended that you configure the clock to reflect the correct date and time by using the clock command in Privileged EXEC. In addition, to add a timestamp to the `debug` output, use the `service timestamp` command in Global Configuration.

Backing Up and Restoring Configurations and IOS Using TFTP

Objective:

Manage system image and device configuration files

Recall from the "Saving Configurations" section that you used the `copy` command to copy the running config in RAM to the startup config in NVRAM. By using this command, you are

basically copying this configuration file from one filesystem component to another. Such is the case if you want to back up and restore configurations and IOSs to and from a TFTP server.

EXAM ALERT

The TFTP server is used to back up and restore configurations and IOS images.

A fair amount of setup and preparation is required to achieve this functionality, but the rewards of being able to back up and restore these files are well worth it. Specifically, the following preparations need to be in place for your switch or router to transfer these files to and from a TFTP server:

1. The TFTP server must have the TFTP service running. You can search the Internet for evaluation TFTP servers from companies such as SolarWinds and FutureSoft.
2. Your device must be cabled correctly. If you're using a switch, plug the TFTP server into the switch with a straight-through ethernet cable. If you're going directly between a router and the TFTP server, use a cross-over cable.
3. You must have IP connectivity to the server. In other words, your interface should be on the same subnet as the server.
4. There must be enough room on the TFTP server and your device's memory to store these files. If your Flash memory cannot store two files, the IOS erases the old file from Flash memory before copying the new one.

EXAM ALERT

Know the preparation steps involved in setting up your network to ensure that files can be transferred between your Cisco device and a TFTP server.

After all the preparations are in place, and you have verified connectivity between the TFTP server and your Cisco router or switch, you can use the `copy` command again to transfer files. Remember, the `copy` command instructs the IOS to copy from somewhere to somewhere. The available keywords, once again, are `startup-config`, `running-config`, `tftp`, and `flash`. When the `tftp` keyword is used, the IOS follows up with a few subsequent questions to help the IOS identify the IP address of the server, and the filenames of the source and destination files.

For example, to back up the IOS stored in Flash, your command would look something like the following:

```
Router#copy tftp flash
Address or name of remote host []? 172.16.1.254
Source filename []? c2600-is-mz.120-3.T3.bin
Destination filename [c2600-is-mz.120-3.T3.bin]?
Copy 'c2600-is-mz.120-3.T3.bin' from Flash to server
as 'c2600-is-mz.120-3.T3.bin'? [yes/no]y
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
...output immited...
Upload to server done
Flash device copy took 00:01:24 [hh:mm:ss]
```

NOTE

Similar to utilities such as `ping` and `traceroute`, successful copying of files to and from a TFTP server is displayed with an exclamation mark (`!`).

Similarly, if you wanted to upgrade your IOS to a new version or you want to restore a previously backed up IOS from your TFTP server, the command would be `copy flash tftp`. Remember, if your flash memory does not have enough space for your current IOS file and the new one, the process erases your old IOS file to make room for the new one. If you accidentally lose power during the file transfer, you inevitably end up in RxBoot. At that point, you can download the IOS again from the TFTP server using the same command.

After the IOS image is loaded to your Flash memory, you have to reboot the device for that IOS to run (because your current IOS is still decompressed and running in RAM). To reboot a Cisco device, use the `reload` command from Privileged EXEC. Do not forget to save any configuration changes that you made with the `copy running-config startup-config` command before rebooting the device because the router or switch uses the contents of your startup configuration when it reinitializes. In many current IOS versions, the IOS reminds you that your configuration has modified and asks you whether you want to save it. Answering "yes" to this prompt saves your configuration to NVRAM.

```
Router#reload
System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload? [confirm]
04:31:02: %SYS-5-RELOAD: Reload requested
```

EXAM ALERT

The `reload` Privileged EXEC command reinitializes the router or switch. The content in the startup configuration is loaded on boot-up.

The `copy` command can also be used to back up and restore your configurations. For example, to back up your current configuration, you can type `copy running-config flash`. Alternatively, you can always save your configuration to a text file by capturing the text output of your terminal program and doing the `show running-config` command. If you want to paste the configuration back into the Cisco device, just go into Global Configuration and paste the text back into the terminal program window.

EXAM ALERT

The `show running-config` command does not show commands such as `no shutdown`. If you paste the configuration into a new configuration, the interfaces remain shut down unless you edit the text file and place the `no shutdown` command in the interface configurations or enter the commands in the configuration afterward.

Neighbor Discovery with CDP

Objective:

Use embedded Data Link layer functionality to perform network neighbor discovery and analysis from the router

Determine IP addresses

Imagine it is your first day at work and your boss wants you to create a topology map of the network, including model numbers, IPs, and IOS versions of all the Cisco equipment. Eager to impress the boss, you want to get this task done as soon as possible. The problem is that the equipment isn't allocated in the same building and your security badge won't allow you into other buildings. Thus, console access isn't possible and you don't know the IP addresses of the other devices to Telnet into them. Instead of spending that free time looking in the want ads because you are afraid you are going to get fired, you can call upon a very useful protocol called Cisco Discovery Protocol (CDP) to gather information of directly connected Cisco neighbors.

As the name indicates, CDP is a Cisco proprietary protocol that operates at the Data Link layer. One unique feature about operating at Layer 2 is that CDP functions regardless of what Physical layer media you are using (UTP, fiber, and so on) and what Network layer routed

protocols you are running (IP, IPX, AppleTalk, and so on). CDP is enabled on all Cisco devices by default, and is multicast every 60 seconds out of all functioning interfaces, enabling neighbor Cisco devices to collect information about each other. Although this is a multicast message, Cisco switches do not flood that out to all their neighbors as they do a normal multicast or broadcast.

EXAM ALERT

Remember the defining characteristics of CDP are that it is a proprietary Layer 2 protocol that can run regardless of the Layer 1 and Layer 3 configuration. It also is enabled by default and sent as a multicast to directly connected Cisco neighbors only.

NOTE

Cisco has expanded CDP's utility to include providing auto-negotiation of power of ethernet for Cisco IP phones and wireless access points. Additionally, CDP is used for sending routing network information with on-demand routing (discussed in Appendix A, "Future Exam Topics").

The amount of information you can display ultimately depends on the command you use. For instance, the following example illustrates the output of the `show cdp neighbors` command:

```
CCNA2621>show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Bldg1-3550       Fas 0/0            128         S I       WS-C3550-2Fas 0/22
Engineering1601  Ser 0/1            134          R        1601      Ser 0
```

Table 7.5 explains the output depicted in the preceding example.

TABLE 7.5 `show cdp neighbors` Output Explanation

Column Heading	Explanation
`Device ID`	Neighbor's configured hostname.
`Local Intrfce`	Local interface in which you received this information.
`Holdtme`	CDP hold-down timer to keep track of how long it has been since you received information from that neighbor and how many seconds to wait until you consider that neighbor dead.
`Capability`	The capabilities of the Cisco devices as explained in the legend at the top of the output.
`Platform`	The model number of the Cisco device.
`Port ID`	The interface in which the neighbor device sent out this CDP information.

By using the `show cdp neighbors detail` command or the `show cdp entry *` command, you can gain even more information about your neighbor Cisco devices. Specifically, you can see all the information from the `show cdp neighbors` output in addition to the Layer 3 information and the IOS version of your directly connected neighbors. Figure 7.7 illustrates the detailed output of these commands.

```
CCNA2621>show cdp neighbor detail
-------------------------
Device ID: Bldg1-3550
Entry address(es):
Platform: cisco WS-C3550-24,  Capabilities: Switch IGMP
Interface: FastEthernet0/0,  Port ID (outgoing port): FastEthernet0/22
Holdtime : 143 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(13)EA1a, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 25-Mar-03 23:21 by yenanh

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=00000000FFFFFFFF010221FF00000000000000
0D65D04E00FF0000
VTP Management Domain: 'ThirteenBlack'
Native VLAN: 1
Duplex: full

-------------------------
Device ID: Engineering1601
Entry address(es):
  IP address: 192.168.100.5
Platform: cisco 1601,  Capabilities: Router
Interface: Serial0/1,  Port ID (outgoing port): Serial0
Holdtime : 145 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 1600 Software (C1600-NY-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 11-Aug-99 01:13 by phanguye
```

FIGURE 7.7 `show cdp neighbors detail` or `show cdp entry *` output.

Based upon this information, you can already begin to see the topology layout of these three devices, as illustrated in Figure 7.8.

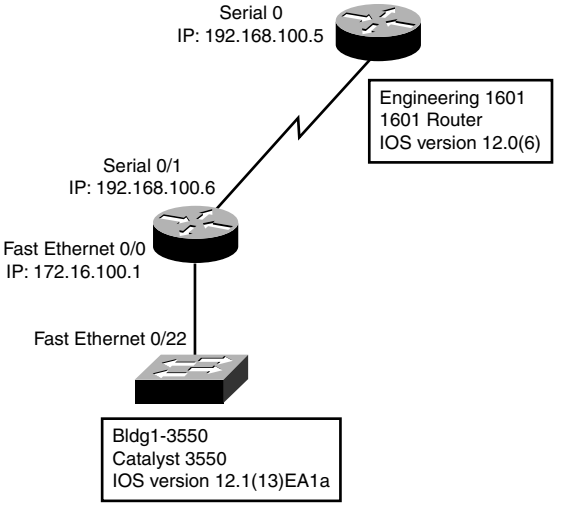


FIGURE 7.8 Example topology derived from CDP output.

At this point, I am sure you are completely in awe of the wonders that CDP can bring to your administrative duties; however, there are times you may wish to disable CDP. As mentioned before, CDP is a Cisco proprietary protocol enabled by default on all Cisco devices. So what happens when you are not connected to a Cisco device? Although the bandwidth usage is minimal, it still serves no purpose to continue sending CDP advertisements to non-Cisco devices that cannot interpret this protocol. In addition, it is a good idea to disable CDP for security reasons because you can gain so much useful information that could prove fatal in the wrong hands.

You can disable CDP in one of two ways: globally on the Cisco device or on an interface-by-interface basis. To disable CDP for the entire device, you have to configure the `no cdp run` command in Global Configuration. Otherwise, you can specify on which interfaces to disable CDP advertisement by navigating to those specific interfaces and using the `no cdp enable` command in the interface configuration.

EXAM ALERT

Keep in mind for the exam that the two commands to disable CDP are `no cdp enable` and `no cdp run`.

Challenge

Imagine that the lead engineer has asked you to install a new router in the lab rack. You connect the serial interfaces together with a v.35 cross-over cable and install the router in the rack. Complete the following steps to get the two devices to communicate:

1. Through your console, connect an EXEC session.
2. The cross-over cable is not labeled. What command can you type to verify if your end is the DCE or the DTE connector?
3. To get the two routers to communicate with each other, you have to assign an IP address in the same subnet as the old router's serial interface. You know the lead engineer uses /30 subnets on his serial interfaces, but you need to figure out what IP address he used. What command can you type to find this information from your local router?
4. Enter the serial configuration.
5. The IP address he used was 192.168.40.41. Configure the only available IP address left in that subnet.
6. You have the DCE connection, so provide clocking for a 128K network.
7. Exit back to Privileged EXEC and save your configuration.

To see whether you have a DTE or DCE cable attached to your serial interface, you should type the `show controllers serial` command. Because the interface is already enabled, CDP information should be mulitcast between your routers. To see the neighbor's configured interface IP address, type `show cdp neighbors detail` or `show cdp entry *`.

The configuration should look like the following (with possible variation on the abbreviation of the commands):

```
Router>enable
Router#configuration terminal
Router(config)#interface s0
Router(config-if)#ip address 192.168.40.42 255.255.255.252
Router(config-if)#clock rate 128000
Router(config-if)#end
Router#copy runnig-config startup-config
```

Using Telnet for Virtual Terminal Access

Objective:

Use embedded Layer 3 through Layer 7 protocols to establish, test, suspend, or disconnect connectivity to remote devices from the router console

Telnet is the most widely used in-band management protocol today for remotely administering Cisco devices. As long as you have IP connectivity to the Cisco device and have configured a password on the vty lines, you can remotely administer your Cisco switches and routers. However, it is possible to limit the devices that can Telnet into your devices based upon their IP addresses, which is discussed later in Chapter 13, "Access Lists."

In User EXEC and Privilege EXEC of the IOS, it is possible to Telnet from your Cisco device to another device. By typing **`telnet`** followed by the IP address that you are trying to reach, you initiate a Telnet session from your local router or switch. In all actuality, you do not even need to use the `telnet` keyword. If you just type an IP address or a hostname (assuming name resolution), the IOS automatically assumes you are attempting to Telnet to that host.

For example, if you Telnet from the 2621 router to the remote 1601, the output would look similar to the following:

```
CCNA2621>telnet 192.168.100.5
Trying 192.168.100.5 ... Open
User Access Verification
Password:
Engineering1601>
```

At this point, you can configure the Engineering1601 router as if you were directly consoled into it. However, there may be a time where you need to jump back to your original router to incorporate additional configurations, verify connectivity, or Telnet into other devices. While connected to the remote device, you can suspend your Telnet session temporarily and return to the origin of the Telnet session (CCNA2621 in our example). The useful, but strangely awkward keystroke to suspend a Telnet session in Ctrl+Shift+6 followed by hitting the *x* key. Keep in mind that this only suspends the Telnet session; the session is still connected and running in a background process.

EXAM ALERT

Know that the keystroke combination Ctrl+Shift+6, *x* suspends a Telnet session.

As shown in Figure 7.9, you can verify the Telnet sessions that have originated from the local device by using the `show sessions` command. This example initiates and suspends two separate Telnet sessions from the CCNA2621 router.

```
CCNA2621>telnet 192.168.100.5
Trying 192.168.100.5 ... Open


User Access Verification

Password:
Engineering1601>
CCNA2621>telnet 172.16.1.100
Trying 172.16.1.100 ... Open


User Access Verification

Password:
Bldg1-3550>
CCNA2621>show sessions
Conn Host            Address            Byte  Idle Conn Name
   1 192.168.100.5   192.168.100.5         0     0 192.168.100.5
*  2 172.16.1.100    172.16.1.100          0     0 172.16.1.100
```

FIGURE 7.9 Multiple Telnet session example.

Notice that each session connection is numbered and there is an asterisk next to connection 2. This is the last Telnet session that was suspended and it is the session that will be resumed if you hit the Enter key without typing a command. You can also choose which Telnet session to resume by typing **`resume`**, followed by the connection number.

Ctrl+Shift+6, *x* suspends the Telnet session, but how do you actually close the Telnet session when you are finished? The answer is twofold. You can close a Telnet session from the originating local device by typing the keyword `disconnect` followed by the connection number. From the device into which you are Telnetted, you can also type **`exit`** or **`logout`** from User EXEC or Privileged EXEC.

EXAM ALERT

Be familiar with the multiple ways you can resume and disconnect a Telnet session.

Terminal Monitor

By default, your Cisco devices send their notification messages such as `debug` outputs, interface alerts, and system error messages to the console port. This means that you cannot see these notifications over a Telnet session to another device by default.

To have these messages copied to the vty lines, you need to use the `terminal monitor` command in Privileged EXEC mode of the device to which you are telnetted. For instance, in the configuration shown, Router A Telnets into Router B and enters Privileged EXEC mode to type the `terminal monitor` command. `debug` outputs, notifications, and errors messages are then sent over the vty lines to be viewed by the remote terminal.

```
RouterA>telnet 10.1.1.1
Trying 10.1.1.1 ... Open
User Access Verification
Password:
RouterB>enable
Password:
Router#terminal monitor
```

EXAM ALERT

The `terminal monitor` command copied `debug` outputs and error messages to the vty terminal lines.

STEP BY STEP

7.2 Telnet Practice

1. Telnet into your neighbor router by typing **`telnet`**, followed by the IP address.
2. Suspend that Telnet session by using the Ctrl+Shift+6, x keystroke.
3. Verify that suspended Telnet session by typing **`show sessions`**.
4. Disconnect the Telnet session by typing **`disconnect`**, followed by the connection number (should be 1).

Chapter Summary

This chapter dealt with a plethora of commands and their respective syntaxes and outputs. In Global Configuration, you learned how to manipulate the startup process using either the `config-register` or `boot system` commands. Additionally, you saw how to use the `hostname` command to name your router or switch and how to create a message-of-the-day login banner with the `banner motd` command. To secure Privileged EXEC, you saw that the `enable password` command displays the password in clear text; however, the `enable secret` command encrypts the password using a one-way MD5 hash and overrides the `enable password` command if both are configured. For DNS-specific functions, you discovered that you can create static DNS entries with the `ip host` command or specify DNS servers using the `ip name-server` command.

In the line configuration for console, Telnet, and the aux port, you saw that you can configure a layer of security by having administrators enter a password to get into User EXEC. This was achieved by using the `login` and the `password` combo in the line configuration of each EXEC line. Additionally, you saw the utility of the `exec-timeout` command for changing the default timeout for an inactive EXEC session. Because these passwords are all in clear text, you can encrypt them in Global Configuration, using the `service password-encryption` command.

The configuration of interfaces entails assigning an IP address to a physical interface in a router and the VLAN 1 interface in a switch, using the `ip address` commands followed by the `no shutdown` command to administratively enable the interface. For switch configuration, you also learned the `ip default-gateway` command is used to define a gateway of last resort for a switch for it to respond to remote management requests from other networks.

You know from this chapter that the `copy` command can be used to meet several objectives such as saving the configuration, backing up and upgrading your IOS from a TFTP server, and backing up and restoring your configurations. You learned that the syntax of the `copy` command is `copy` from a source to a destination. The keywords you can use to identify the source and destination are `startup-config`, `running-config`, `tftp`, and `flash`.

To see your configurations, you now know that the `show running-config` command can show you the active configuration in RAM, and that `show startup-config` displays the configuration booted from NVRAM that you saved with the `copy running-config startup-config` command. For verification and viewing statistics of interfaces, you discovered that the `show interfaces` or the `show ip interface brief` command show you that the interface statues can be one of the following: up/line protocol up (active), up/line protocol down (Layer 2 down), down/line protocol down (Layer 1 down), administratively down/line protocol down (interface requires `no shutdown` command). What's more, the `show controller serial` command can show you whether the interface has the DTE or the DCE cable connected to it in a lab environment with a cross-over serial cable.

You can sleep better at night knowing now that your Cisco devices, by default, receive Layer 2 proprietary CDP multicast messages from directly connected Cisco devices that advertise the hostname, local and remote interfaces, capabilities, device model, and its hold-down time. You saw these statistics by using the `show cdp neighbors` command; however, you also saw the IOS revision and the Layer 3 address of your neighbors by using the `show cdp neighbors detail` or `show cdp entry *` command. Disabling this useful utility was demonstrated with the `no cdp run` command in Global Configuration or `no cdp enable` in the interface configuration.

Finally, you learned in this chapter that you can Telnet into other devices from your Cisco router or switch. You suspended the Telnet session by using the Ctrl+Shift+6, *x* keystroke and verified that Telnet session by typing **`show sessions`**. Closing the Telnet session was achieved by typing **`exit`** or **`logout`** while in the active Telnet session, or **`disconnect`** followed by the connection number in the device where the Telnet originated.

Key Terms

- `config-register` *`register`*
- `boot system` *`location filename`*
- `hostname` *`hostname`*
- `banner motd` *`delimiting_char banner delimiting_char`*
- `enable password` *`password`*
- `enable secret` *`password`*
- `service password-encryption`
- `ip host` *`hostname IP`*
- `ip name-server` *`dns_server_IP`*
- `ip domain-lookup`
- `login`
- `password` *`password`*
- `exec-timeout` *`minutes seconds`*
- `ip address` *`address subnet_mask`*
- `clock rate` *`speed(bps)`*
- `bandwidth` *`speed(kbps)`*
- `no shutdown`
- `full-duplex`
- `ip default-gateway` *`gateway_IP`*
- `interface range` *`media port_range`*
- `copy` *`from to`*
- `erase startup-config`
- `show interfaces`
- `show ip interface brief`
- `show controller`
- `show flash`
- `show version`
- `show cdp neighbors`
- `show cdp neighbors detail`
- `cdp run`
- `cdp enable`
- `telnet` *`IP_address`*
- `Ctrl+Shift+6,` *x*

- `show sessions`
- `resume` *conn#*
- `disconnect` *conn#*
- `terminal monitor`
- `ping`
- Destination Unreachable
- extended ping
- `debug`

Apply Your Knowledge

Exercises

7.1 Configuring a New Router

You are now onsite at the customer's location and it is time to prove your configuration skills by setting up their router with the following parameters. This exercise assumes you have a router that is not in production to utilize.

Estimated Time: 25 minutes.

1. In Global Configuration, assign the hostname, CstmrARtr, create an appropriate login banner, and use the strongest encryption for access to Privileged EXEC with the password, giforgot.
2. In line configuration, secure Telnet and console access by using the password imnotsure.
3. For the LAN interface, assign the IP address of 172.16.31.17 /28 and enable the interface.
4. For the serial interface, assign the IP address of 192.168.1.17 /30 and enable the interface.
5. Verify the status of your interfaces by using the `show interfaces` and `show ip int brief`.
6. Verify your active configuration and save it to NVRAM.

That configuration should look similar to the following 1601 configuration:

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname CstmrARtr
!
enable secret 5 $1$PHvQ$Gouu3MIDqY9G5d9hq9tr7/
!
```

```
ip subnet-zero
!
!
interface Ethernet0
 description /28 is 255.255.255.240 in decimal notation
 ip address 172.16.31.17 255.255.255.240
 no ip directed-broadcast
!
interface Serial0
 description /30 is 255.255.255.252 in decimal notation
 ip address 192.168.1.17 255.255.255.252
 no ip directed-broadcast
 no fair-queue
!
ip classless
!
banner motd ^C This is a private system and may be accessed only by authorized users.
➥ Unauthorized access is strictly prohibited and will be enforced to the full
➥ extent of the law.^C
!
line con 0
 exec-timeout 0 0
 password imnotsure
 login
 transport input none
line vty 0 4
 password imnotsure
 login
!
end
```

7.2 Configuring a New Switch

The router is now all configured, and you notice that the switch is already plugged in and running. The customer has requested that you make sure that the switch is secured with passwords and is able to respond to Telnet sessions from their remote Network Operations Center.

Estimated Time: 15 minutes.

1. In Global Configuration, assign the hostname, CstmrASwtch, create an appropriate login banner, and use the strongest encryption for access to Privileged EXEC, using the password, giforgot.
2. In line configuration, secure Telnet and the console User EXEC access by using the password imnotsure.

NOTE

Catalyst switches may have more than the typical five vty lines you saw in router configurations.

3. Assign a management IP address of 172.16.31.30 /28.
4. Set the default gateway to be the router's ethernet address from Exercise 7.1.
5. Verify your active configuration and save it to NVRAM.

The configuration should look similar to the following Catalyst 3550 configuration:

```
Current configuration : 1819 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname CstmrASwtch
!
enable secret 5 $1$ueGU$jTruyGB16bJKo9AIa8kkO/
!
ip subnet-zero
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/2
 no ip address
!
…Output ommitted…
!
interface GigabitEthernet0/1
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface Vlan1
 ip address 172.16.31.30 255.255.255.240
!
ip default-gateway 172.16.31.17
ip classless
ip http server
!
!
```

```
banner motd ^C This is a private system and may be accessed only by authorized users.
➥ Unauthorized access is strictly prohibited and will be enforced to the full
➥ extent of the law.^C
!
line con 0
line vty 0 4
 password imnotsure
 login
line vty 5 15
 password imnotsure
 login
!
end
```

Review Questions

1. What is the purpose of assigning an IP address and a default gateway to a Layer 2 switch?
2. What is the purpose of configuring passwords on the line configurations?
3. What are the available keywords for the `copy` command?
4. How is CDP useful to a Cisco administrator?
5. What ICMP protocol commands can help you determine whether you have IP connectivity to a device?
6. What is the significance of x and y in the output of the show interfaces stats output: x/line protocol is y?

Exam Questions

1. You wish to assign the password Cisco to only the first Telnet line. What series of commands will achieve this?

   - ❍ **A.** `line vty 0 4, login, password Cisco`
   - ❍ **B.** `line vty 0, login, password cisco`
   - ❍ **C.** `line telnet 0, login, password Cisco`
   - ❍ **D.** `line vty 0, login, password Cisco`

2. You just issued the `show ip interface brief` command. You noticed that interface serial 0 is down/line protocol is up. What can be determined by this output?

- ❍ **A.** Physical layer is up.
- ❍ **B.** Data Link layer is down.
- ❍ **C.** You cannot have a down/line protocol is up status.
- ❍ **D.** The interface is active.

3. You are trying to remotely Telnet into your switch, but you cannot connect the Telnet session. What are two possible reasons for this? (Choose 2.)

- ❍ **A.** A password was not assigned to the vty lines in the switch.
- ❍ **B.** The switch is operating in half-duplex.
- ❍ **C.** The router did not configure vty passwords.
- ❍ **D.** The switch was not properly assigned its `ip default-gateway`.

4. What are two commands that you can use to encrypt the password that allows you access into Privileged EXEC? (Choose 2.)

- ❍ **A.** `service password-encryption`
- ❍ **B.** `enable secret` *`password`*
- ❍ **C.** `enable password` *`password`*
- ❍ **D.** `encrypt enable` *`password`*

5. You copied and pasted a known working configuration from a text file into your new router via the terminal window; however, you do not have connectivity out all your interfaces. Why?

- ❍ **A.** You have to use TFTP to copy a configuration.
- ❍ **B.** The font in your text file was not Courier New.
- ❍ **C.** You have to do a `no shutdown` on the interfaces.
- ❍ **D.** The baud rate of your terminal program needs to be set to 38800.

6. What command shows you the configuration register?

- ❍ **A.** `show version`
- ❍ **B.** `show config-register`
- ❍ **C.** `show interfaces`
- ❍ **D.** `show flash`

7. You entered the following configuration in global config:

```
Router(config)#enable password cisco
Router(config)#enable secret giforgot
Router(config)#no enable secret giforgot
```

What will happen when you log out and try to re-enter Privileged EXEC?

- ❍ **A.** There will be no password.
- ❍ **B.** The password will be cisco.
- ❍ **C.** The password will be giforgot.
- ❍ **D.** Both passwords will work.

8. Which of the following commands does not close a Telnet session?

- ❍ **A.** `exit`
- ❍ **B.** `disconnect`
- ❍ **C.** Ctrl+Shift+6, *x*
- ❍ **D.** `logout`

9. Given the partial configuration output,

```
interface Ethernet0
 description /28 is 255.255.255.240 in decimal notation
 ip address 172.16.31.17 255.255.255.240
 shutdown
```

which of the following would you see when you issue the `show ip interface brief` command?

- ❍ **A.** `Ethernet 0  172.16.31.17... up  up`
- ❍ **B.** `Ethernet 0  172.16.31.17... up  down`
- ❍ **C.** `Ethernet 0  172.16.31.17... down  up`
- ❍ **D.** `Ethernet 0  172.16.31.17... administratively down down`

10. What command assigns a management IP address to a Layer 2 switch?

- ❍ **A.** `ip default gateway`
- ❍ **B.** `interface vlan 1`
- ❍ **C.** Layer 2 switches do not use IPs
- ❍ **D.** `interface fastethernet 0/1`

11. Given the following output, what can be determined about this interface? (Choose 2.)

```
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0003.e32a.4080 (bia 0003.e32a.4080)
  Internet address is 172.16.1.1/16
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliablility 255/255, txload 235/255, rxload 235/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:10, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     31 packets output, 2673 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 156848 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

- ❍ **A.** There is a duplex mismatch.
- ❍ **B.** The administrator needs to do a `no shutdown` on this interface.
- ❍ **C.** The bandwidth is incorrect.
- ❍ **D.** This link is congested.

12. Given the following output, how can you reconnect to Telnet session 2? (Choose 2.)

```
CCNA2620#show sessions
Conn    Host                Address           Idle  Conn Name
 1      131.108.100.152     131.108.100.152   0     131.108.100.152
*2      126.102.57.63       126.102.57.63     0     126.102.57.63
```

- ❍ **A.** `disconnect 2`
- ❍ **B.** Enter
- ❍ **C.** Ctrl+Shift+6, *x*
- ❍ **D.** `resume 2`
- ❍ **E.** `logout`

13. Which of the following is not a necessary step in copying configuration and IOS files to and from your Cisco router and switch and a local TFTP server?

- ❍ **A.** The TFTP server software must be running.
- ❍ **B.** Your router should be directly connected with a straight-through cable.
- ❍ **C.** Your interface must be on the same subnet as the TFTP server.
- ❍ **D.** You should test whether you have IP connectivity by pinging the server from your router.

14. What command assigns the last IP address in the 10th subnet of the network 192.168.100.0/29? Zero subnets are allowed.

- ❍ **A.** `ip address 192.168.100.80 255.255.255.240`
- ❍ **B.** `ip address 192.168.100.79 255.255.255.248`
- ❍ **C.** `ip address 192.168.100.70 255.255.255.240`
- ❍ **D.** `ip address 192.168.100.73 255.255.255.248`
- ❍ **E.** `ip address 192.168.100.78 255.255.255.248`

15. Given the following output,

```
Router>show flash
System flash directory:
File  Length   Name/status
  1   5510192  c2600-is-mz.120-3.T3.bin
[5510256 bytes used, 2878352 available, 8388608 total]
8192K bytes of processor board System flash (Read/Write)
```

What is the command used and what will be the outcome of upgrading to an 7KB IOS file from a TFTP server?

- ❍ **A.** `copy tftp ios`, the current IOS file will be erased.
- ❍ **B.** `copy flash tftp`, the current IOS will be unchanged.
- ❍ **C.** `copy tftp flash`, the current IOS file will be erased.
- ❍ **D.** `copy tftp flash`, the new IOS file is too large and it will go into RxBoot.

Answers to Review Questions

1. The IP address configured on a Layer 2 switch is used for remote management of the device (for example, Telnet, SSH, or SNMP). The default gateway is also important for a Layer 2 switch so it can respond to any of these management requests from devices that are not on its LAN. The switch must send these remote requests to the default gateway (router on the local LAN segment) to reach back to the management station initiating the request.
2. The password configurations on the terminal lines serve as a way to protect your router or switch from anyone gaining access to User EXEC.
3. The `copy` command tells the Cisco device to copy a file from somewhere to somewhere. The available keyword options for the `copy` command are `startup-config`, `running-config`, `tftp`, and `flash`.
4. CDP enables Cisco administrators to gain information from directly connected Cisco devices without requiring that they be connected with a terminal session. The `show cdp neighbors detail` or `show cdp entry *` command displays the Layer 3 address and the IOS version of the neighbors.
5. `ping` and `traceroute` use ICMP to test IP connectivity. `ping` tests if one device has connectivity to another device. `traceroute` displays the path the packets take to reach the destination. `traceroute` is useful for determining faulty routers along the path to the destination.
6. Given the `show interfaces` output x/line protocol is y, x represents the Physical layer status of the interface. y represents the Data Link layer status.

Answers to Exam Questions

1. **D**. To assign a login prompt and password for only the first vty line, you have to navigate to line vty 0. Answer A is incorrect because `line vty 0 4` is configuring all 5 vty lines. B has the correct navigation; however, the password is case sensitive. C is incorrect because the navigation to enter the Telnet lines is `line vty 0`.
2. **C**. The first part of the `show ip interface brief` command represents the status of the Physical layer, followed by the Data Link layer status. It is impossible to have this output because you cannot have Layer 2 without Layer 1 functionality. Answer A is incorrect because the Physical layer represented on the left side of the forward slash is down. B is also false because the Data Link layer represented on the right side of the forward slash is up. D is incorrect because an active interface is up/line protocol is up.
3. **A**, **D**. If the switch did not assign passwords to the vty lines, you receive the `password required, but none set` error, and cannot log in. In addition, because you are remotely Telnetting into this switch, there has to be a default gateway configured in the switch for you to be able to return the Telnet data to a remote network. B is incorrect because it does not matter at what speed or duplex the switch is operating. C seems viable, but you are not Telnetting into the router, so passwords are irrelevant.

4. **A**, **B**. The `enable secret` command encrypts the password with a one-way MD5 hash. The `service password-encryption` encrypts the `enable password` command and all other clear text passwords. C is incorrect because the command does not encrypt the password. D is not a valid command.

5. **C**. The configuration was saved to Notepad through the use of the `show running-config` command and copied from the terminal window into the file. The problem that occurs is that the `no shutdown` command does not display in the configuration, which means when the configuration is pasted back into a new router, the interfaces are still administratively shut. A is incorrect because you do not require TFTP to copy configurations that are saved in a text file on your computer. B is false because the font is not essential. D is incorrect because the baud rate does not need to be changed.

6. **A**. `show version` displays the current configuration at the bottom of the command output. Answer B is incorrect because the command does not exist. Answers C and D are valid commands, but they will not display the configuration register.

7. **B**. If the `enable secret` and `enable password` command are in the same configuration, `enable secret` overrides `enable password`. However, the example removed the `enable secret` command, leaving only `enable password` left in the configuration. Thus, the password to get into Privileged EXEC is cisco. A is incorrect because the `enable password` command was not removed. C and D are incorrect because the `enable secret` password was removed from the configuration.

8. **C**. Ctrl+Shift+6, x suspends the Telnet session. Answers A, B, and D are incorrect because those commands will actually disconnect the Telnet session.

9. **D**. Because the interface configuration is configured in a shutdown state, the interface status should report the ethernet interface as administratively down/line protocol is down. Answers A, B, and C are incorrect because a shutdown interface does not have the Physical layer or the Data Link layer in an up state.

10. **B**. To configure a management IP address on a switch, you have to apply it to the VLAN 1 logical interface. A is incorrect because that sets the gateway of last resort, not the IP of the switch. C is incorrect because Layer 2 switches use IPs for management. D is incorrect because Layer 2 switches do not assign passwords to physical interfaces.

11. **A**, **D**. Because there is an excessive number of late collisions in the output, it is safe to assume that there is a duplex mismatch. Also, the link is 92% congested as indicated by the load statements (235/255). B is incorrect because the interface status is up/line protocol is up. C is incorrect because the bandwidth is accurate for a FastEthernet interface.

12. **B**, **D**. You can resume the suspended Telnet sessions in this device by hitting the Enter key or typing the keyword, `resume`. Answers A and E disconnect the Telnet session and C suspends it.

13. **B**. If connecting directly to a TFTP server from a router, you must use a cross-over cable. Answers A, C, and D are necessary steps to copy files to and from a TFTP server.

14. **E**. With a /29 or 255.255.255.248 subnet, the increment of these subnets is 8. Starting with 0, counting 10 networks gives you a Network/Subnet identifier of 192.168.100.72 (0,8,16,24,32,40,48,56,64,72). The last IP address in that subnet is 192.168.100.78. Answer A is a network ID and the wrong subnet mask. Answer B is the broadcast address for that subnet. Answer C is that last IP address in ninth subnet with the wrong subnet mask. D is the first valid IP address in that subnet.

15. **C**. The command to upload your IOS from a TFTP server is `copy tftp flash`. Given the `show flash` output, there is not enough space for another 7KB file, so the current IOS file will be erased during the copy process, after which the actual download of the new IOS will occur. Answer A is incorrect because the `ios` keyword does not exist. B is false because there is not enough room in Flash for both files, so the current IOS is will be erased.

Suggested Readings and Resources

1. Valentine, Michael and Whitaker, Andrew. *CCNA Exam Cram 2*, Que Publishing, 2005.
2. Boney, James. *Cisco IOS in a Nutshell*, O'Reilly Publishing, 2001.
3. "Configuration Fundamentals Command Reference," www.cisco.com.

8

CHAPTER EIGHT

Bridging and Switching Operations

Objectives

This chapter covers the following Cisco-specific objective for "Technology," "Implementation and Operation," "Planning and Design," and "Troubleshooting" section of the Cisco Certified Network Associate exam:

Implement a LAN

Describe the principles and practice of switching in an ethernet network

Describe the Spanning Tree process

Customize a switch configuration to meet specified network requirements

- By adding Catalyst switches to your LAN and configuring them for optimal delivery of ethernet frames, you utilize a smart design for a LAN implementation.
- Although relatively transparent, it is still imperative that you understand the process involved with switches and bridges when they are forwarding frames in our LAN.
- A thorough knowledge of the inner workings of STP is a valuable tool to have when implementing and troubleshooting a switched network.
- Even though a Cisco switch's default configuration is enough for basic Layer 2 operations, having the knowledge necessary to customize and tweak the configuration settings is invaluable to ensure your LAN is running at its full potential.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- One of the best practices when reading about the switching and bridging functions is to visualize the information contained in the ethernet frames and imagine how the bridge and switch use that information to build its forwarding table and forward frames to other network segments.
- Complete the Challenge Exercises and the Exercises at the end of the chapter. The exercises will solidify the concepts that you have learned in the previous sections.
- After you have read and understood Spanning Tree Protocol, try to draw your own LAN design and determine the STP elections and port roles that will result from your design.
- Complete the Exam Questions at the end of the chapter. They are designed to simulate the type of questions you will be asked in the CCNA exam.

Introduction

You have already learned in Chapter 3, "Data Link Networking Concepts," that you can use bridges and switches to segment a LAN into smaller collision domains. This chapter looks in close detail at the operations of bridges and switches. Specifically, you will investigate the transparent functionality that occurs when a bridge or switch is building and utilizing its frame forwarding logic, as well as the peculiar nature of Spanning Tree Protocol (STP) in redundant switched networks.

Bridging and Switching Functionality

Objective:

Implement a LAN
Describe the principles and practice of switching in an ethernet network

Bridges and switches forward frames based upon the Layer 2 ethernet MAC addresses. Both devices receive ethernet frames transmitted from other devices and dynamically build a MAC address table based upon the source MAC address inside of those frames. This MAC address table is commonly referred to as a Content Addressable Memory (CAM) table.

These dynamic entries in the CAM table are not permanent, however. After the switch or bridge stops receiving frames from a certain MAC address (varies, but typically 5 minutes), the entry is removed from the CAM table to save memory and processor resources. The exceptions to this are static MAC entries that have been manually configured on a port-by-port basis for security and control purposes.

When deciding to which port to forward the ethernet frame, a bridge or switch consults this CAM table and forwards the ethernet frame based upon the destination MAC address of the ethernet header. In instances where the destination MAC address is not in the table, it copies and forwards the frame out every port except the one at which it was received. This action is commonly known as flooding.

EXAM ALERT

It is important to remember that switches and bridges build their MAC address tables using the source address in an ethernet frame header. In addition, they base their forwarding decisions on the destination MAC address in an ethernet frame header.

Recall that bridges and switches segment LANs into collision domains; however, they still are in a single broadcast domain. Switches and bridges do not have entries for broadcast addresses (FFFF.FFFF.FFFF) or multicast addresses (0100.5E00.000-0100.5E7F.FFFF) in their CAM

tables. As previously mentioned, when a bridge or a switch receives a frame with a destination MAC address not in its table, it floods that frame out every port.

EXAM ALERT

When a switch receives an ethernet frame with a broadcast, multicast, or unknown unicast (destination MAC address of ethernet frame not in CAM table), it will flood that frame out every port except the one with which it was received.

For instance, consider the switched topology example illustrated in Figure 8.1. When Computers A, B, C, and Printer D originally sent an ethernet frame, the switch recorded the source MAC address of that frame and the associated port in its CAM table. If Computer A sends an ethernet frame destined for Printer D's MAC address of 1111.2222.3333, the switch forwards only that frame out to its Fast Ethernet 0/14 interface. If Computer A sends a broadcast with a destination of FFFF.FFFF.FFFF, that entry does not exist in the CAM table, so that frame is flooded out all interfaces except for Fast Ethernet 0/1.

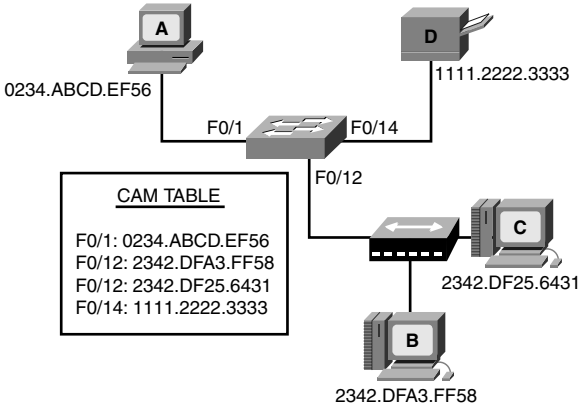


FIGURE 8.1 Switch address learning and forwarding.

Notice that Computers B and C are plugged into a hub. So what happens when Computer B sends an ethernet frame to Computer C? The frame hits the Layer 1 hub, which regenerates the signal out all ports (regardless of the MAC address because it is a Physical layer device). When the frame reaches the switch, the switch realizes that the source and destination MAC addresses reside on the same interface, so it does not send that frame on to any other ports. This process is also known commonly as *filtering*.

Frame Transmission Methods

Switches are often classified based upon the method in which they process and forward frames in and out of their interfaces. This classification differs depending on the device's processing

capabilities and manufacturer. The three transmission methods that a bridge or switch may use are discussed in the following sections.

Store-and-Forward

Properly named, the store-and-forward method of frame transmission involves the switch or bridge, which buffer (store temporarily in a small memory location) the entire ethernet frame and perform a cyclic redundancy check (CRC) of that frame to make sure it is not a bad frame such as a runt (frame that is below minimum frame size) or a giant (frame that is above maximum frame size). If the frame calculation detects a bad frame, it is dropped at that point. Thus, the frame is forwarded only if the CRC calculation results in a normal frame.

Because the entire frame is checked, store-and-forward switching is said to be latency (delay) varying. In other words, depending on the payload inside the frame, the switch takes varying processing times to buffer the entire frame and perform the CRC before sending it to its destination. Although this method sounds like a lengthy process, this is the most widely used method of switching in Cisco Catalyst switches because the hardware processors for the interfaces are so advanced and robust that the switch hardly works up a sweat.

Cut-Through

Cut-through transmissions are practically the antithesis of store-and-forward frame transmission. In fact, instead of processing the entire frame, cut-through switching entails the switch or bridge buffering just enough information to know where to forward the frame before sending it on to another segment. In other words, it looks only up to the destination MAC address in the ethernet header and sends it on regardless of whether the frame contains errors.

This "hot potato" method of frame transmission was once appealing for devices with low processing power. Because it has to inspect only the beginning of an ethernet frame header, latency is not a factor with this method. The downside to cut-through switching, however, is that it still passes bad frames on to other segments because it does not perform CRC calculations of any kind.

Fragment-Free

In a true Goldilocks fashion, if cut-through is too hot and store-and-forward is too cold, then fragment-free may be just right for you. Fragment-free is a hybrid of the two transmission methods because it buffers up to the first 64 bytes of a frame to ensure that it is not a runt frame (most collisions occur within the first 64 bytes). This obviously is not as fast as cut-through; nevertheless, it ensures that many of the invalid frames in the LAN are not transmitted on to other segments. Figure 8.2 illustrates how much of an ethernet frame is buffered and processed with each of the three transmission methods discussed.

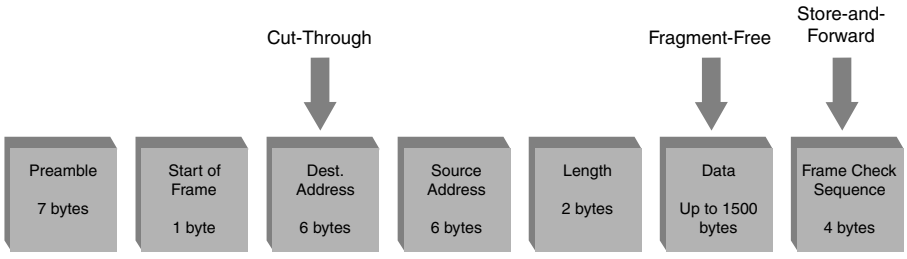


FIGURE 8.2 Frame transmission comparison.

EXAM ALERT

Store-and-forward buffers the whole frame, does a CRC calculation, and is latency varying. Cut-through buffers up to only the destination MAC address. Fragment-free buffers up to the first 64 bytes before sending the frame on to another segment.

Half- and Full-Duplex Connections

Data communication on bridge and switch ports can occur in either half- or full-duplex transmissions. Half-duplex connections are unidirectional in that data can be sent in one only direction at one time. This is similar to the two-way radios or walkie-talkies in which only one person can speak at one time. With half-duplex communication in an ethernet network, CSMA/CD (carrier sense multiple access with collision detection) is enabled, which allots 50-60% of the bandwidth on the link.

Full-duplex, on the other hand, is indicative of two-way communication in which devices can send and receive information at the same time. With these connections, CSMA/CD is automatically disabled, allowing for 100% of the bandwidth in both directions. In fact, it uses the two wires that typically are used for detecting collisions to simultaneously transmit and receive. Because CSMA/CD is disabled, that means the connection has to be in an environment where collisions cannot occur. In other words, it must be connected to a switch or directly connected with a cross-over cable.

EXAM ALERT

If you are connected to a hub, the connection must be half-duplex with CSMA/CD. When running full-duplex, you must be connected to a switch.

NOTE

Because full-duplex allows 100% in both directions, it is sometimes advertised at twice the speed. For instance, a 100Mbps interface might be marketed as achieving 200Mbps. Although it is advertised as 200Mbps, in reality, you are receiving 200Mbps of *throughput*.

Switches and Bridges Comparison

Because switches and bridges share so many commonalities, the question becomes, "What is the difference between a bridge and a switch?" The most glaring difference is that ethernet bridges are older devices that rely on software for forwarding frames. Catalyst switches have frame-processing hardware chips called ASICs (Application-Specific Integrated Circuits) that can forward frames exponentially faster than software can.

In addition, a multi-port bridge can support up to only 16 interfaces. Modern switches, on the other hand, can have a port density of 10 times or more that of their older sibling. In fact, some of the larger Catalyst chassis can hold blades and blades of switch ports that can support modern speeds (such as 10 gigabit ethernet) and forward millions of frames per second.

A bridge can also operate only in half-duplex mode, in which the interfaces forward frames with the store-and-forward method. This was problematic with older bridges: You could notice the delay in storing the entire frame and performing the CRC because this was all done by slow software. Today, switches don't share those concerns because their interfaces have ASIC technology and can operate in half- or full-duplex.

Switching Design

You have already seen how switches operate when connected to end-user devices such as PCs, printers, and servers. However, when switches are connected to other switches to form a redundant network, a switching loop can occur. Figure 8.3 illustrates a scenario in which a switching loop can occur.

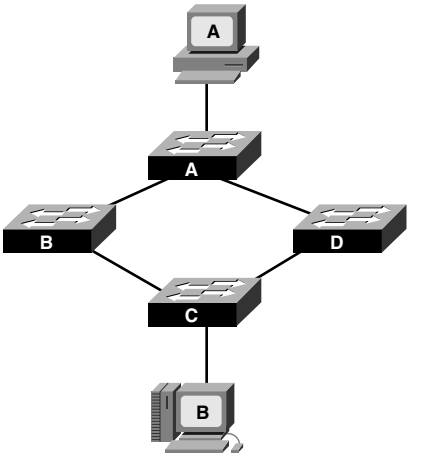


FIGURE 8.3 Redundant switch design.

In this design, redundant links interconnect the switches together. Although it is a good idea to have redundancy in the network, the problem arises when a computer sends out a frame with a broadcast, multicast, or unknown unicast destination MAC address. Recall that any of these three transmissions causes a switch to copy and flood that frame out all ports except for the one on which it came in. So if Computer A sends a broadcast, Switch A floods that out to Switches B and D. Once again, if this is a broadcast message, Switches B and D flood that frame out to Switch C. Staying true to its design, Switch C floods the frame back to Switches B and D, and so on. Broadcasts continuously circle the switched network until ultimately the amount of broadcast traffic consumes the switched network's bandwidth and all traffic ceases to flow. This unsettling scenario just described is called a *broadcast storm* and can be avoided completely by using a Layer 2 protocol sent among switches called the *Spanning Tree Protocol*.

Spanning Tree Protocol

Objective:

Describe the Spanning Tree process

Once a proprietary protocol from DEC, Spanning Tree Protocol (STP) was standardized and blessed by the IEEE specification, 802.1d. STP allows networks to maintain a level of redundancy while disabling the detrimental side effects that can occur such as broadcast storms. Enabled by default on most switches, STP forms non-circular (no looping) paths throughout the internetwork by performing an election and basing calculations on that election. These calculations dictate which ports should remain in a non-forwarding (known as *blocking*) state to eliminate redundant loops that can cause broadcast storms. STP also can react to changes in the switched network to ensure that the redundant links may be used in the event of a topology change such as a link going down. The following sections exactly how this remarkable protocol operates behind the scenes in a LAN.

EXAM ALERT

Remember that STP is standardized by the IEEE 802.1d specification and is used to prevent switching loops in a switched network.

Root Bridge

As previously mentioned, STP performs an election in the switched topology. The winner of this election serves as the base of all calculations and ultimately becomes the root to the spanning tree. Conveniently, this elected bridge or switch is called the *root bridge*. From the root

bridge, non-circular branches extend throughout the switched network like those of a tree—a spanning tree.

NOTE

Don't let the term "root bridge" confuse you. When the 802.1d specification was drafted for STP, it was referred to as a "root bridge" because bridges were the prominent devices at the time. In modern times, it can just as easily be a switch.

So how does this election take place? You can rule out electoral votes because each bridge or switch believes itself to be the root bridge at startup. The deciding factor on who becomes the root bridge is something referred to as the Bridge ID. The Bridge ID comprises two components:

- *Priority*—This is an arbitrary number from 0–61440, which can be administratively set in increments of 4096. The default value for priority is 32768, or 8000 in hex.
- *MAC Address*—The 48-bit MAC address of the switch itself.

The device with the lowest Bridge ID becomes the root bridge. If a new switch or bridge is added with a lower Bridge ID to the switched network, a new election takes place and that switch ultimately becomes the new root bridge for the switched network.

Consider the example displayed in Figure 8.4. Notice that all switches have their default priority value of 32768 in their Bridge IDs. Thus, the lowest MAC address ultimately dictates who will win the election. Because Switch A has the lowest MAC address in the switched network, it will be the root bridge.

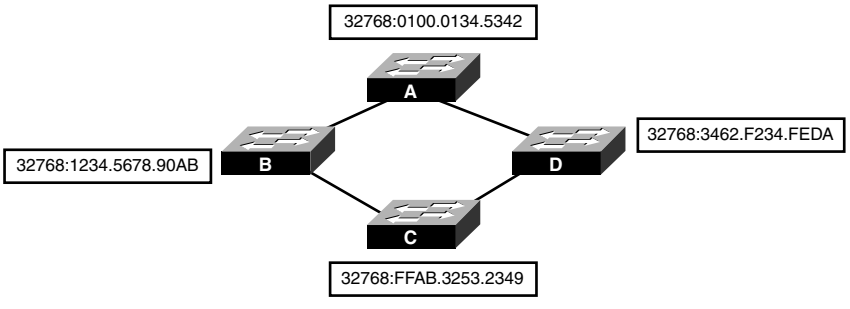


FIGURE 8.4 Root bridge election.

EXAM ALERT

Be prepared to be able to determine which switch is the root bridge, given a topology diagram of a switched LAN.

Because this election process occurs automatically with bridges and switches, it is highly advised that you change your priority in a robust and reliable switch in your internetwork as opposed to letting this election occur by chance. This is especially true because manufacturers choose the MAC address, and a lower MAC address could very well mean an old or low-end switch or bridge, which might not be the best choice for your root bridge. How to manually set the priority is discussed later in this chapter.

These Bridge IDs are advertised to each other through Bridge Protocol Data Units (BPDUs). These messages are sent as multicasts every 2 seconds out a switch's interfaces to other switches on adjoining segments. In addition, these messages also contain the Bridge ID of the root bridge in every update that is sent. As long as you are receiving BPDUs that contain a higher Bridge ID than your Bridge ID, you will remain the root bridge (because all devices assume they are the root at startup).

Root Ports

In addition to the local Bridge ID and the root Bridge ID, BPDUs contain information that helps switches perform calculations to decide which ports should be forwarding and which should be blocking to create a loop-free switched network. The key to this calculation lies within the cumulative cost back to the root bridge. Although it sounds as if these Cisco switches are keeping track of how much you paid for them, this is not what is meant when you use the term "cost." The cost is actually an inverse of the bandwidth for each link segment. Because it is the inverse, the lower the cumulative cost back to the root bridge, the faster the path is. Table 8.1 lists the standard costs used today in switches. It is possible to change these values administratively if you want to control which link becomes the best path to the root bridge.

TABLE 8.1 Port Cost Values

Interface	Cost
10Gbps	2
1Gbps	4
100Mbps	19
10Mbps	100

After the root bridge is determined, each **non-root** switch or bridge forms an association back to the root bridge based upon the lowest cumulative path cost back to the root. Whichever interface has the fastest route to the root bridge automatically becomes a forwarding port called the *root port*.

NOTE

The root port is determined for the entire switch. Thus, each switch should contain only one root port back to the root bridge.

The root bridge advertises a root path cost of 0 to Switches B and D. As the BPDU enters their interfaces, they add the cost value of that interface and advertise that to any adjacent switches on other segments. Every **non-root** bridge determines its fastest path back to the root by looking at these BPDUs that it receives from other switches. For instance, Switch B knows that going out of the top segment back to the root has a cost of 4, and going through Switch C has a cost of 42. Because the top segment has the lowest cumulative cost, that becomes the root port for Switch B.

What would happen if there were a tie in the root path cost? For instance, Switch C has two equal cost paths of 23 back to the root bridge through Switch B and Switch D. In the event of a tie, the following are calculated in order to determine the root port:

1. The port with a switch advertising the lowest Bridge ID.
2. If the same Bridge ID (parallel links to the same switch), then the lowest port priority is used. The port priority is an arbitrary number assigned to an interface that can be administratively set to choose one link over another. The default value is 128.
3. If the same port priority, the ultimate tiebreaker is the lowest interface number, for example, Fast Ethernet 0/1 over Fast Ethernet 0/6, because the links are identical.

Figure 8.5 has expanded on the switched networking example to include the path costs.

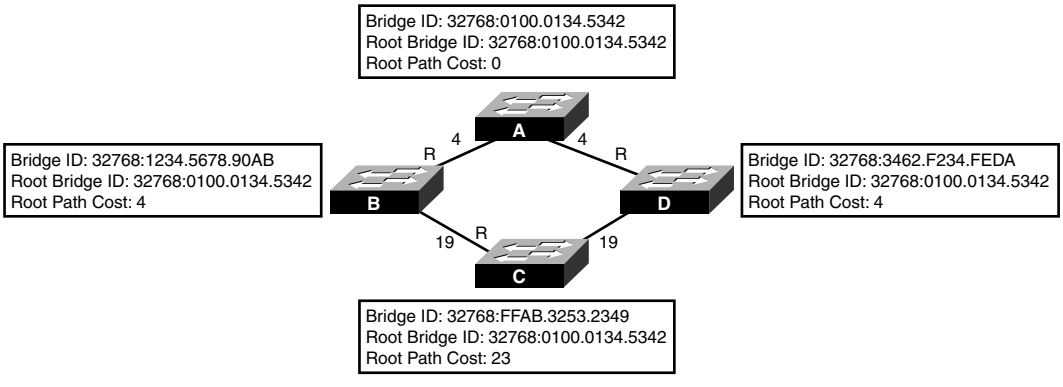


FIGURE 8.5 Root port calculation.

Designated Ports

After every switch has determined its root port, the switches and bridges determine which port is to become the designated port for every segment that connects the two switches. As the name states, the designated port is the port on each interconnecting segment that is designated to forward traffic from that segment to another segment back to the root bridge. This too is determined through a calculation of the fastest way back to the root port. In the case of a tie, the same decision criteria applies to designated ports as root ports as described earlier.

In the example depicted in Figure 8.6, the designated ports have been calculated based upon which switch is advertising the lowest cumulative cost back to the root on each segment. For instance, the BPDUs from Switch B to Switch C are advertising a root path cost of 19, whereas the BPDU being sent from Switch C to Switch B is advertising 38. Because Switch B has the lower root path cost, that is the designated port for that segment.

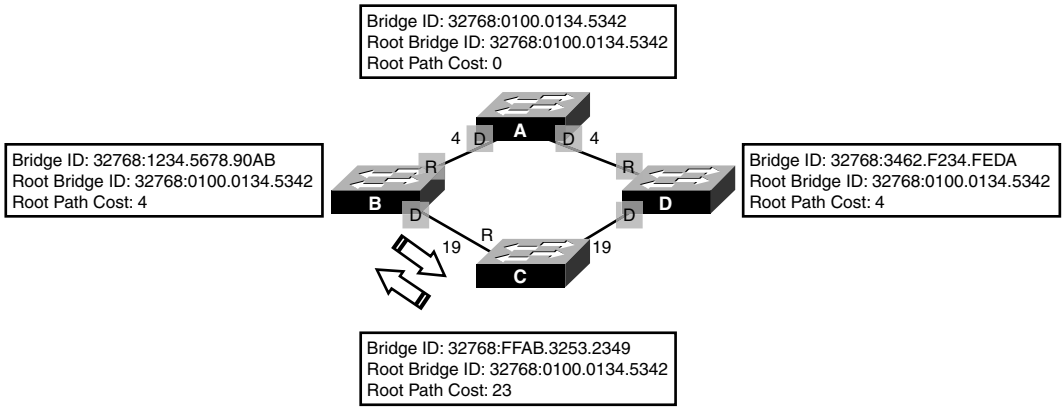


FIGURE 8.6 Designated port calculation.

Blocked Ports

To this point, the discussion has focused on how to determine which ports will be forwarding traffic in a switched network. Yet to be addressed is the original point of STP, which is to remove any potential switching loops. To remove potential switching loops, switches and bridges keep any port that is not a root or designated port in a blocked state. Keep in mind: A blocked state is not disabled (shut down); the interface is just not participating in forwarding any data. Blocked interfaces still received BPDUs from other switches to react to any changes in the topology.

EXAM ALERT

Keep in mind for the exam that a blocked interface will still receive BPDUs from other switches.

In Figure 8.7, notice that all the root ports have been elected, as well as the designated ports for each segment. Notice on the segment between Switch C and Switch D that a port connected to Switch C is not a root port or a designated port. This port blocks user data to ensure that a switching loop does not occur and expose the network to broadcast storms. This also means that any devices connected to Switch C sending ethernet data to any device connected to Switch D will ultimately go through Switch B, then Switch A, to finally arrive at Switch D.

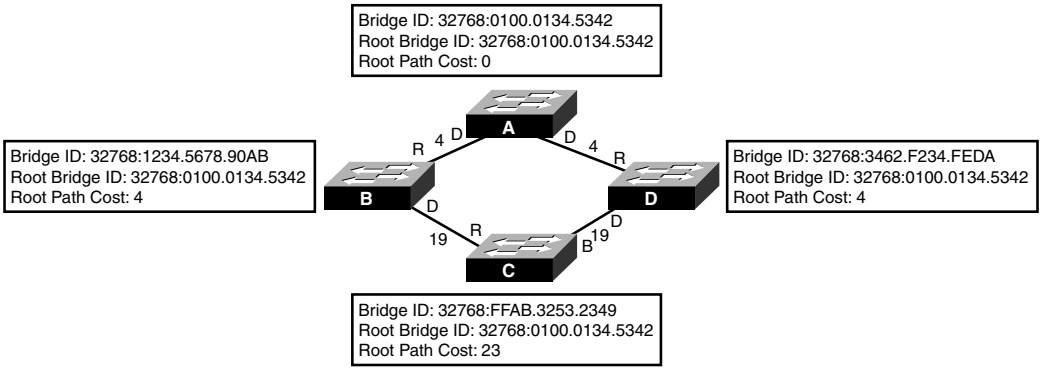


FIGURE 8.7 Blocked port calculation.

Challenge

To ensure your understanding of STP, this challenge steps you through the scenario illustrated in Figure 8.8.

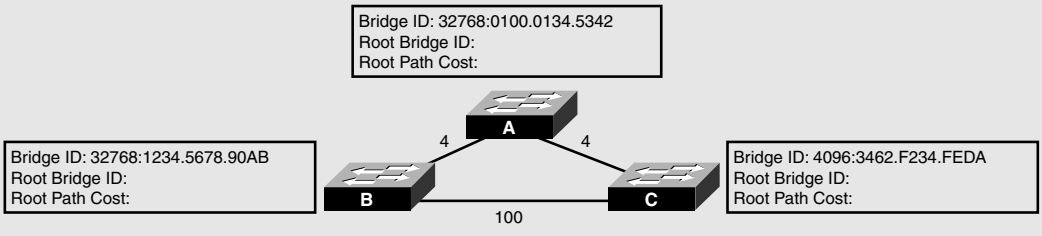


FIGURE 8.8 STP challenge scenario.

1. All switches believe themselves to be the root bridge at startup. After sending their BPDUs, which switch remains the root bridge and why?
2. Every **non-root** bridge determines its root ports. Which interfaces become root ports based upon the election result?
3. Every segment must have a designated port to use to forward traffic onto other segments. Which interfaces on the three segments will be designated ports?
4. One port should remain that is not designated or a root port. In what state will this port be?

Challenge Answer

Figure 8.9 displays the end result of the STP election and calculation. Switch C becomes the root bridge in this design because the default priority was administratively changed in this design to 4096, giving Switch C the lowest Bridge ID. Because Switch A and Switch B are **non-root** bridges, they must calculate their root ports based upon the lowest cumulative cost back to the root bridge. For each segment, the switch with the lowest root path cost will be the designated port. Because Switch C's interface on the lower segment is not a root or designated port, that interface will be blocking.

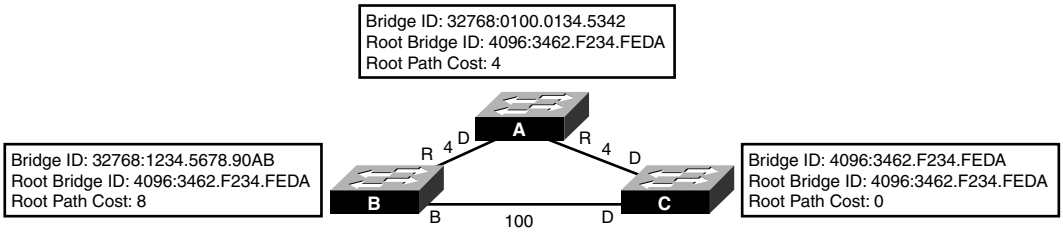


FIGURE 8.9 STP challenge scenario answer.

Port State Transitions

You now know how STP removes switching loops in your switched LAN by electing a root bridge and calculating which ports should forward based upon the lowest root path cost. However, as explained earlier, STP must be able to react to topology changes, such as a segment or switch going down, to ensure the redundant design is put to good use. When this type of change occurs, ports that were once in a blocking state could quite possibly transition to a forwarding state.

If devices were to immediately transition from a blocking state to a forwarding state, they could easily cause loops in the network because the topology change did not have a chance to propagate throughout the entire switched network. To remedy this dilemma, STP transitions into two intermediate states before moving to a forwarding role. In these transitionary states, the switch ensures that enough time has transpired to propagate the changes, and it undergoes a pre-forwarding routine to ensure that it will know where to forward the data when the interface is forwarding. Table 8.2 displays, in order, the possible STP states, their functions, and the time it takes to transition out of each state.

TABLE 8.2 STP Port States

State	Function	Transition Time
Disabled	Interface is administratively shut down or inoperative as a result of a security violation.	NA
Blocking	Does not forward any user data. All ports start out in this state. Does not send, but still can receive BPDUs to react to topology changes.	0–20 seconds
Listening	Begins to transition to a forwarding state by listening and sending BPDUs. No user data sent.	15 seconds
Learning	Begins to build MAC addresses learned on the interface. No user data sent.	15 seconds
Forwarding	User data forwarded.	

It may initially take the switch 20 seconds to start the transition process to the listening stage because that is the default time limit that STP uses to consider a neighbor switch to be down. In other words, if a switch stops hearing 10 BPDUs (equal to 20 seconds) from an adjoining switch or bridge, it considers that device to be dead and must react to the new topology. This 20-second timer is known as the *max age timer*.

The listening and learning states wait 15 seconds each by default, but can be administratively changed if you have a relatively small switched network. These 15-second intervals are commonly referred to as *forward delays* because they delay the transition to a forwarding state. It is important to consider that it could take up to 50 seconds for an interface to transition to a forwarding state when the topology changes. Consequently, no data will be transferred in those 50 seconds—which in the networking world is about 10 phone calls of complaining endusers.

EXAM ALERT

A STP topology change could take up to 50 seconds.

The max age and forward delay timers are based upon a default network diameter of seven switches including the root bridge. Diameter (in switching terms) refers to the number of bridge or switches between any two hosts. If your network is, for instance, only a diameter of 2, you can decrease these timers because it doesn't take as long to propagate a change in the topology. Another benefit of STP is that these timers are ultimately dictated by the root bridge. Thus, to change the timers, you have to configure the change on only the root bridge and it will get propagated to the other switches. This change could possibly backfire and cause switching loops in instances when you add more switches to the network and forget to change the timers. The next section discusses some safer alternatives to speed up the convergence time of STP when a topology change occurs.

Enhancements to Spanning Tree Protocol

The steps to transition to a forwarding state in STP are critical to ensure that the switched network has enough time to propagate a change in the topology. However, in the networking world, 50 seconds is a lot of down time. In some instances, these 50 seconds may be detrimental because of the disruption of data traffic and should be avoided if it is safe to do so. In light of these scenarios, Cisco has created some enhancements to normal STP operation that can decrease the time it takes for the switched network to converge (have a consistent perspective of network), which is discussed in the next sections.

PortFast and BPDU Guard

Imagine you just plugged in your DHCP or Cisco CallManger VoIP server into your switch. Because STP is running on all ports on the Catalyst switches by default, the interface into which you plug your server transitions from a blocking state to the listening, followed by the learning, and finally forwarding. In those 30 seconds, devices such as IP phones and computers cannot use those services that the server provides because no data transfer can occur until spanning tree is in a forwarding state.

To speed up the spanning tree process for end devices such as servers, you can configure your first STP enhancement, called PortFast. If you configure this feature on an interface, it skips the listening and learning stages and transitions immediately to a forwarding state to enable instant data transfer.

If you enable PortFast on an interface, it is imperative that you never plug a switch or a hub into it. This could easily cause a loop in your switched network. In fact, Cisco has added a function to PortFast called BPDU Guard that acts as a loop-preventive detector for BPDUs on a PortFast-enabled interface. When a BPDU is received on a PortFast-configured interface with BPDU Guard enabled, the port is disabled automatically and must be enabled by an administrator to ensure that a switching loop will not occur.

EXAM ALERT

PortFast will immediately transition from a blocking to a forwarding state on ports connected to end-devices. BPDU Guard is a feature that disables the PortFast-enabled interface if a BPDU is received on that port.

UplinkFast

In an optimal redundant switching design, you would have redundant high-end distribution layer switches in your network, with your access layer switch having an uplink to both as depicted in Figure 8.10. With this design, if your root port were to fail, it would still take at least 30 seconds to transition the backup link to a forwarding state. With a feature called

UplinkFast, you can bypass the listening and learning state for this redundant uplink to ensure faster recovery.

NOTE

For UplinkFast to work, the access later switch must have direct knowledge of link failure (a link that is connected to the switch), it must have one port in a blocking state, and the link failure must be on the root port.

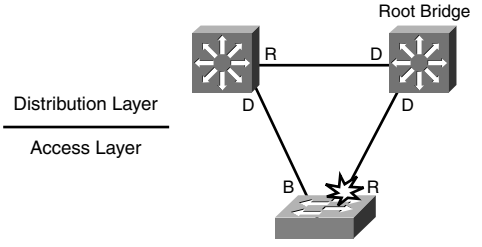


FIGURE 8.10 UplinkFast switching design scenario.

BackboneFast

BackboneFast is similar to UplinkFast, in which a redundant link transitions faster than normal to a forwarding state. The difference is that the transition occurs without having direct knowledge of the link failure. Consider the scenario displayed in Figure 8.11. In this scenario, the failure actually occurs on the link between the two distribution layer switches. When that link fails, the distribution switch on the left begins to have delusions of grandeur and believe it is the root bridge, and it advertises that to the access layer switch. Because this access switch still has connectivity to the actual root bridge, it disregards the left distribution switch's false BPDUs (referred to as *inferior BPDUs*). By design, it must wait the max age (20 seconds) before transitioning to a learning state on its backup link and send a BPDU to the distribution switch informing it of access to the actual root bridge.

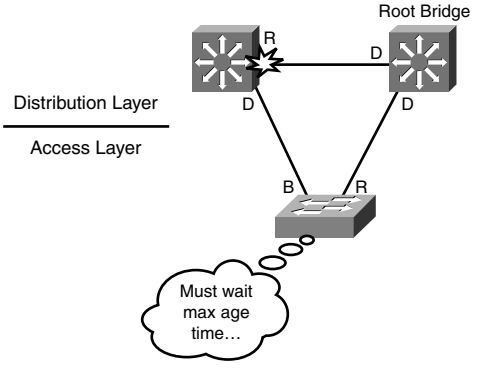


FIGURE 8.11 BackboneFast switching design scenario.

With BackboneFast, the access layer switch bypasses the max age time and immediately transitions from blocking to listening. After the distribution switch receives that BPDU from the access layer switch, it realizes it has a path to the root bridge through the access layer switch, and that corresponding interface becomes its root port.

Configuring and Verifying MAC Addresses

The default state of Cisco Catalyst switches is to learn MAC addresses dynamically. For security purposes, you have the capability to assign static MAC addresses to an interface to ensure that a MAC address is recognized on only a specific interface. For instance, if you want to make sure that no one tries to connect to your switch and spoof (falsely configure) your server's MAC address of FA23.239B.2349, you could use the following command to statically assign that MAC to the Fast Ethernet 0/2 interface:

```
Switch(config)#mac-address-table static FA23.239B.2349 vlan 1 interface
➥FastEthernet 0/2
```

To verify your static and dynamically learned MAC addresses stored in the CAM table of the switch, use the `show mac-address-table` command as demonstrated here:

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
…Output Omitted…
   1    0000.399e.0789    DYNAMIC     Fa0/3
   1    000d.65d0.4e18    DYNAMIC     Fa0/1
   3    FA23.239B.2349    STATIC      Fa0/2
Total Mac Addresses for this criterion: 50
```

Port Security

Anybody that has physical access to the ports of your switches can easily attach another switch or hub to enable more devices to be on the switched network. If you want to limit the number of MAC addresses that can be dynamically learned on a switch port (for environments such as college campuses and hotels), you can enable the port security feature on your switch ports that are accessible to end-users. With the `switchport port-security` commands, you can define the maximum number of MAC addresses to be learned on an access port. If this maximum number is exceeded, the switchport can be put in a disabled state in which you have to re-enable the interface. Although a bit drastic, it is a sure fire way to ensure switch administrators are aware where the violation occurred and help identify the users who might be responsible.

To configure port security, you must enable this function on each interface, followed by the maximum MAC count allowed on the interface. For example, if you wanted to restrict the number of MAC addresses allowed to one MAC addresses, you would use the following configuration on the port:

```
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
```

Furthermore, the switch can disable the switchport when a violation occurs by entering the following command:

```
Switch(config-if)#switchport port-security violation shutdown
```

EXAM ALERT

The `switchport port-security maximum` command restricts the number of MAC addresses that can be learned on a switch interface. The `switchport port-security violation shutdown` instructs the switch to disable the port when a violation occurs.

Configuring and Verifying Spanning Tree Protocol

Objective:

Customize a switch configuration to meet specified network requirements

STP is enabled by default on all Cisco Catalyst switches. In fact, if you are running multiple VLANs on your switch (discussed in Chapter 9, "Virtual LANs"), Cisco switches run an instance of STP on each VLAN configured. With that being said, no configuration is required unless you want to alter the default parameters of STP or you want to utilize some of the Cisco enhancements such as PortFast, UplinkFast, or BackboneFast.

Changing Priority and Port Cost

One of the common configurations you might encounter in your travels is to change the default priority of a switch to ensure that it will win the election for root bridge. To configure this option, you have to define which VLAN's priority you want to change and give a value in increments of 4096. For instance, if you wanted your switch to be the root bridge for VLAN 1, you would configure the following in Global Configuration:

```
Switch(config)#spanning-tree vlan 1 priority 4096
```

Cisco also created a command that automatically changes the switches priority to become the root bridge for a given VLAN:

```
Switch(config)#spanning-tree vlan 4 root primary
```

If you wanted to change the default cost calculations for a specific interface to ensure that a port becomes a forwarding interface, you can change the spanning tree cost on any interface by entering the interface configuration mode and using the following command:

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#spanning-tree cost 1
```

Configuring Cisco STP Enhancements

To enable the Cisco enhancements on a Catalyst switch, you can configure PortFast with BPDU Guard on an interface-by-interface basis; conversely, UplinkFast and BackboneFast are configured globally on the switch as demonstrated in the following configuration:

```
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#spanning-tree portfast bpduguard
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
Switch(config-if)#exit
Switch(config)#spanning-tree uplinkfast
Switch(config)#spanning-tree backbonefast
```

Verifying Spanning Tree Protocol

To verify spanning tree operation in your switch, you can issue the `show spanning-tree` command to see a display of the STP operations for each VLAN. If you want to see specific information regarding a particular VLAN or interface, you can also add additional keywords after the command to see the output for only those items. For example, Figure 8.12 illustrates the output of the STP statistics for VLAN 1.

```
Switch#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000d.65d0.4e00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000d.65d0.4e00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg LIS 19        128.1    P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Back BLK 19        128.24   P2p
```

FIGURE 8.12 `show spanning-tree` output.

Notice in this output that you can see the MAC address and the priority of the root bridge and the local switch (which happens to be the root bridge for this VLAN). In addition, you can see the timers using in 802.1d for port state transitions including the max age and forward delay. Finally, this useful `show` command displays the interfaces that are active and participating in STP and their associated role and state in the spanning tree network.

Chapter Summary

This chapter explored the mysteries behind ethernet bridging and switching. Namely, it showed how bridges and switches build their MAC address table (also known as a CAM table), using the source MAC address of ethernet frames, and forward, filter, or flood those frames based upon the destination MAC. The method in which it forwards the frames differs from switch to switch. Specifically, the switch might use the latency varying store-and-forward transmission method, which buffers the entire frame and calculates the CRC before forwarding the frame. Cut-through switching looks at only the destination MAC address in an ethernet frame, whereas fragment-free looks at up to the first 64 bytes, in which most collisions occur.

Switch connections can communicate in half-duplex or full-duplex, depending on the device to which they are connected. For instance, half-duplex connections are unidirectional and must be used when connecting to a hub because collisions must be detected. Full-duplex allows bidirectional communications to occur on the link is used when you are connecting to other switches or directly to devices that support it. With full-duplex connections, CSMA/CD is disabled so the devices can send and receive at the same time.

When multiple switches are connected in a redundant design, STP (IEEE 802.1d) removes the possibility of switching loops, which can cause broadcast storms. It achieves this by electing a root bridge based upon the lowest Bridge ID (priority + MAC) being advertised in BPDUs. After the root bridge is elected, every **non-root** bridge forms an association to the root bridge by determining the port with the best path (lowest cumulative cost), which becomes the root port. For every segment, a designated port is also elected based upon the fastest route back to the root bridge. In the event of a tie, the Bridge ID is used, followed by the lowest port priority, and finally the lowest port ID.

STP ports start in a blocking state in which no data or BPDUs are being sent. If the port is capable of forwarding frames, it transitions to a listening state for 15 seconds (forward delay), where it begins to exchange BPDUs. The learning stage follows for another 15 seconds to learn the MAC address on the interface, then finally transitions to a forwarding state.

Cisco created some means to speed up these STP transitions that can be configured on Catalyst switches. PortFast allows the switch port to go immediately to a forwarding state for end devices such as servers. To protect these interfaces from forming a switching loop (by accidentally connecting a hub or switch to the PortFast interface), Cisco created BPDU Guard that disables the interface if a BPDU is received on the interface. UplinkFast also skips the listening and learning transitions when a direct failure occurs on a switch with redundant uplinks to its distribution switch. BackboneFast speeds up convergence by skipping the max age time when switches learn of a failure indirectly.

Key Terms

- CAM table
- Store-and-Forward
- Cut-through
- Fragment-free
- Half-duplex
- Full-duplex
- STP
- Root Bridge
- BPDUs
- Bridge ID
- Root Port
- Cost
- Designated Port
- Blocking
- Listening
- Learning
- Forwarding
- Max-age timer
- Forward-delay timer
- PortFast
- UplinkFast
- BackboneFast
- BPDU Guard

Apply Your Knowledge

Exercises

8.1 Force the Election

This exercise entails connecting two switches and watching the election with STP.

Estimated Time: 10 minutes

1. Power on both switches without connecting the two together.
2. Console into one switch and navigate to User EXEC.
3. Connect the two switches with a cross-over cable.
4. Verify which switch is the root bridge from the `show spanning-tree` output.
5. On the switch that is not the root bridge, force the election by changing the priority to 4096.

8.2 Witness the Wonders of STP

This exercise will force the STP election by changing the priority in a switch.

Estimated Time: 5 minutes

1. Power on both switches without connecting the two together.
2. Console into one switch and navigate to User EXEC.
3. Connect the two switches with a crossover cable.
4. Issue the `show spanning-tree` command immediately after connecting to watch the port state change to listening.
5. Issue the `show spanning-tree` command within another 15 seconds to see the state change to learning.
6. Issue the `show spanning-tree` command after another 15 seconds to see the state change to forwarding.

8.3 Time Flies with PortFast

This exercise will force the STP election by changing the priority in a switch.

Estimated Time: 5 minutes

1. Power on both switches without connecting the two together.
2. Console into one switch and navigate to User EXEC.
3. Configure an interface for PortFast.
4. Plug a device into that interface.
5. Issue the `show spanning-tree` command within 15 seconds to see the state change immediately to forwarding.
6. Issue the `show spanning-tree` command after another 15 seconds to see the state change to forwarding.

Review Questions

1. What do switches do when a frame with a new source and destination MAC address are received?
2. What is the purpose of Spanning-Tree protocol?

3. Why would you use PortFast with BPDU Guard?
4. How can you restrict the number of MAC addresses on a port?
5. When is it appropriate to run a switch interface in half-duplex versus full-duplex?

Exam Questions

1. What two components make up a Bridge ID? (Choose 2.)

   - ❍ **A.** IP address
   - ❍ **B.** Port priority
   - ❍ **C.** MAC address
   - ❍ **D.** Bridge priority

2. Considering the following output:

```
Switch>show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     000c.418f.6542
             Cost        19
             Port        23 (FastEthernet0/23)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000d.65d0.4e00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/23           Root FWD 19        128.23   P2p
```

   Which of the following are false?

   - ❍ **A.** This switch is the root bridge.
   - ❍ **B.** The forward delay times have been changed.
   - ❍ **C.** The max age timer has been changed.
   - ❍ **D.** The priority has been changed.

3. Given the following output:

```
Switch>show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     000c.418f.6542
             Cost        19
             Port        23 (FastEthernet0/23)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
…Ouput Omitted…
```

What speed is the interface?

- ❍ **A.** 10Mbps
- ❍ **B.** 1Gbps
- ❍ **C.** 10Gbps
- ❍ **D.** 100Mbps

4. Which of the following can be determined from the following output?

```
Switch>show spanning-tree
…Output Ommitted…
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/5            Root LRN 19        128.5   P2p
```

- ❍ **A.** This port has the slowest connection back to the root bridge.
- ❍ **B.** The port priority has been administratively changed.
- ❍ **C.** This interface is learning MAC addresses.
- ❍ **D.** Data is being forwarded.

5. Based upon Figure 8.13, which of the following STP roles will Switch A and Switch D have on their shared link? (Choose 2.)

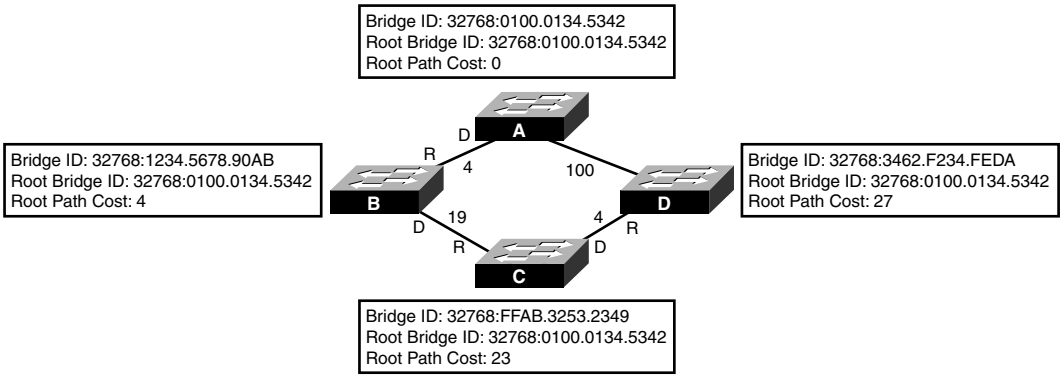


FIGURE 8.13 STP topology exhibit.

- ❍ **A.** Switch A will have a root port.
- ❍ **B.** Switch D will have a designated port.
- ❍ **C.** Switch D will have a blocking port.
- ❍ **D.** Switch A will have a designated port.

6. Which frame transmission method is latency varying?

- ❍ **A.** Store-and-forward
- ❍ **B.** Cut-through
- ❍ **C.** Fragment-free
- ❍ **D.** All of the above

7. Why is the following output false?

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
…Output Omitted…
   1    0300.3E9E.07E9    DYNAMIC     Fa0/3
   1    FFFF.FFFF.FFFF    DYNAMIC     Fa0/1
   1    0300.3E3E.531A    DYNAMIC     Fa0/3
```

- ❍ **A.** There are no static MAC address entries.
- ❍ **B.** There cannot be two MAC addresses learned on the same interface.
- ❍ **C.** There are no multicast entries shown.
- ❍ **D.** A broadcast address should not be present in the CAM table.

8. Which of the following is not a difference between bridges and switches?

- ❍ **A.** Switches are faster.
- ❍ **B.** Switches use ASIC hardware.
- ❍ **C.** Bridges cannot make as many collision domains as most Catalyst switches.
- ❍ **D.** Bridges use the source MAC address to build their forwarding tables.

9. You connected your switches together with a crossover cable. What would be a possible reason for a switching loop to occur?

- ❍ **A.** Because STP is disabled by default, you need to enable it on both switches.
- ❍ **B.** You configured one of the interfaces for PortFast.
- ❍ **C.** You need to use a straight-through cable.
- ❍ **D.** The forward delay timers were set to 15 seconds.

10. You just connected your interface to a hub. Which of the following must be true?

- ❍ **A.** Your speed must be 10Mbps.
- ❍ **B.** Your duplex must be full.
- ❍ **C.** Your duplex must be half.
- ❍ **D.** CSMA/CD must be disabled.

Answers to Review Questions

1. When a switch receives an ethernet frame that contains an unknown source MAC address, it associates that MAC address with the receiving interface in the CAM table. When the switch receives an ethernet frame with an unknown unicast destination MAC address, the switch floods that frame out every port except the one in which it was received.
2. Spanning-Tree protocol eliminates switching loops in environments when multiple switches are connected in a redundant design.
3. PortFast is a Cisco-proprietary enhancement to STP that enables a switchport to bypass the Listening and Learning STP states for end-devices such as workstations and servers. BPDU Guard protects PortFast interfaces from switching loops by disabling an interface if a BPDU is received from another switch.
4. Port security will enable you to limit the amount of MAC addresses that are learned on an interface. When the number of MAC addresses are exceeded, a violation occurs and the switchport becomes disabled.
5. When you connect to a hub, collision detection must be enabled; thus, you must run the interface as half duplex. Full-duplex interfaces have collision detection disabled and can only be enabled when the switch port is connected to another switch or an end-device.

Answers to Exam Questions

1. **C,D.** The Bridge ID comprises the bridge priority plus the MAC address of the switch. Answer A is incorrect because Layer 2 switches do not use IP addresses for Bridge IDs. Answer B is incorrect because the port priority is used as a tiebreaker only when determining the root or designated ports.
2. **A.** The output displays the Root Bridge ID with a different MAC address than the local switch. So, this switch is not the root bridge. The timers and priority are all still their default values. B is incorrect because the forward delay timers are at their default value of 15 seconds. Answer C is incorrect because the max age timer is at its default value of 20 seconds. D is incorrect because the switch's priority is at its default value of 32768.
3. **D.** A port cost of 19 is 100Mbps. Answers A, B, and C are incorrect because 10Gbps has a port cost of 2, 1Gbps has a port cost of 4, and 10Mbps has a port cost of 100.
4. **C.** Because the interface is in the learning state, it is beginning to learn the MAC addresses on that interface. Answer A is incorrect because the port is the root port, indicating that it is the fastest back to the root bridge. Answer B is incorrect because the port priority has not changed from its default value of 128. Answer D is false because the port is in the learning state; it still is not able to forward traffic.

5. **C, D.** Switch A has the fastest way back to the root (itself) on that segment, so it will be designated. Because Switch D's interface is not a root or a designated port, it must be blocking. Answer A is incorrect because only non-root switches and bridges have root ports. Answer B is incorrect because Answer D has the slowest path back to the root for that particular segment.

6. **A.**Only the store-and-forward are latency varying because they have to buffer frames of different sizes. Answers B, C, and D are incorrect because cut-through looks at only the destination MAC address, and fragment-free looks at the first 64 bytes, so their latency will not vary.

7. **D.** The source MAC address in an ethernet frame should not be a broadcast (only destination addresses), so a switch should never have that entry in its CAM table. Answer A is insignificant because static entries are not mandatory. Answer B is incorrect because a switch can learn multiple MAC addresses on a single interface. Answer C is incorrect because multicast addresses should not be present in a CAM table by default.

8. **D.** Both bridges and switches use the source MAC address to build their forwarding table. Answers A and B are differences because the ASIC hardware enables faster switching. Answer C is a difference because switches can have more ports (thus more collision domains) than bridges.

9. **B.** When PortFast is enabled, you must not connect a switch, bridge, or hub to that interface or loops may occur. Answer A is false because STP is enabled by default. Answer C is incorrect because you must use crossover cables when connecting two switches together. Answer D is incorrect because the forward delay timers are set to 15 seconds by default.

10. **C.** When connecting to a hub, you have to be able to detect collisions, thus you must be running half-duplex. It does not matter what speed, so Answer A is incorrect. Answers B and D are incorrect because setting the port to full duplex disables CSMA/CD.

Suggested Readings and Resources

1. Barnes, David and Sakandar, Basir. *Cisco LAN Switching Fundamentals.* Cisco Press, 2004.

2. Castelli, Matthew J. *LAN Switching first-step*, Cisco Press, 2004.

3. Perlman, Radia. *Interconnections: Bridges and Routers*. Addison-Wesley, 1992.

4. "Spinning-Tree Protocol," www.cisco.com.

CHAPTER NINE

9 Virtual LANs

Objectives

This chapter covers the following Cisco-specified objective for the "Technology," "Implementation and Operation," "Planning and Designing," and "Troubleshooting" sections of the CCNA exam:

Configure a switch with VLANS and inter-switch communication

Perform LAN and VLAN troubleshooting

Customize a switch configuration to meet specified network requirements

- VLAN, VTP, and trunk configuration are a multi-step process, which entails a new configuration mode called the vlan database.
- With the show commands, you can determine any misconfiguration or malfunction in a VLAN internetwork.
- With basic switch layouts, there is typically little configuration to be completed. With VLANs and VTP, the configuration requires planning to ensure that the configuration is customized to meet the network design and requirements.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- Complete the Challenge Exercises and the Exercises at the end of the chapter. The exercises will solidify the concepts that you have learned in the previous sections.
- Complete the Exam Questions at the end of the chapter. They are designed to simulate the type of questions you will be asked in the CCNA exam.

Introduction

One of the underlying problems with Layer 2 switches is that excessive broadcast and multicast traffic can affect other devices in a switched network because bridges and switches flood these types of messages. If you are a receiver of all this excessive traffic, you have to waste processing utilization and endure wasted bandwidth even if those devices are not in your department. This chapter explores how VLANs solve your broadcast concerns by segmenting broadcast domains at Layer 2 and how they affect your switched network design.

Overview of VLANs

In your company, you may have several departments connected to the same Layer 2 switch or switched network. Quite often, departments may be running applications and protocols that are unique to users within their own group. Unfortunately, if this traffic consists of multicasts and broadcasts (or unknown unicasts, for that matter), that traffic hits all users connected to that switched network.

For instance, imagine that the Not-So-Human Resources department is running a developed program that helps them track employee lunch break times. Unfortunately, this traffic relies heavily on broadcasts to communicate with other applications being used by personnel in that department. The broadcast and multicast traffic from the Not-So-Human Resources department continues to be flooded out to everyone else in the network because they are all connected to the same switched network. Because this is the only department that uses this software, ideally it would be convenient to separate the Not-So-Human Resources group into their own separate switched LAN so their traffic doesn't affect any other department.

To this point, the only way you could segment this network into smaller broadcast domains is by using a router because routers do not forward broadcasts or multicasts by default. The problem with this solution is that routers can be expensive, considering you need an interface for each department to keep the traffic separate. In addition, because routers have to process all the way into the Layer 3 information of a packet before sending the traffic to a different segment, throughput is considerably slower than that of a switch. Not to mention, if you have users within departments physically dispersed all throughout your network, the broadcast and multicast traffic would never reach them because the router does not forward them onto other interfaces.

The answer to all these problems lies within the magic of virtual LANs (VLANs). VLANs enable you to segment broadcast domains at Layer 2 without a router. Each VLAN created in a switch represents a logical grouping of devices into their own broadcast domain. Thus, each department can have its own VLAN that separates traffic from one department from that of other departments. In fact, devices in one VLAN cannot communicate with other devices in another VLAN, even if those devices are plugged into the same switch. What's more, VLANs

can span multiple switches, so the geographic location of the devices is no longer a limiting factor. As members of a specific department are added or moved, you simply need to assign their switch interface to the department's VLAN.

What is also remarkable about VLANs is that because each VLAN represents a broadcast domain in which devices can communicate only with other devices in that same VLAN, there must be a separate instance of Spanning Tree Protocol (STP) running for each VLAN. In other words, if you have 20 VLANs running in your switched network, you will have 20 instances of STP running, each with its own root bridge. It is for this very reason that the configuration for the STP priority (discussed in Chapter 8, "Bridging and Switching Operations") required that the VLAN be specified in the command syntax.

EXAM ALERT

Unless VLANs are specifically mentioned in an exam question or answer choices, routers segment broadcast domains and switches segment collision domains.

VLAN Membership Methods

After the VLANs are created, they have to be associated with the users or departments connected to the switches. The most common way to associate VLANs is statically on a port-by-port basis. When the VLAN is associated with the switch port, it is referred to as an *access port*. When a single VLAN is assigned on the interface, traffic is sent to and received by only devices connected to interfaces with the same VLAN.

For instance, consider the typical single-switch VLAN configuration exhibited in Figure 9.1. All these switches are access ports that have a single VLAN assigned to them. On Fast Ethernet interfaces 0/1 and 0/3, they are assigned to VLAN 1. Our Not-So-Human Resources VLAN (VLAN 3) has been assigned to Fast Ethernet interfaces 0/2, 0/4, and 0/5. The devices connected to these interfaces can communicate only with other interfaces that also contain that VLAN. So in the example, the printer and the computer on the right can communicate with each other and the computer connected to interface Fast Ethernet 0/2. Even though they are connected to the same switch, these devices cannot communicate with the computers connected to interfaces assigned to VLAN 1 because they are in a completely different broadcast domain.

An alternative to static VLANs is to have the VLANs dynamically associated with the frames entering a switch. To achieve this, you must configure a VLAN Membership Policy Server (VMPS). The VMPS is a device, such as a server or even a high-end Catalyst switch, that has an association of every MAC address with a VLAN. When the frame enters a port, the switch acts as a client and queries the VMPS for the VLAN assigned to that MAC. This is appealing because you don't have to configure VLANs on every interface; however, it does require a good deal of initial setup on the actual server.

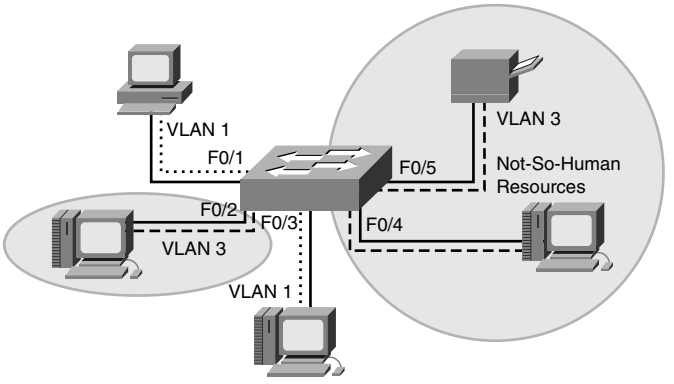


FIGURE 9.1 Single-switch VLAN scenario.

The Management VLAN

Conveniently enough, your switch is already configured with a default VLAN that is used for management on access ports. This is used for a management communication channel because the IP address, CDP, and VTP (discussed later in this chapter) all exist in the management VLAN for ethernet, VLAN 1. This VLAN is created by default in all Cisco Catalyst switches and assigned to all interfaces. Because it is applied to all switch ports, it still holds true that all devices connected to a switch are in the same broadcast domain.

Recall from Chapter 7, "Basic Cisco Configurations," that to assign a management IP address to a switch, you configure the IP on interface VLAN 1. This means that your management workstation must have access to VLAN 1 to remotely manage the Catalyst switch. If you change the VLAN on the port in which your management station or your router (if managing it remotely) is connected, you lose the ability to manage the switch with Telnet, SSH, HTTP, or SNMP.

Configuring and Verifying VLANs

Objective:

Configure a switch with VLANS and inter-switch communication

Perform LAN and VLAN troubleshooting

Customize a switch configuration to meet specified network requirements

All interfaces are already assigned to VLAN 1. To create smaller broadcast domains in your switch, you must create those VLANs for each department you want to segment and assign

them to their respective interfaces. Specifically, the configuration steps for VLANs are as follows:

1. Create the VLAN, using a number between 2 and 1001.
2. Name the VLAN. If you do not assign it a name, it uses VLAN*xxxx*, where *xxxx* is the VLAN number.
3. Assign it to a switch port.

EXAM ALERT

Know the three steps involved in configuring VLANs.

VLAN-specific configurations are permanently stored in NVRAM in a special file called the VLAN database. To configure VLAN information, you must enter a special configuration mode that interacts directly with the VLAN database. Because this is a special configuration location, any configurations in the VLAN database are not displayed in the startup-config or the running-config. In addition, unlike configurations in the running-config, VLAN database configurations are not applied until you exit the VLAN database configuration mode or type the `apply` command.

From Privileged EXEC, you enter the VLAN database by typing the `vlan database` command. The prompt changes to signify that you have entered the VLAN database as shown in the following output:

```
Switch#vlan database
Switch(vlan)#
```

Here, you can create all the VLANs that you want to create for your switched network by using the `vlan` command as illustrated here:

```
Switch(vlan)#vlan 3 name NSHR
VLAN 3 added:
    Name: NSHR
Switch(vlan)#vlan 4
VLAN 4 added:
    Name: VLAN0004
Switch(vlan)#exit
APPLY completed.
Switch#
```

Notice in the second VLAN entry that a specific name is not assigned to VLAN 4. Because there is no name for this VLAN, the Cisco IOS automatically assigns the name VLAN0004. If you need to change a specific VLAN configuration, you just need to re-type the command

and it overwrites the previous command. After the VLAN configurations are completed, they are applied as soon as you exit the VLAN database configuration mode back to Privileged EXEC.

A VLAN is useful only if it is assigned to an interface. To statically assign the VLANs to a switch port, you must navigate to the interface and use the `switchport access vlan` command as demonstrated here:

```
Switch(config)#interface FastEthernet 0/2
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/7
Switch(config-if)#switchport access vlan 4
```

EXAM ALERT

Be prepared to configure VLANs in the VLAN database and assign them to an interface.

To verify your VLAN configuration, use the `show vlan` command to observe the VLANs that you created and the interfaces to which they are applied, as demonstrated in Figure 9.2.

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2
3    NSHR                             active    Fa0/2
4    VLAN0004                         active    Fa0/7
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    srb      0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

FIGURE 9.2 `show vlan` output.

Alternate VLAN Configuration Method

The VLAN database is the most prominent means of configuring VLANs in the switch; however, it is possible to configure VLANs from global configuration as well. To navigate to this configuration mode, you type the command `vlan` followed by the VLAN number you want to create. At this point, the prompt changes to `Switch(config-vlan)#`, signifying that you are in the VLAN configuration mode. As before, these VLAN configurations are stored in the VLAN database and are not displayed in the running or startup configs.

Here is a similar VLAN configuration mode output as used in the VLAN database configuration earlier in this section:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 3
Switch(config-vlan)#name NSHR
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#exit
Switch(config)#
```

VLAN Trunking

One of the most remarkable features of VLANs is that they can span multiple interconnected switches. VLAN traffic is carried from switch to switch over interfaces called *trunks*. These trunk links must be at least 100Mbps because the traffic must carry all the VLAN traffic from the access ports.

Just as access ports have a single VLAN assigned to them, trunk ports essentially have all VLANs assigned to them. As frames traverse a trunk link, the VLAN identifier is added to the ethernet frame. The receiving switch uses the VLAN identifier and sends the frames out only the access ports that have that VLAN assigned to them. As the frame is sent out the interface, the VLAN identifier is removed, which gives the illusion to the end devices that the entire process is transparent.

EXAM ALERT

Remember that a trunk carries traffic for all the VLANs that are present on the switch by default.

NOTE

All VLAN traffic traverses a trunk link by default; however, it is possible to configure a trunk link to allow only traffic from certain VLANs.

Similar to VLANs in a single switch, traffic is contained to only those devices that are members of the same VLAN. For example, Figure 9.3 displays a typical scenario in which VLANs span multiple switches over a trunk link. Tagged frames from VLANs 1 and 3 are multiplexed (multiple messages combined over a single channel) over the trunk between the switches. However, traffic from VLAN 3 goes out to only those access interfaces that have VLAN 3 assigned to them; likewise, traffic from VLAN 1 is passed out only to the ports with VLAN 1 assigned.

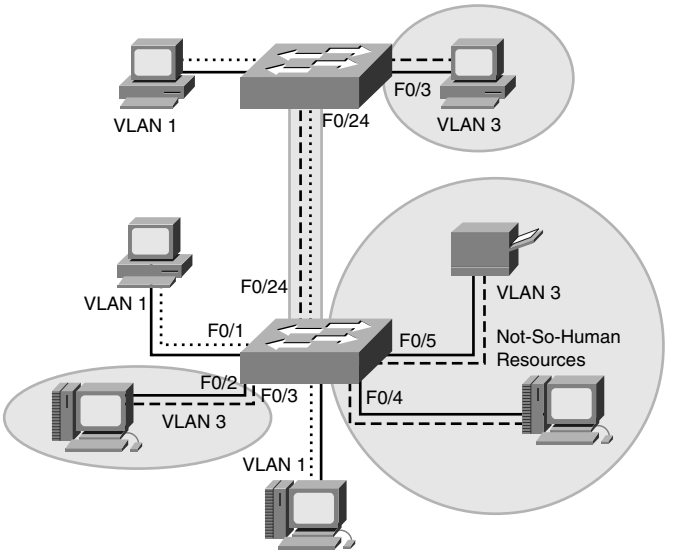


FIGURE 9.3 Multiple-switch VLAN scenario.

EXAM ALERT

Be prepared to identify which devices can communicate with each other given a VLAN configuration in one or several switches.

ISL Trunks

The VLAN identification is added to Layer 2 ethernet frames differently, depending on the type of trunk that is configured. Cisco's proprietary method of adding VLAN IDs to an ethernet frame is called Inter Switch Link (ISL). ISL trunking entails the original ethernet frame being encapsulated by ASIC chips with the VLAN information. The ISL encapsulation has a 26-byte header and an additional 4-byte CRC trailer at the end. Because an additional 30 bytes are added to the ethernet frame, the size of the frame can exceed a typical ethernet frame size of 1518 bytes. If the interface isn't configured as an ISL trunk, it drops the giant frame because it violates the MTU limit of a typical ethernet frame. For this reason, ISL requires a direct point-to-point (no intermediate devices) trunk connection between the switches.

EXAM ALERT

Remember that ISL links encapsulate the ethernet frame with a 26-byte header and a 4-byte CRC, which causes a frame to exceed a standard ethernet MTU.

802.1q Trunks

The IEEE created its own standard VLAN tagging method standardized as 802.1q. 802.1q differs from ISL because the VLAN ID is not encapsulated, but actually inserted in the originally ethernet frame. The VLAN identifier is contained within the four extra bytes inserted in the ethernet frame after the source address. Because the original frame size is manipulated when these four bytes are added to the frame, a new CRC must be calculated for the original ethernet Frame Check Sequence (FCS) field. Because only four bytes are added to the ethernet frame, these frames are known as baby giant frames and may be passed by other intermediary Layer 2 devices that are not configured as a trunk.

Native VLANs

Another unique feature of 802.1q trunks is the concept of a native VLAN. Traffic originating from access ports that shares the same VLAN as the trunk's native VLAN goes untagged over the trunk link. Similarly, any untagged frame that is received on an 802.1q trunk port is considered destined for the native VLAN assigned to the trunk port. For this reason, it is imperative that each side of the IEEE 802.1q link be configured with the same native VLAN, or the traffic from one VLAN leaks into another VLAN as illustrated in Figure 9.4. By default, the native VLAN for trunk ports is the same as the management VLAN, VLAN 1.

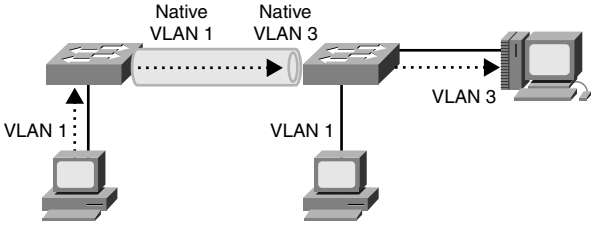


FIGURE 9.4 Native VLAN leakage.

Configuring and Verifying ISL and 802.1Q Trunks

Objective:

Configure a switch with VLANS and inter-switch communication

Perform LAN and VLAN troubleshooting

Customize a switch configuration to meet specified network requirements

The first step to configuring a trunk link is deciding which type of trunk you want to use. For instance, if you are connecting to a non-Cisco switch, you have to use a standard trunk VLAN

tagging method such as IEEE 802.1q. In addition, certain models of Cisco switches (such as the Catalyst 2950) support only 802.1q trunking, so make sure you research the capabilities of your switch model before configuring the interfaces.

To configure a trunk port, navigate to the interface that is connected to the other switch. On models that support ISL and 802.1q trunking, you must first specify which VLAN tagging you want to use with the `switchport trunk encapsulation` command, as shown here:

```
Switch(config)#interface FastEthernet 0/24
Switch(config-if)#switchport trunk encapsulation dot1q
```

Notice the syntax starts with `switchport trunk` instead of `switchport access` (from the VLAN configurations) because this interface is being configured as a trunk to carry all VLANs.

With the trunk encapsulation configured, you are ready to enable the interface to begin forwarding all VLAN traffic. The port, however, is still operating as an access port until you specifically configure the interface to switch to trunking mode. To set this interface into a permanent trunking state, you must also type the following command:

```
Switch(config-if)#switchport mode trunk
```

EXAM ALERT

Be prepared to configure an interface as a trunk port.

Dynamic Trunking with DTP

Cisco switches can dynamically enable trunking on an interface through the use of a Cisco proprietary protocol called Dynamic Trunking Protocol (DTP). For instance, the default dynamic trunking state is called *desirable*, which actively tries to negotiate trunking as long as the other side of the trunk uses a compatible DTP condition.

The possible trunking modes are as follows:

- **Access**—The port does not trunk because it is an access port with a single VLAN.
- **Trunk**—The port permanently trunks and tries to negotiate the far-end to trunk with DTP.
- **Dynamic Desirable**—The port negotiates to trunk if the other side is set to trunk, desirable, or auto.
- **Dynamic Auto**—The port negotiates to trunk if the other side is set to trunk or desirable.
- **Nonegotiate**—The port permanently trunks, but disables DTP negotiation (for connecting to non-Cisco switches).

To verify the trunk configuration and status, use the `show interface trunk` command:

```
Switch>show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/24      1-4094

Port        Vlans allowed and active in management domain
Fa0/24      1-4

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1-4
```

The output lists the ports that are configured to trunk and the encapsulation and VLANs that are allowed to traverse the trunk (all VLANs by default). In addition, because the interface is now set up as a trunk, you no longer see interface Fast Ethernet 0/24 listed in the `show vlan` output because it is no longer an access port.

EXAM ALERT

If the output of the `show vlan` command is displayed, know that missing interfaces are set up as a VLAN trunk and are not listed.

VLAN Trunking Protocol

Imagine you just configured 50 VLANs in your local switch. If you want to have these VLANs span your 5 switches in your network, you have to configure each switch with those exact VLANs. That is at least 200 more configurations that you have to perform before you can even begin to assign the VLANs to their respective ports.

To minimize the administrative overhead involved in replicating VLAN configurations on the remaining switches in your internetwork, Cisco has created a proprietary protocol called VLAN Trunking Protocol (VTP). With VTP, you have to make the initial VLAN configuration on only a single switch. This switch has a special role to propagate any VLAN revisions (additions, changes, or deletions) to the rest of the switches that want to receive these updates, known collectively as a VTP domain.

VTP Modes

A VTP domain is similar to a large corporation in that there are specific job responsibilities and functions that everyone must perform in accordance to a job role. The switches inside a

VTP domain also have a hierarchy in the roles that they can perform and the responsibilities of the switches that result from that role. These roles are dictated by the VTP mode in which they operate and ultimately define the level of VLAN configuration allowed on the switches and whether the VLAN information is stored and propagated. The three VTP modes in which a switch can operate are server, client, and transparent mode, which are discussed in the following sections.

NOTE

VTP only advertises the VLANs that are configured. It does not advertise the VLAN interface assignments because switches can contain different hardware.

Server Mode

In the corporation analogy, a switch operating in server mode would be considered the CEO of the network. It is responsible for maintaining the VLAN information for the rest of the network by telling everyone else what to do. In server mode, you have complete autonomy and are able to make any additions, deletions, or changes to the VLAN configurations. Because this functionality seems to be a reasonable function of all switches, server is the default VTP mode of all switches.

After you make a revision to the VLAN information in the VLAN database, the changes are propagated across trunk links to other switches in the VTP domain to synchronize their VLAN databases with the server's configuration. Each VTP advertisement from the VTP server contains a revision number in the message. When other switches receive this information, they compare the revision number of the new message to the last revision received. If the information is new (higher revision number), the switches apply those changes to their VLAN configurations. If the revision number is the same as the advertisement, the switches know that they have the latest information and ignore the update. In instances when the revision number advertised is lower than the current one in the database, they send an update to the sender because the sender's information is older than what they contain in their VLAN databases.

Client Mode

Imagine the chaos your company would have if everyone in the organization was the CEO. You would have everybody trying to tell each other what to do and nothing would ultimately get done. At some point, you need to have faithful workers who follow every word that the CEO tells them. In other words, you need yes-men.

The yes-men in the VTP domain are those switches that operate in client mode. Their sole purpose is to take the configuration revision from server switches and incorporate them into their operations. These switches also propagate those changes to other switches to ensure that

the advertisement is heard across the entire VTP domain. Unlike switches in server mode, however, client mode switches do not permanently store their VLAN information in the VLAN database. Thus if switches in client mode reboot, they do not contain any VLAN information until they receive an update from the VTP server.

Because they receive their configuration from the VTP server, switches in VTP client mode cannot add, change, or delete VLANs. In fact, the IOS reports back an error similar to the following:

```
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

This lack of functionality is actually quite useful when new switches are added to an existing VTP domain so they do not accidentally advertise incorrect VLAN information to switches in the VTP domain (assuming their revision number is higher).

Transparent Mode

To round out the corporation analogy, the inevitable third type of worker in large corporations is the disgruntled employee. These employees believe they know how to run the company better than the CEO, so they do things their way. However, to ensure that they keep their jobs, they don't let anyone know about their delusions.

Similarly, switches running in transparent mode also do their own thing in the sense that they are allowed to add, change, and remove VLAN configurations. In addition, they store those VLAN configurations in their VLAN database so they are present when the switch reboots. The key difference between server and transparent mode switches is that transparent mode switches do not advertise their configurations to other switches. In addition, they also do not use any configuration revisions being advertised by server switches. They do, however, send those advertisements out their trunk ports to other switches in case there are client mode switches downstream from them. In other words, the switch is transparent because the advertisements from the server seem to pass right through them.

So why have transparent mode in the first place? Basically, transparent mode enables you to create your own VLAN configurations that are contained within a single switch. This is useful if you have VLANs connected to that switch that are not used by any other switches in the domain.

The obvious follow-up question to this is, "Why use VTP on this switch if it does not listen to the VTP server revisions or advertise its own VLANs?" To answer this question, take a look at the exhibit in Figure 9.5. When the switch in server mode sends its VTP revision to the switch operating in transparent mode, that switch ignores the advertisement and passes it to the client switches below. If the transparent switch did not participate in VTP, it would drop those advertisements from the server and the client switches would never receive the configuration revisions.

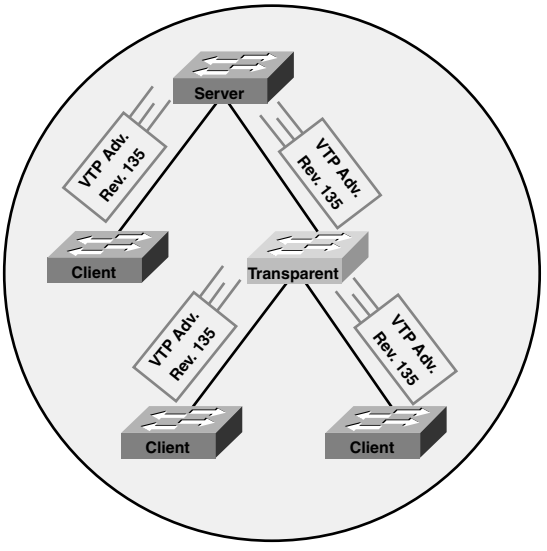


FIGURE 9.5 VTP domain with transparent switch.

EXAM ALERT

Make sure you understand the functions of each VTP role. Also, remember that you must be in either server or transparent mode to make any VLAN configuration changes in a switch.

CAUTION

VTP Revision Mayhem When adding a new switch to an existing VTP domain, it is highly recommended that you put the switch in client mode. If you left your switch in the default server mode, you could possibly have a higher revision number than the existing server of the domain. If you add that switch to the domain and you do not have any VLANs configured, when you advertise that to the rest of the VTP domain, the client and the other server use that configuration because it has a higher number. That would cause all the VLANs to be removed in all switches because your VLAN database does not contain any VLAN configurations.

To reset your revision number, you can either change the name of your VTP domain or set your switch to transparent mode followed by server mode.

VTP Pruning

VLAN traffic is being sent over trunk links to other switches no matter whether or not the VLAN is active on an interface. In other words, if a user connected to VLAN 2 sends a broadcast, that message is replicated to all switches in the domain regardless of whether VLAN 2 is assigned to a switch port. This could consume unnecessary bandwidth on the trunk links connecting the switches.

To minimize the traffic overhead, you can configure VTP pruning on the VTP server of the domain. When enabled, switches advertise to each other which VLANs are active. With this information, the switch can limit VLAN traffic to other switches that do not have the VLAN active on an interface, minimizing the amount of unnecessary traffic that is sent to other switches on the trunk link.

Configuring and Verifying VTP

Similar to the VLAN configurations, VTP is configured in the VLAN database. In this configuration mode, you can easily change the VTP mode of the switch from server to transparent or client mode. In addition, you can define your VTP domain name as well as assign an MD5 password for VTP updates. The domain name (and password if configured) are case sensitive and must match in all switches in the VTP domain or the VTP updates will be ignored from other switches and VTP will not function.

To configure VTP-specific properties, use the `vtp` command followed by the VTP parameter you want to configure. Similar to VLAN configurations in the VLAN database, they are not applied until you exit the VLAN database or type the `apply` command, as illustrated in the following configuration example:

```
Switch#vlan database
Switch(vlan)#vtp transparent
Setting device to VTP TRANSPARENT mode.
Switch(vlan)#vtp domain CCNA
Changing VTP domain name from null to CCNA
Switch(vlan)#vtp password imustmatch
Setting device VLAN database password to imustmatch
Switch(vlan)#apply
APPLY completed.
```

In this configuration, the default server mode was changed to transparent mode. To communicate with other switches in the VTP domain, you have to configure the VTP domain to CCNA as shown in this switch. In addition, the VTP password must also match in all configurations to ensure VTP updates are authenticated from each other.

EXAM ALERT

Be prepared to configure VTP parameters in a switch.

NOTE

Similar to VLAN configurations, VTP can also be configured in Global Configuration.

The `show vtp status` command is a critical command for verifying your VTP configuration. As demonstrated in Figure 9.6, the `show vtp status` command displays the revision number of the VTP updates from the server, the operating mode, domain name, pruning status, and the MD5 digest of the password.

```
Switch>show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Transparent
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x88 0xC0 0x7F 0x02 0xCB 0xE9 0xBA 0xA4
Configuration last modified by 192.168.100.2 at 3-1-93 00:31:16
```

FIGURE 9.6 `show vtp status` output.

EXAM ALERT

Given the output(s) of the `show vtp status` command, be able to identify the operating mode and what functionality the switch has because of that VTP mode. In addition, be able to troubleshoot VTP inconsistencies such as non-matching VTP domain and MD5 passwords.

Challenge

The concepts and configurations are very critical to comprehend for the CCNA exam. The following challenge tests your comprehension of the concepts and configuration of VLANs, trunks, and VTP.

1. How many broadcast domains are present in the switch by default and what VLAN(s) are present?
2. Enter the VLAN database and change your VTP domain to VTPMaster.
3. Create the VTP password for the domain to be allhailme.
4. Change the VTP mode to client.
5. You need to create two separate broadcast domains in your local switch for the ExamCram and the ExamPrep departments. Configure them with VLAN numbers 100 and 200, respectively, and apply the configuration.
6. Why will this fail?
7. Change your VTP mode back to the default, add the VLANs, and exit the VLAN database.
8. Apply VLAN 100 to interface Fast Ethernet 0/1.
9. Apply VLAN 200 to interface Fast Ethernet 0/2.
10. Make Fast Ethernet 0/24 an interface to carry all VLAN traffic to a neighboring switch, using the IEEE standard VLAN tagging.

Challenge Answer

In solving this Challenge the switch is configured, by default, for a single broadcast domain in the management VLAN 1. The configuration for steps 1–4 is as follows:

```
Switch#vlan database
Switch(vlan)#vtp domain VTPMaster
Changing VTP domain name from CCNA to VTPMaster
Switch(vlan)#vtp password allhailme
Setting device VLAN database password to allhailme
Switch(vlan)#vtp client
Setting device to VTP CLIENT mode.
```

Any VLAN creation will fail at this point because you cannot add, change, or delete VLANs in VTP client mode. The remaining configuration steps are demonstrated here:

```
Switch(vlan)#vtp server
Setting device to VTP SERVER mode.
Switch(vlan)#vlan 100 name ExamCram
VLAN 100 added:
    Name: ExamCram
Switch(vlan)#vlan 200 name ExamPrep
VLAN 200 added:
    Name: ExamPrep
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport access vlan 100
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/2
Switch(config-if)#switchport access vlan 200
Switch(config-if)#exit
Switch(config)#interface FastEthernet 0/24
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```

InterVLAN Routing

One of the remarkable features about VLAN segmentation with a Layer 2 switch is that the traffic from one VLAN remains separate from all other VLANs. Quite often, however, devices need to communicate or access services with another device that is in another VLAN. Because the VLANs are in separate networks (broadcast domains), you need a device that is capable of routing in between networks. In other words, you need a router or a Layer 3 switch.

Each broadcast domain that is created in a switch is associated with an IP subnet. Devices in the same VLAN share the same subnet so they can use IP to communicate with each other. Routers and Layer 2 switches route between the logical subnets to allow traffic from one VLAN to reach another VLAN. This is known as interVLAN routing.

Router on a Stick

Objective:

Customize a switch configuration to meet specified network requirements

One method of routing between VLANs is to use a router. Because each VLAN is associated with its own subnet, a router needs to have an interface for each VLAN (IP subnet) so it can route in between them. This can become a costly and unscalable solution if you have a large number of VLANs in your switched network.

The most effective manner of using a router to perform interVLAN routing is something commonly referred to as "router on a stick." The gist behind this solution is to produce a configuration in which the router can see all the VLAN traffic over a single link. In other words, the router trunks to a switch over a single link, hence the term "router on a stick." Despite the router being able to see all the VLAN traffic, however, it still requires interfaces with IP subnets assigned to them to route in between these VLANs. The answer for this is something called *subinterfaces*.

Subinterfaces are virtual interfaces that are created on a single physical interface. When a physical interface is divided into these virtual interfaces, the router still considers them to be directly connected interfaces with subnets assigned to them and can route in between them. To create the subinterfaces, you navigate in the IOS as you would to a physical interface; however, you add a decimal followed by the logical subinterface number. The IOS prompt changes to reflect `Router(config-subif)#`, signifying you are in the subinterface configuration mode, as demonstrated here:

```
Router(config)#interface FastEthernet 0/1.1
Router(config-subif)#
```

The decimal number you assign to an interface does not have to be in any sequential order. In fact, for good design practices, you should use the same number of the VLAN for which you created the subinterface. In addition, because these are logical interfaces, if one subinterface goes down, it does not affect the rest of the subinterfaces. However, if the physical interface happens to go down, then logic follows that all your subinterfaces go down with the ship, so to speak. Additionally, you do not need to enable `no shutdown` on each subinterface; this is required only on the physical interface itself.

After you create a subinterface for a VLAN on your Fast Ethernet or Gigabit interface (remember trunks must be at least 100Mbps), you can assign the IP address to the interface for that VLAN's subnet. This IP address is the default gateway for all the devices in that VLAN because the default gateway is the IP address to which devices send their traffic destined for another network. To assign the VLAN to each subinterface, you must use the `encapsulation` command and signify which method of VLAN tagging you have configured on the trunk, followed by the VLAN assigned to that subinterface.

EXAM ALERT

To use a router-on-a-stick solution for interVLAN routing, you must trunk between the router and the switch. In addition, the interface must be at least Fast Ethernet and contain subinterfaces for each VLAN.

For instance, given a scenario similar to Figure 9.7, you would create a subinterface in the router for each VLAN. The IP address assigned to these interfaces acts at the default gateway for the PCs. When the computer in VLAN 1 wants to send traffic to the computer in VLAN 3, it sends the traffic over the switch trunks to the router that is to route and re-encapsulate the ethernet frame to have a VLAN ID of VLAN 3. When the switches receive the frame, they forward it out of only access ports that have VLAN 3 assigned to it.

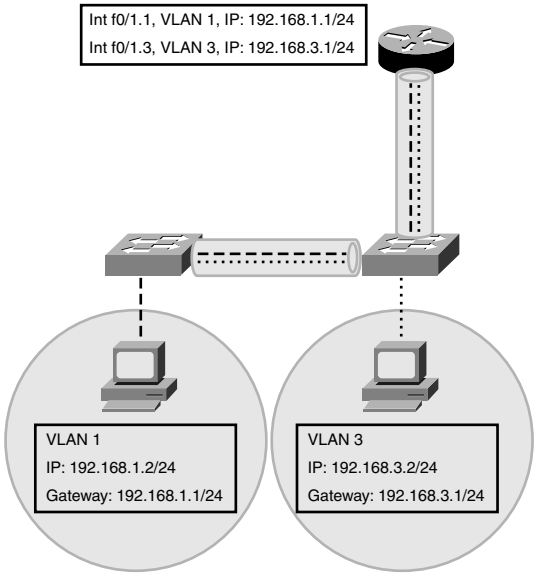


FIGURE 9.7 Router-on-a-stick scenario.

The router configuration for Figure 9.7 would look like the following, assuming you are using ISL trunks:

```
Router(config)#interface FastEthernet 0/1.1
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#encapsulation isl 1
Router(config)#interface FastEthernet 0/1.3
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#encapsulation isl 3
```

NOTE

Refer to Appendix A, "Future Exam Topics," if you wish to learn how to configure interVLAN routing using a Layer 3 switch.

Chapter Summary

VLANs are convenient for segmenting broadcast domains at Layer 2. The departments of an enterprise can be assigned their own logical VLAN to ensure traffic in one VLAN does not affect other VLANs. In fact, VLAN traffic cannot go from one VLAN to another VLAN without the assistance of an external router or a Layer 3 switch.

VLANs can be statically assigned to switch access ports, or a VMPS can be used to assign them dynamically. By default, all interfaces are assigned to the management VLAN, VLAN 1. To configure a VLAN, enter the VLAN database and create the VLAN and name it. After the VLANs are created, you must assign them to your switch ports by using the `switchport access vlan` command.

VLANs can span multiple switches by using ISL or 802.1q trunks. This makes it simple to move users throughout a switched network with no geographic restrictions. ISL is a Cisco proprietary VLAN tagging that encapsulates the original ethernet frame with a 26-byte header and a 4-byte CRC. Because this exceeds a typical frame MTU, the trunk must be point-to-point (directly connected). 802.1q is an IEEE standard of frame tagging that inserts the VLAN ID in the original ethernet frame and calculates a new CRC. 802.1q also uses the concept of native VLANs, which are VLANs that are not tagged as they traverse a trunk. To configure a trunk, you must first define the encapsulation method with the `switchport trunk encapsulation` command, and then set the interface to trunk with the `switchport mode trunk` command.

To minimize the amount of VLAN administration in switches, Cisco created VTP, which entails a VTP server sending advertisements with revision numbers containing the VLANs in the VTP domain. VTP clients use that information from the server; however, they cannot create, modify, or delete any VLANs. Transparent mode does not use the information sent from VTP servers; conversely, they can create, modify, or delete (but not advertise) their VLANs. VTP configuration also transpires in the VLAN database, in which you can switch the switch's operating mode, define the domain name, and assign a VTP password for update authentication.

To allow traffic from one VLAN to another, you must configure interVLAN routing. If you use an external router (router on stick), you must trunk to the interface and configure subinterfaces to route in between the VLANs.

Key Terms

- VLANs
- access ports
- VMPS
- management VLAN
- trunk
- multiplexing
- ISL
- 802.1q
- native VLANs

- DTP
- VTP
- VTP Domains
- server mode
- client mode
- transparent mode
- VTP pruning
- port security
- interVLAN routing
- router on a stick
- subinterfaces

Apply Your Knowledge

Exercises

9.1 Create Your VTP Domain

In this exercise you establish your own VTP domain and ensure that your switch propagates the VLANs you will create in Exercise 9.2.

NOTE

These exercises assumes that you have two Cisco Catalyst switches. As always, if you do not have the equipment, mentally go through the configuration and practice typing the commands as you would if you were configuring the switches.

Estimated Time: 10 minutes

1. Enter the VLAN database.
2. Configure your switch for VTP server mode (default, but for redundancy's sake).
3. Name the VTP domain GoldiLocks (remember domain name is case-sensitive).
4. Create a VTP password for VTP updates to be 3Bears (remember password is case-sensitive).
5. Exit the VLAN database and verify the configuration with the `show vtp status` command.

9.2 VLAN Creation and Assignment

In this exercise you create the VLANs that will be propagated by the VTP domain created in Exercise 9.1 and forwarded by the trunks in Exercise 9.3.

Estimated Time: 15 minutes

1. Enter the VLAN database.
2. Create VLAN 100 with the name 2hot.

3. Create VLAN 200 with the name 2cold.
4. Create VLAN 300 with the name justright.
5. Exit the VLAN database.
6. Assign VLAN 100 to interface Fast Ethernet 0/1.
7. Assign VLAN 200 to interface Fast Ethernet 0/2.
8. Assign VLAN 300 to interface Fast Ethernet 0/3
9. Verify VLAN configuration with the `show vlan` command.

9.3 802.1q Trunking

This exercise enables the VLAN traffic to span multiple switches with IEEE 802.1q trunking.

Estimated Time: 5 minutes

1. Connect the switches together with a cross-over ethernet cable using interface 0/12.
2. Configure Fast Ethernet 0/12 to 802.1q encapsulation.
3. Set the interface mode to trunking.
4. Verify your trunk with the `show interface trunk` command.

9.4 InterVLAN Routing

This exercise enables traffic to be routed from one VLAN to another with an external router.

Estimated Time: 15 minutes

1. Connect the switch to the router's Fast Ethernet interface with a straight-through cable.
2. Configure the switch port to become a 802.1q trunk (see Exercise 9.3).
3. Configure a subinterface for VLAN 100, 200, and 300 (set their encapsulation to dot1q and assign their respective VLANs).
4. Assign an IP address to each subinterface (from different subnets).

Review Questions

1. What are the characteristics of VLANs?
2. What are trunks and how do they work?
3. What is the purpose of VTP?
4. What are the characteristics of the three VTP modes?
5. Why is router-on-a-stick sometimes necessary in switched environments?

Exam Questions

1. Given the following output, which two facts can be determined? (Choose 2.)

```
Switch>show vtp status
VTP Version                     : 2
Configuration Revision          : 45
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xCC 0x69 0x27 0x01 0xC8 0xA8 0x59 0xD7
```

   - ❍ **A.** This switch will save VLAN information into NVRAM.
   - ❍ **B.** This switch will synchronize its VLAN database with updates starting with number 46 or above.
   - ❍ **C.** This switch can add, change, and delete VLANs.
   - ❍ **D.** This switch passes VTP advertisements from the server.

2. Considering the following output:

```
Switch>show vlan

VLAN Name                              Status    Ports
---- --------------------------------- ------ --------
1    default                           active   Fa0/1, Fa0/2, Fa0/3, Fa0/4,
➥ Fa0/5,Fa0/6, Fa0/7, Fa0/8, Fa0/9
2    VLAN0002                          active
100  ExamCram                          active
200  ExamPrep                          active
```

   Which of the following is false?

   - ❍ **A.** Interface Fast Ethernet 0/1–0/9 are in the management domain.
   - ❍ **B.** Interfaces above Fast Ethernet 0/24 could be configured as a trunk.
   - ❍ **C.** Interface Fast Ethernet 0/10 is an access port.
   - ❍ **D.** VLAN 2 was not configured with a custom name.

3. Which of the following VTP modes save their VLAN information to NVRAM? (Choose 2.)

- ❍ **A.** Transport
- ❍ **B.** Client
- ❍ **C.** Server
- ❍ **D.** Transparent

4. Which is not a characteristic of VLANs?

- ❍ **A.** Users can be moved easily because VLANs span multiple switches.
- ❍ **B.** Users can be logically grouped according to their departments.
- ❍ **C.** There is a separate instance of STP for each VLAN.
- ❍ **D.** Broadcasts are not forwarded over trunks.

5. You want to connect your Cisco Catalyst switch to a Nortel switch. Which of the following is true?

- ❍ **A.** 802.1q trunks should be used.
- ❍ **B.** ISL trunks should be used.
- ❍ **C.** VLAN configurations will be accepted by the Nortel switch if it is in VTP client mode.
- ❍ **D.** Cisco is the only switch that can configure VLANs.

6. Which of the following would cause VLAN leakage?

- ❍ **A.** Incorrect ISL configuration.
- ❍ **B.** Native VLAN mismatch.
- ❍ **C.** VTP passwords don't match.
- ❍ **D.** Saggy VLAN diapers.

7. Given the following output from two switches, why are the VLAN databases not synchronized?

```
SwitchA>show vtp status
VTP Version                     : 2
Configuration Revision          : 45
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 10
VTP Operating Mode              : Server
VTP Domain Name                 : Examprep
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xCC 0x69 0x27 0x01 0xC8 0xA8 0x59 0xD7

SwitchB>show vtp status
VTP Version                     : 2
Configuration Revision          : 45
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : ExamPrep
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xCC 0x69 0x27 0x01 0xC8 0xA8 0x59 0xD7
```

- ❍ **A.** VTP versions are incorrect.
- ❍ **B.** Passwords do not match.
- ❍ **C.** Both devices should be set to server mode.
- ❍ **D.** VTP domains do not match.

8. What can be determined from the following output?

```
Switch>show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/24      1-4094

Port        Vlans allowed and active in management domain
Fa0/24      1-4,100,200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1-4,100,200
```

   - ❍ **A.** The trunk is proprietary to Cisco.
   - ❍ **B.** Ethernet frames from VLAN 1 will not be tagged over the trunk.
   - ❍ **C.** This trunk will create giant frames that will be dropped by non-Cisco devices.
   - ❍ **D.** Ethernet frames are being encapsulated with a 30-byte VLAN ID.

9. How do you associate VLANs to an interface in a router-on-a-stick configuration?

   - ❍ **A.** By creating a VLAN interface in the switch.
   - ❍ **B.** By creating the subinterface number to match the VLAN.
   - ❍ **C.** By having a separate physical interface for each VLAN.
   - ❍ **D.** By using the **`encapsulation`** command.

10. Which of the following is not a characteristic of router-on-a-stick?

   - ❍ **A.** The interface must be 10Mbps or higher.
   - ❍ **B.** The link must be a trunk.
   - ❍ **C.** Subinterfaces are used to route in between the VLANs.
   - ❍ **D.** The IP address assigned is used as the VLAN's default gateway.

Answers to Review Questions

1. VLANs are created in switches to segment broadcast domains at Layer 2. Departments in your organization can be assigned their own VLAN, which provides a logical segmentation in which traffic from one department does not interfere with that of another department. VLANs can span multiple switches, which simplifies administration when users need to move throughout the switched network.

2. Trunks are used to carry VLAN traffic from one switch to another switch. Frames are tagged with a VLAN identifier as they traverse the trunk link and are removed on the receiving switch. ISL is a Cisco proprietary method of trunking in which the original frame is encapsulated with a 26-byte header and a 4-byte CRC. IEEE 802.1q trunks insert a 4-byte VLAN identifier inside the ethernet frame.

3. VTP is a convenient Cisco proprietary Layer 2 protocol that enables switches to advertise VLAN configuration information to other switches in a VTP domain.

4. Server mode is the default VTP mode in which VTP advertisements are sent to other switches in the VTP domain. VLAN configurations in Server mode are saved to NVRAM. Client mode processes and forwards VTP advertisements from the VTP Server. You cannot change any VLAN configurations or save the VLAN configuration in Client mode. Transparent mode also forwards VTP advertisements from the VTP Server; however, switches in Transparent mode do not process the VTP advertisements. In Transparent mode, you can configure VLANs and save them to NVRAM; however, these local VLANs are not advertised to other switches in the VTP domain.

5. Router-on-a-stick is used when you want to allow traffic from one VLAN to be routed into another VLAN. Router-on-a-stick requires a switch to trunk to a Layer 3 router. The router uses subinterfaces to logically separate the VLANs into virtual interfaces in which the router can route in between.

Answers to Exam Questions

1. **B, D.** Because this switch is operating in client mode, it synchronizes with updates received from the VTP server as long as the revision number is greater than its current revision number. It passes the advertisements from the VTP server to other switches in the VTP domain. Answer A is incorrect because client mode switches do not save their VLAN information into NVRAM. Answer C is incorrect because you cannot add, change, or delete VLANs in client mode.

2. **C.** Interface Fast Ethernet 0/10 could not be an access port, or it would be included in the list of interfaces assigned to a VLAN. Answer A is true because they are all assigned to VLAN 1. Answer B is true because the interface number does not show up in the `show vlan` output if it is a trunk. D is true because the VLAN name is VLAN0002, which is the default naming convention the IOS uses when a name isn't configured for a specific VLAN.

3. **C, D.** Server and transparent VTP modes are the only modes that save their VLAN configuration to NVRAM. Answer A is incorrect because Transport is not a VTP mode. Answer B is incorrect because switches operating in Client mode do not save their VLAN information in NVRAM.

4. **D.** Broadcasts will still be forwarded over trunks to other switches in the same VLAN. Broadcasts in one VLAN, however, do not affect other VLANs. Answers A, B, and C are all characteristics that apply to VLANS.

5. **A.** Because you are connecting to a Nortel switch, you must use a standard method of trunking (IEEE 802.1q). ISL and VTP are Cisco proprietary functions. Answer B is incorrect because ISL is a Cisco proprietary trunk encapsulation. Answer C is incorrect because VTP is a Cisco proprietary protocol. Answer D is false because other switch manufacturers support VLAN configurations.

6. **B.** VLAN leakage occurs when there is a VLAN mismatch on a trunk link with 802.1q. Answer A is incorrect because ISL does not use native VLANs. Answer C is incorrect because VTP does not affect VLAN leakage. Answer D is incorrect because switches don't wear diapers.

7. **D.** The domain names are case sensitive. If they do not match, the switches cannot synchronize their VLAN database information. Answer A is incorrect because both switches are operating in the same VPT version. Based upon the fact that the MD5 digest of the VTP password is identical, Answer B is incorrect. Answer C is incorrect because both switches do not need to be in server mode in order for the switches to exchange VLAN configurations via VTP.

8. **B.** Because the trunk is 802.1q with a native VLAN of 1, ethernet frames originating from VLAN 1 going over this trunk are not tagged. Answers A, C, and D are incorrect because they are characteristics of ISL.

9. **D.** The `encapsulation` command is used to assign VLANs to a subinterface. Answer A is incorrect because SVIs are in Layer 3 switches, not external routers. Answer B is a good design practice, but does not assign the VLANs to the subinterface. Answer C is incorrect because router-on-a-stick is over one interface.

10. **A.** Because the interface must be a trunk, the speed of the link should be 100Mbps or greater. Answers B, C, and D are all characteristics of router on a stick.

Suggested Readings and Resources

1. Barnes, David and Sakandar, Basir. *Cisco LAN Switching Fundamentals.* Cisco Press, 2004.

2. Castelli, Matthew J. *LAN Switching first-step.* Cisco Press, 2004.

3. Perlman, Radia. *Interconnections: Bridges and Routers*. Addison-Wesley, 1992.

4. "Virtual Local Area Networks," www.firewall.cx.

5. "Configuring VLANs," Catalyst 3550 Configuration Guide on www.cisco.com.

CHAPTER 10

Introduction to Routing and Routing Protocols

Objectives

This chapter covers the following Cisco-specified objective for the "Technology," "Implementation and Operation," "Planning and Designing," and "Troubleshooting" sections of the Cisco Certified Network Associate exam:

Evaluate the characteristics of routing protocols

Select an appropriate routing protocol based on user requirements

Design an IP addressing scheme to support classful, classless, and private addressing to meet design requirements

- Each routing protocol is unique, based upon characteristics such as the contents of their routing updates, the frequency of their routing updates, and their capability to converge in the face of a topology change.
- Because each routing protocol has varying characteristics, you must choose the right protocol based upon the users' requirements and the existing infrastructure and design.
- With classless routing protocols, you can design a network assigning the appropriate number of IP addresses required for each segment, based upon your design requirements.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- Because routing is a method of passing IP packets along to Layer 3 forwarding devices, take the perspective of the routing devices as it receives the packet and try to determine the information required in order to send it on to the next forwarding device.
- Complete the Challenge Exercises and the Exercises at the end of the chapter. The exercises will solidify the concepts that you have learned in the previous sections.
- This chapter involves several mathematical challenges that are based upon the subnetting foundations learned in Chapter 4. If necessary, review those concepts before tackling this chapter.
- Complete the Exam Questions at the end of the chapter. They are designed to simulate the type of questions you will be asked in the CCNA exam.

Introduction

Having exhausted the functionality and features of Layer 2, it is time to step up one more rung of the OSI model and delve into Layer 3, the Network layer. Recall that Layer 3 is responsible for determining the best path to a network, using logical addressing such as IP addresses. This chapter discusses the fundamentals of how Layer 3 devices such as routers and Layer 3 switches develop the routing logic to determine where to forward IP packets to reach a destination network.

The Default Gateway

To fully comprehend the routing of data, it helps to start where much of the data in a network originates: the computer. As application data is sent down the protocol stack, the source and destination IP address is added to the IP header. If the destination IP address is located on the same IP subnet as that on which the computer is, the computer adds the destination MAC address of that device at Layer 2 and sends it on the wire.

In instances where the destination IP address is on a remote network, it must send that traffic to a router on its segment that can forward the packet toward the destination network. Although you are going to forward traffic to this default gateway, the destination IP address remains unchanged. However, at Layer 2, the destination MAC address of the ethernet frame reflects the default gateway's MAC address because this is the forwarding device on the local data link segment.

In the example illustrated in Figure 10.1, the PC is sending traffic to the server on the remote 10.1.34.0 network. The source IP address and MAC address are those matching the PC. On the other hand, the Layer 3 destination IP address of the IP packet reflects the IP address of the server (10.1.34.101). Because the destination IP address does not exist on the PC's local subnet of 192.168.1.0, the PC encapsulates the router's Ethernet 0 MAC at Layer 2 because that is the configured default gateway for this segment. The switch in this scenario is operating as only a Layer 2 switch. Thus, despite having an IP address for management, this is not the default gateway for this segment because it is only forwarding frames at Layer 2.

EXAM ALERT

Despite having IP addresses assigned to switches for management purposes, Layer 2 switches do not act as the default gateway. If the exam does not mention the switch is Layer 2 or Layer 3, assume it is a Layer 2 switch.

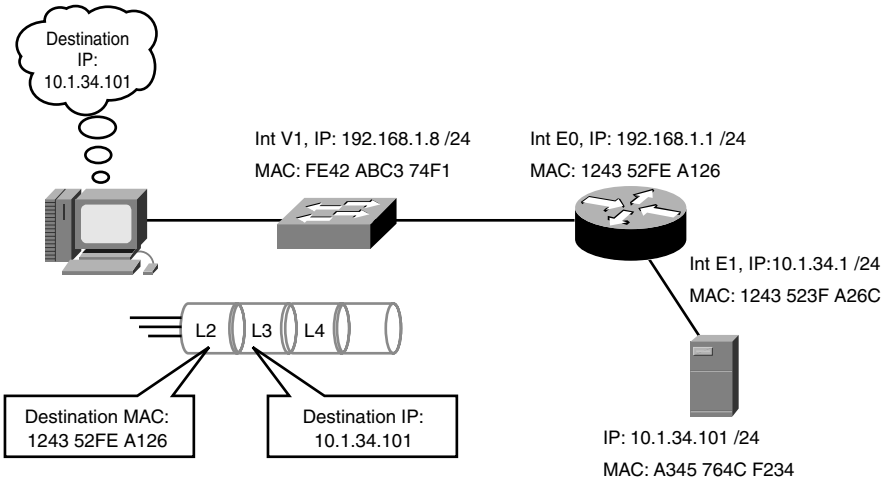


FIGURE 10.1 Default gateway example.

When the router receives the frame addresses to its interface MAC, it processes the Layer 3 information and consults its routing logic to determine whether it knows where to route the packet. Because the destination network is attached to the router, it knows to send the packet out its Ethernet 1 interface. A new ethernet frame using its Ethernet 1 MAC address (1243 523F A26C) for the source MAC address and the server's MAC address (A345 764C F234) as the destination MAC are added to the original IP data as it is sent out to the destination segment.

EXAM ALERT

Be comfortable identifying what the source and destination IP address and MAC address should be at any point of the data delivery.

Routing Sources

Routers are methodical, tactless devices in that they do not necessarily care about the individual IP addresses that exist on a subnet. Their sole obsession is to maintain their routing logic by keeping track of the networks that exist and which interfaces to use to send the traffic if an IP packet is destined for that network. By using routing devices to relay packets out of their interfaces to other forwarding devices or the destination network, the IP packet eventually reaches the destination.

At the heart of the routing logic for Layer 3 devices is the routing table. This table, located in volatile RAM, contains a mapping of all the best routes to networks that the router is aware

of and the interfaces to exit to reach those networks. So how is the router aware of these networks? Generally, there are three routing sources that can feed the routing table with this information:

- **Connected Interfaces**—As soon as you assign an IP address to a working (up/line protocol up) interface, the router associates the entire subnet of the interface's IP address in the routing table.
- **Static Routes**—These are manual entries that an administrator enters into the configuration to specify the destination network and the next hop (router along the destination path).
- **Routing Protocols**—Protocols exchanged between routing devices to dynamically advertise networks.

Connected interfaces remain in the routing tables as long as the interface is active and has a valid IP address assigned to it. Static routes remain in the table as long as you do not remove the static route configuration and the next hop is valid (interface to next hop is up). Networks learned from dynamic routing protocols remain in the routing table as long as the next hop is valid and the routing devices do not stop hearing the network(s) being advertised from the neighbor routers.

Administrative Distance

Now that you are aware of the multiple sources of routing information, you must consider a feasible anomaly that could occur with your routing sources. Namely, if you have several sources of information such as connected interfaces, static routes, and multiple routing protocols, which one are you to trust when more than one source advertises the same network? For example, if a router learns about the 192.168.1.0/24 network from a routing protocol and a static route, how does the router decide which entry to place into its routing table?

The answer lies within a program logic in the IOS called the *administrative distance*. The administrative distances are arbitrary values between 1 and 255 that are assigned to routing information sources. These values represent a level of trustworthiness of the information source, in which lower administrative distances are preferred over higher ones.

NOTE

The administrative distance applies only when multiple sources are advertising exactly the same subnet.

Table 10.1 lists the Cisco IOS default administrative distances for some of the routing sources.

TABLE 10.1 Default Administrative Distances

Routed Source	Default Distance
Connected	0
Static Route	1
EIGRP (internal)	90
IGRP	100
OSPF	110
RIPv1 and v2	120
EIGRP (external)	170

It should come as no shock that connected interfaces are the most trustworthy sources because they are connected directly to the local router. Static routes have a low administrative distance of 1 because the Cisco IOS assumes that you are competent administrators and any manual entry of a routable network is trusted over any dynamic routing protocols such as EIGRP, IGRP, OSPF, and RIP.

EXAM ALERT

Memorizing the default administrative distances serves as a resourceful tool in answering questions on the CCNA exams.

Static Routes

When you interconnect routers together as demonstrated in Figure 10.2, they are aware of only their directly connected networks. Unless you configure a static route or use routing protocols, the routers will never know about their neighbors' ethernet networks because they are not connected. In other words, Router A is not aware of Router B's 172.17.0.0 network and Router B is not aware of Router A's 172.16.0.0 network.

So when do you use static routes as opposed to routing protocols? As mentioned before, static routes are manual configuration entries in which you tell the router how to get to destination networks that are not locally attached. This is useful in simple networks such as the one in Figure 10.2 in which there is a single link in or out of the networks, known as a *stub network*. Because there is only one link to get to the neighbor network, you don't need to worry about reacting dynamically if the path fails because there are not any alternate paths to that network. Additionally, if you want to have complete control of your routing path decisions or you want to conserve bandwidth on your links (routing protocols consume bandwidth), static routes can provide you authoritative control without requiring any link bandwidth or resources because they require only a local configuration.

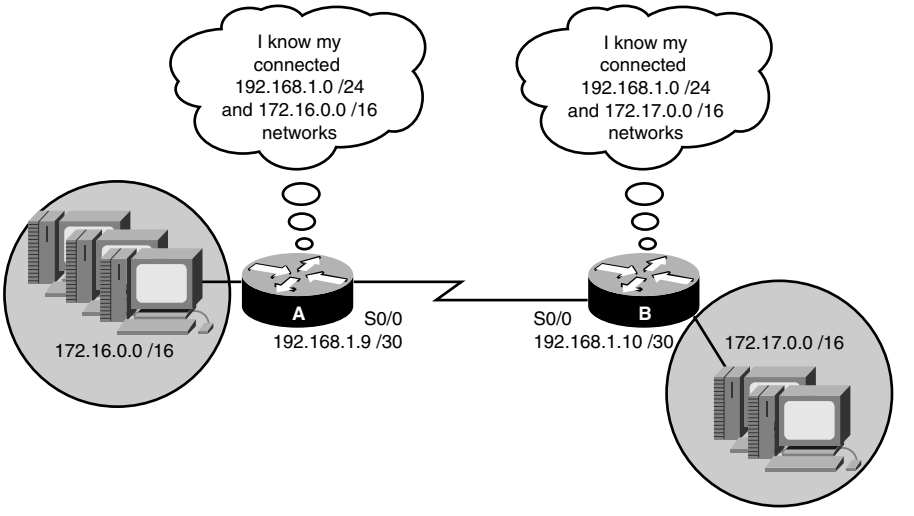


FIGURE 10.2 Static route exhibit.

EXAM ALERT

Keep in mind that static routes are used when you have a stub network, want control of your routing decisions, or want to conserve bandwidth on links.

Configuring Static Routes

The general idea behind the static route is to tell the router how to get to a destination network that is not attached to it by going through another router's interface. It is similar to telling someone, "To go outside, go through that door." The syntax to configure a static route in global configuration is `ip route` followed by the destination network, destination subnet mask, and the next-hop IP address of the neighbor's interface. For example, to configure a route to the 10.0.0.0/8 network through the neighbor's serial interface of 192.168.2.5, the command would look like the following:

```
Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.2.5
```

NOTE

It is possible to specify the local interface instead of using a next-hop IP address on point-to-point links (a link with only two routers connected it on each side). On multi-access links such as ethernet or Frame Relay, you should not use the interface because the local router does not know to which router to forward the information if multiple devices exist on the link.

In the stub network example in Figure 10.3, a static route to Router A and one to Router B were added, telling them about their neighbors' ethernet networks. These entries are placed in their routing tables, specifying any packets that are destined for those respective networks must go to the IP of the neighbor's serial 0/0 interface. From that point, the packets will be routed out Router A and Router B's ethernet interface because those destination networks are directly connected to the router. This entry remains in the routing table as long as the next hop address remains valid (the serial network does not go down) or the configuration is not removed.

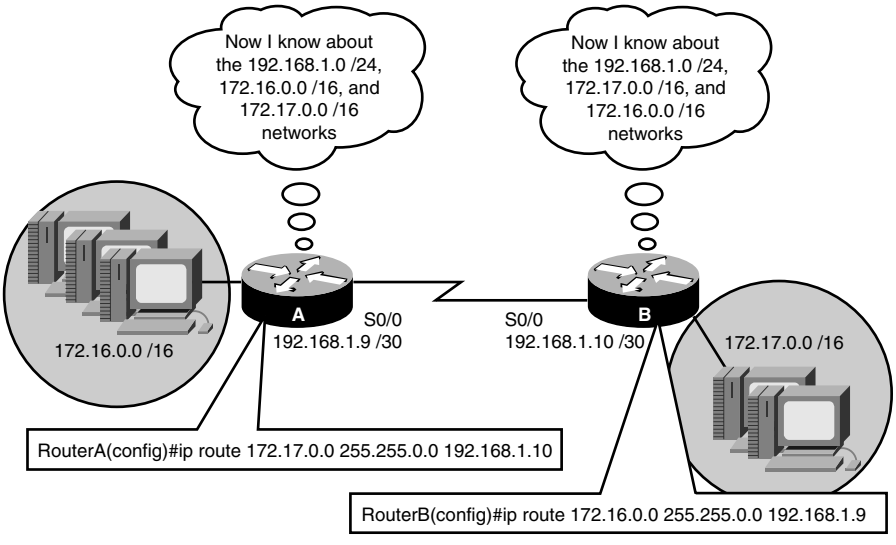


FIGURE 10.3 Static route configuration example.

Floating Static Routes

At the end of an `ip route` static route command, it is possible to add a parameter to assign this particular static route a higher administrative distance than the default administrative distance of 1. These entries, known as *floating static routes*, are not placed in the routing table if the subnet is being advertised by a routing source with a lower administrative distance. Floating static routes are useful when you have a stand-by redundant link to another network that will activate in the event of a primary link failure.

For example, consider the example configured in Figure 10.4. Because you have redundant point-to-point links, you can configure the primary static route as usual and include a floating static route to be used if the primary link fails. The `2` at the end of the second static route identifies that route as the floating static route. This entry does not show up in the routing table because the primary route advertises the same subnet with a lower administrative distance (if not specified, the default is 1). If one of the serial 0/0 interfaces on the primary link goes down, the next hop is no longer valid and is removed from the routing table. Because the floating static route has the next lowest administrative distance, that entry is put in the routing table and that link is used until the primary link returns.

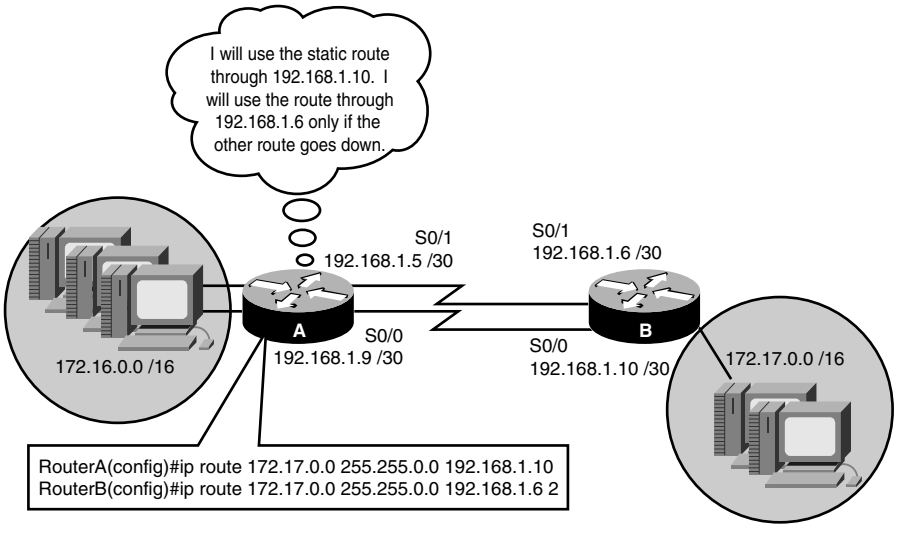


FIGURE 10.4 Floating static route configuration example.

EXAM ALERT

If an administrative distance is not specified, a Cisco router uses the default administrative distance for static routes (1). If an administrative distance is specified, it is being used as a floating static route if a redundant link fails.

Default Routes

Static routes have proved their usefulness in situations where you want to add a network entry in a routing table when the network is reachable via a single path. This can turn into a daunting administrative task when there are a large number of networks in which you must configure static routes. This is especially true when you are connecting to your ISP because you do not want to configure a static route for every network on the Internet.

In these situations, you might be better served using something called a *default route*, as illustrated in Figure 10.5. This entry is a gateway of last resort for routers in that if a destination IP address does not have a network entry in the routing table, this route is used. The syntax for a default route is similar to a static route except that the destination and subnet mask are both 0.0.0.0:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.10
```

NOTE

Once again, you can specify the local interface as opposed to the next-hop IP address on a point-to-point link.

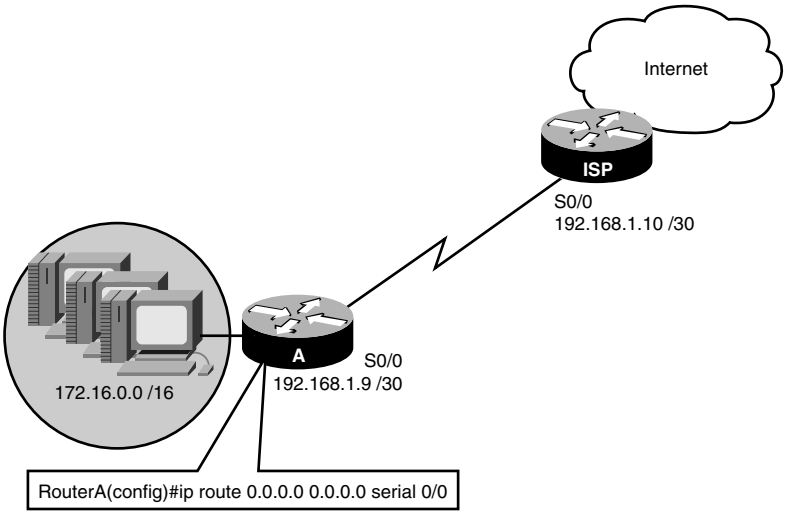


FIGURE 10.5 Default route configuration example.

EXAM ALERT

Be sure to look closely at the wording in a question regarding a default route (gateway of last resort). When used in a router, the command is `ip route 0.0.0.0 0.0.0.0`; however, to configure a default route in a Layer 2 switch, it is `ip default-gateway` because Layer 2 switches do not have Layer 3 routing entries.

Verifying Static and Default Routes

The best way to verify a static or default route configuration is by checking that the route is evident in the routing table. The command to view the IP routing table is `show ip route`. If you want to see the routing entry for a specific network, you can append that subnet to the `show ip route` command (for example, `show ip route 192.168.23.0`). Figure 10.6 displays the output of the `show ip route` command.

```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

S    172.17.0.0/16 [1/0] via 192.168.1.10
C    172.16.0.0/16 is directly connected, FastEthernet0/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.8 is directly connected, Serial0/1
S*   0.0.0.0/0 [1/0] via 192.168.1.10
```

FIGURE 10.6 `show ip route` output.

Notice the top of the output has a legend identifying the possible codes that can be listed in the routing table. In the table itself, you can see the two directly connected networks signified by the letter *C*. In addition, you can also see the static route to 172.17.0.0 and the static default route entries (indicated by the letter *S*), using 192.168.100.10 as the next hop. Also notice that the routing table identifies that the gateway of last resort (192.168.100.10) is set on this router because a default route was configured with the next hop to that address.

TIP

You can clear out an entry in your routing table by using the `clear` command followed by the network or * for all networks in Privileged EXEC. For example, to clear the 192.168.1.0 network from your routing table, you would type the following:

```
Router#clear ip route 192.168.1.0
```

Dynamic Routing Protocols

Objective:

Evaluate the characteristics of routing protocols

Select an appropriate routing protocol based on user requirements

When complex networks contain multiple interconnections, static routes are no longer a practical solution because they cannot adapt or react to changes in the topology. Not to mention, the configuration complexity can grow exponentially as you add more devices to the network.

EXAM ALERT

Do not confuse routing protocols with routed protocols on the exam. Routed protocols are protocols such as those in the IP protocol suite that are used to carry the data across our network. Routing protocols are exchanged between routing devices to determine the optimal path to route the routed protocols.

For example, given the network design in Figure 10.7, Router A will know only the three directly connected networks attached to the router. For IP packets to reach the 172.17.0.0 network via static routes, you would have to configure Router A to go through one of its neighbor routers, such as Router B. However, Router B also requires a static route to 172.17.0.0 because that network is not directly connected to it. Supposing that the router is using Router F as its next hop, that router does not require a static route since it is directly connected. Unfortunately, our configuration undertaking does not stop there because we have to configure a static route in Router F and Router B back to the 172.16.0.0 network.

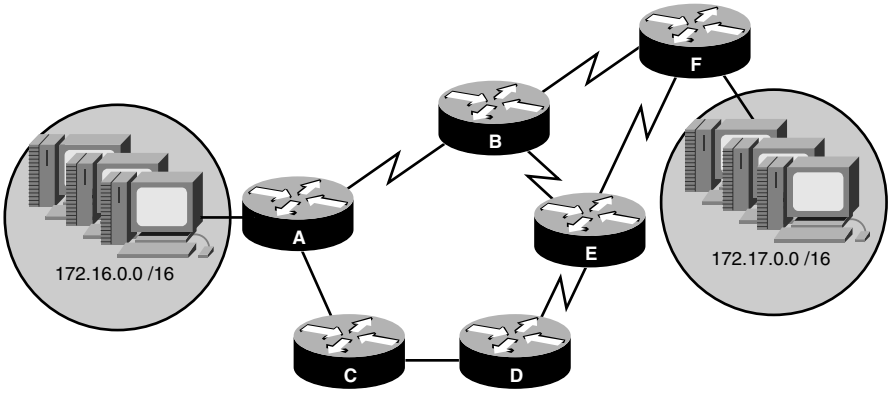


FIGURE 10.7 Complex internetwork design.

Granted, the configuration scenario in Figure 10.7 is not drastically difficult or strenuous, but imagine if the network contained 20 more routers. More importantly, consider what would happen if the link between A and B went down. Because the routes are statically configured in the routers, you must now go back and remove the static routes in Routers A and B and redirect the traffic by configuring static routes to go through Routers C, D, and E. Not to mention, you must remove and reconfigure static routes back to the 172.16.0.0 network in Routers F, E, D, and C.

To alleviate the administrative calamity you might have to encounter with static routes in complex networks, you can use dynamic routing protocols. If you configure routing protocols, the routers will advertise their connected networks to the rest of the routers in the network, thus minimizing the amount of configuration required. In addition, routing protocols can detect and adapt to topology changes in the internetwork.

Routing Metrics

Because one of the core responsibilities of routing protocols is to build routing tables to determine optimal routing paths, you need to have some means of measuring which routes are preferred when there are multiple pathways to a destination. Routing protocols use some measure of metrics to identify which routes are optimal to reach a destination network. The lowest cumulative metric to a destination is the preferred path and the one that ultimately enters the routing table. Different routing protocols use one or several of the following metrics to calculate the best path:

- **Hop count**—The number of routing devices that the packet must travel to reach a destination network.
- **Bandwidth**—The cumulative bandwidth of the links to the destination in kilobits per second.

- **Delay**—The length of time (measured in microseconds) a packet takes from source to destination.
- **Reliability**—The consistency of the links and paths toward the destination based upon error rates of the interfaces.
- **Load**—The cumulative amount of congestion or saturation of the links towards the destination.
- **MTU**—The maximum frame size that is allowed to traverse the links to the destination.
- **Cost**—An arbitrary number typically based upon the bandwidth of the link.

Classful and Classless Routing Updates

As you will see in the following sections, routing protocols are categorized into several different classifications based upon common characteristics and properties that they share. The first of these classifications revolves around the contents of routing updates that Layer 3 devices advertise to their neighbors. Specifically, if the routing updates do not contain the subnet mask along with their respective advertised networks, they are said to be *classful routing protocols*. Conversely, if the subnet mask is transmitted along with the network information, it is characterized as a *classless routing protocol*. This may seem like a trivial characteristic to define routing protocols, but as you will see, the results of the subnet mask being present or not in routing updates can affect the routing protocols you choose and how efficiently you can design your entire network.

With classful routing protocols, you assume that your network's design conforms to the class boundaries of IP subnets. In other words, major networks in your design use their default classful subnet masks as described in Chapter 4, "IP at the Network Layer" (for example, Class A uses 255.0.0.0, Class B uses 255.255.0.0, and Class C uses 255.255.255.0). If you happen to subnet a major network into smaller subnets, classful routing protocols are disadvantageous because they do not receive the revised subnet mask. For this reason, classful routing protocols will updates in one of two ways:

- If the network in the updates matches the same major classful network on the interface through which it was received, it uses the subnet mask of the interface and places it in the routing table.
- If the router advertises a network to a different major network out an interface that is not in the same major network, it automatically summarizes the network to its classful boundary.

For example, when Router B in Figure 10.8 sends an update to Router A using a classful routing protocol (RIP in this example), it summarizes the 172.17.30.0/24 to a default Class B 172.17.0.0 network because it is going out the serial 0/0 interface, which does not contain a subnet in that major network. The 192.168.1.60 network, on the other hand, is in the same major network, so it does not automatically summarize that subnet. When Router A receives that update, it adds the 172.17.0.0 network to its routing table, specifying Router B's serial interface IP (192.168.1.10) as the next hop to reach that network. In addition, it adds the 192.168.1.60 network as well, using its interface mask because it is in that same major network.

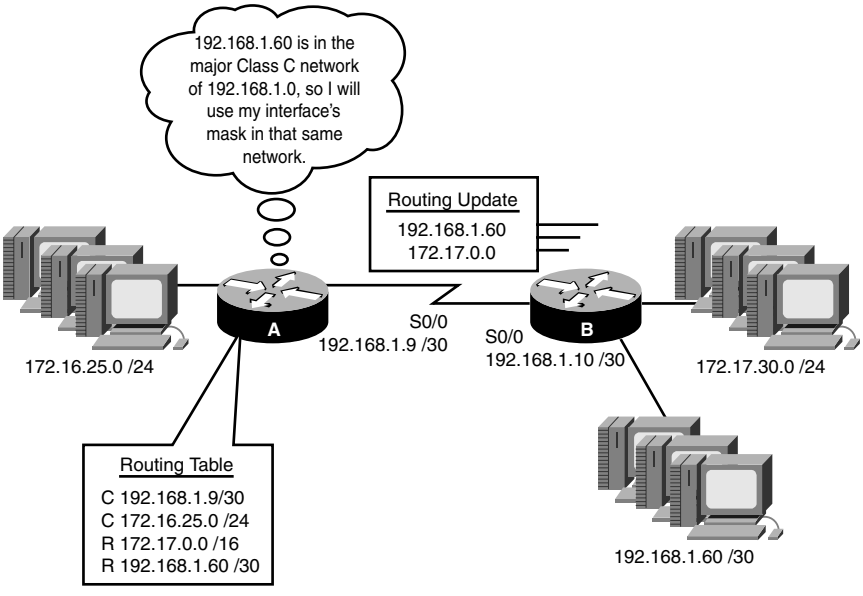


FIGURE 10.8 Classful routing update scenario.

Now consider if the ethernet segment of Router B's 192.168.1.60 network had a /29 subnet mask. The end result would still be the same as before in that Router B would advertise the 192.168.1.60 subnet and Router A would use its interface's subnet mask of /30. In these instances, classful routing protocols are not the optimal choice because Router A has a route to only a third of the 192.168.1.60 /29 subnet. For this reason, when you subnet a major network, you must be sure that you use the same subnet mask throughout your network design with classful routing protocols. This same subnet design is commonly referred to as a *Fixed Length Subnet Mask (FLSM)* network design.

Classful routing protocols can also be problematic when major classful networks are subnetted and are haphazardly dispersed throughout the network, as illustrated in Figure 10.9. When Routers A and C summarize their networks to Router B, Router B thinks that the 172.16.0.0 network is out both of its serial interfaces. This could easily result in traffic destined for 172.16.10.0 and 172.16.50.0 being load balanced out each interface, resulting in 50% packet loss because the packets are sent in a round robin fashion between both interfaces.

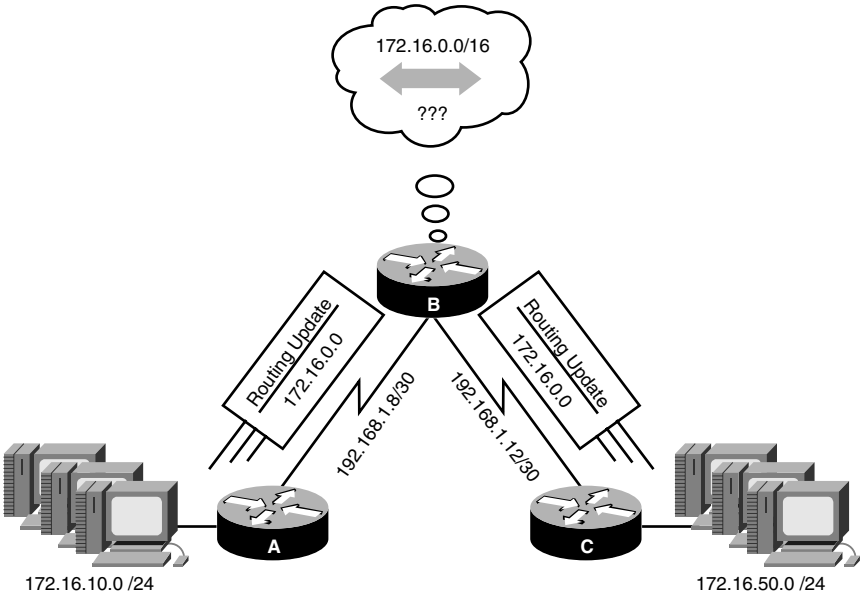


FIGURE 10.9 Discontiguous network example.

EXAM ALERT

Be sure to know that classful routing protocols support automatic summarization and must have a FLSM network design without any discontiguous networks.

Because classless routing protocols advertise the subnet masks in their routing updates, discontiguous networks are no longer an issue because routing devices are aware of the subnetted networks. In addition, the requirement of using the same subnet mask throughout the network ceases to apply because the routers do not automatically summarize the networks to a classful boundary. No longer inhibited by these constraints, you are free to use different subnet masks, known as Variable Length Subnet Masks (VLSMs) in your network design. In addition, you now have full autonomy to manually summarize networks as you wish to help keep routing tables small to conserve resources. VLSM and route summarization are described in greater detail in the following sections.

EXAM ALERT

Be sure to know that classless routing protocols support discontiguous networks, VLSM, and route summarization.

VLSM

Objective:

Design an IP addressing scheme to support classful, classless, and private addressing to meet design requirements

Using classless routing protocols affords you the luxury of having support for a VLSM network design. This is advantageous in your network planning because you can allot the appropriate number of IP addresses required for each link. Not to mention, by assigning the minimal number of IP addresses required for an given link, you conserve IP addresses. For example, you can use a /30 subnet mask for point-to-point links because you need only two available IP addresses and a /27 subnet mask on an ethernet segment to accommodate 30 hosts. If you were using classless routing protocols, you would have to use a /27 for all links, which would inevitably waste 28 IP addresses on the point-to-point links.

EXAM ALERT

Remember that point-to-point links require only a /30 (255.255.255.252) subnet mask because you need only an IP address for the router's interfaces on each side of the link.

Throughout your certification and career, it is quite possible you will have to design your network given a usable subnet and host requirements for all your links. When tackling this designing task, be sure to adhere to the following guidelines:

1. If possible, start with the larger subnets first.
2. Write out the ranges that you have assigned to ensure you do not accidentally overlap subnets.
3. Make sure your networks start on incremental boundaries (128, 64, 32, and so on).

EXAM ALERT

Be prepared to use VLSM to assign subnets to links given the subnetable network and host requirements.

Challenge

Given the design shown in Figure 10.10, you are going to determine how you can use VLSM to ensure you are using the appropriate subnets given a design scenario. In this example, the zero subnets are available for use.

(continues)

(continued)

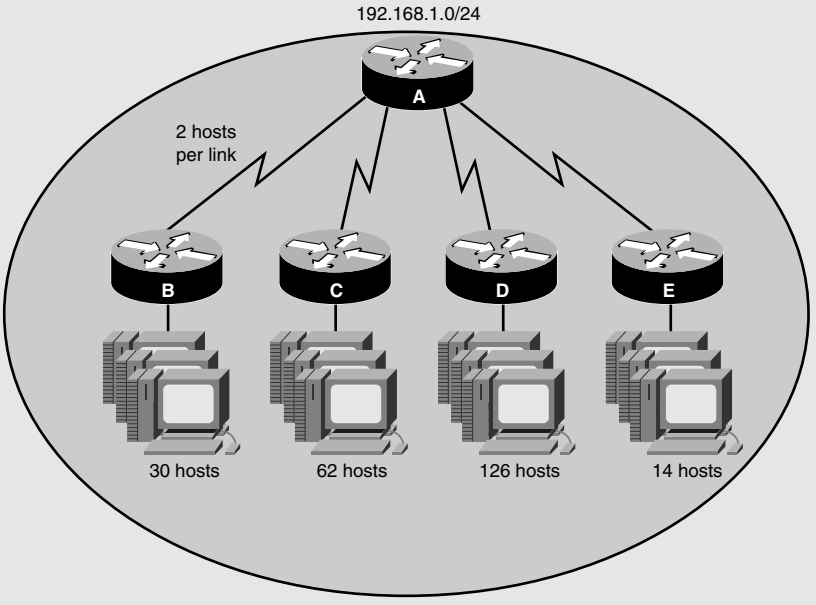


FIGURE 10.10
VLSM design scenario.

1. Remember to add 2 to each network to accommodate the network ID and broadcast address.
2. Calculate the network and subnet mask for Network D (the largest network).
3. Given the remaining IP addresses, calculate the network and subnet mask for Network C.
4. Given the remaining IP addresses, calculate the network and subnet mask for Network B.
5. Given the remaining IP addresses, calculate the network and subnet mask for Network E.
6. Given the remaining IP addresses, calculate the network and subnet mask for the four point-to-point links.

Challenge Answer

Network D needs to have a subnet that accommodates 128 addresses. A subnet mask of 255.255.255.128 or /25 provides enough hosts for that network. The next subnet for Network C begins at 192.168.1.128 (because you just took 128 IPs) and use a subnet mask of 255.255.255.192 or /26 to accommodate the 64 IP addresses. Network B is assigned the network of 192.168.1.192 with a subnet mask of 255.255.255.224 or /27 to give you 32 IPs. A subnet mask of 255.255.255.240 or /28 with a network ID of 192.168.1.224 is assigned to Network E for the 16 IPs required for that link. The four point-to-point links

all use a 255.255.255.252 or /30 subnet mask using the last four networks: 192.168.1.240, 192.168.1.244, 192.168.1.248, 192.168.1.252. To summarize:

- **Network D**—192.168.1.0 /25
- **Network C**—192.168.1.128 /26
- **Network B**—192.168.1.192 /27
- **Network E**—192.168.1.224 /28
- **Point-to-point links**—192.168.1.240 /30, 192.168.1.244 /30, 192.168.1.248 /30, and 192.168.1.252 /30.

Route Summarization

As already mentioned, classful routing protocols automatically summarize advertised networks to the classful subnet boundaries. Classless routing protocols, on the other hand, require you to manually control the networks being summarized to your neighbors in the router configuration. By aggregating a contiguous set of networks into an advertised summarized route, you keep the size of the routing tables to a minimum. Neighbors that receive the summarized route do not need to know about the individual subnets you create behind your router because they inevitably have to go through your router to get to them. The additional offshoot of this summarized picture is that your classless routing protocols do not need to notify those neighbors if one of those subnets goes down because they do not even have that subnet in their routing tables. Thus, you can isolate topology changes to be contained behind that summarizing router.

Because you are required to manually specify the networks you are to advertise, you must learn how to accurately summarize smaller subnets into one or several larger networks, or supernets. The rules for supernetting are similar to subnetting, except in this case, you are stealing bits from the network portion of an IP network to create a larger network. The rules for supernetting are as follows:

1. Be sure that the networks are contiguous (otherwise you would be summarizing networks that you do not have behind the router).
2. Count the number of networks you want to summarize.
3. Determine an increment that is equal to or less than the number of networks.
4. Make sure your base networks start on incremental boundaries (128, 64, 32, and so on) for the number of networks you are summarizing.
5. Calculate the subnet mask by the number of bits you need to steal from the original subnet to equal that incremental value.

The beauty of supernetting is that the resultant network and subnet mask will designate many IP address networks in a single entry. The fact that you are stealing bits from the network portion of an IP address could quite easily violate the traditional barriers of classful addressing, known as *Classless Interdomain Routing Notation* or CIDR.

For instance, it would not be uncommon to see a summary entry look like the following: 192.168.16.0 /20. This single entry used to be a Class C (/24), but four bits were stolen from the network portion to represent 16 networks ($2^4 = 16$). When you advertise this supernet to neighbors, they know that they must go through your router to get to networks 192.168.16.0 through 192.168.31.0 (16 total networks).

EXAM ALERT

Be prepared to determine the networks being advertised in a given supernet or determine the summary network, given the networks to be summarized.

Figure 10.11 illustrates a typical route summarization example in which Router B is summarizing all its subnetted networks to Router A as one supernetted network. Following the steps outlined previously, you can determine the aggregate network entry to advertise, as follows:

- The networks are all contiguous so you can summarize them accurately.
- There are 32 total networks that are to be summarized.
- 32 conveniently falls on an incremental boundary.
- Because the network is 192.168.64.0, 64 is an increment of 32 so we can use that as the base network for the summary route.
- You must steal 5 bits ($2^5 = 32$) from the /24 network, so /19 (24 – 5 = 19).

By creating the summary route 192.168.64.0 /19, Router A will only be required to maintain that one entry in its routing table as opposed to the individual 32 subnets. If a topology change occurs in one of the subnets behind Router B, there is no need to advertise that change to Router A because it knows about only the summarized network.

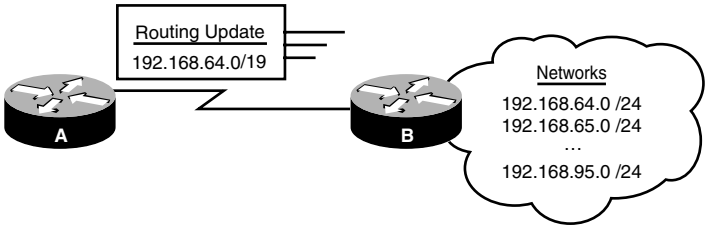


FIGURE 10.11 Supernetting route summarization example.

NOTE

The number of summarized networks or the base network do not always conveniently fall on incremental boundaries. In those instances, it may take several summary network entries to encompass all the networks you want to summarize.

Interior and Exterior Gateway Routing Protocols

Routing protocols can fall under two major categories depending on the autonomy of the network on which the routing protocol exists. The identifying characteristic of the category to which the routing protocol belongs ultimately depends on whether the routing protocols exchanges updates within a network that is under your administrative control. When the network is under your control in your own administrative domain, it is known as an *autonomous system*. Routing protocols used to disseminate information to maintain routing tables and establish pathways inside an autonomous system are categorized as Interior Gateway Protocols (IGPs).

Conversely, the other category of routing protocols is designed to route in between these autonomous systems. For instance, Border Gateway Protocol (BGP) is a routing protocol that is used by ISPs for routing traffic over the Internet. Because the Internet comprises thousands of networks, each under different administrative control, you need to use an Exterior Gateway Protocol such as BGP to route in between these autonomous systems.

Distance Vector Routing Protocols

In addition to being an IGP/EGP or classful/classless, routing protocols can also fall into one of three classes. Once again, the functionality and characteristics of the routing protocol dictate under which class it falls. The most long-standing of these classes is *distance vector routing protocols*.

Distance vector routing protocols concern themselves with the direction (vector) in which the destination lies and some means of measurement (metric) it takes to reach that destination. Distance vector routing protocols inform their directly connected neighbors of all the connected and learned networks they know about in their routing tables. In fact, they broadcast the contents of the entire routing table to their neighbors periodically, regardless of whether there is a change in the network topology. When the neighbors receive that routing information, they identify and add any new networks to their routing tables and update the metric before eventually passing it on to their neighbors. Because the routing table information is updated before it is sent on to neighbors, downstream routers do not learn that information first hand. For this reason, distance vector routing protocol update processing is often referred to as "routing by rumor." Distance vector routing protocols are discussed in greater detail in Chapter 11, "Distance Vector Routing Protocols."

Link-State Routing Protocols

As the name states, *link-state routing protocols* advertise the state of the links in the network. In fact, they advertise the states and metrics (cost) of all the links they know about for the entire topology to their neighbors, as opposed to just the best routes in your routing table. This detailed overview of the entire routing domain enables each router to calculate and make a decision on the best route from this first-hand information, rather than listen to what its neighbor believes is the best route. In fact, link-state routing protocols keep three tables: a neighbor table of all discovered neighbors, a topology table of all the possible routes to reachable networks learned, and a routing table that contains the best route based upon the lowest metric calculated from the topology table.

At first, this may sound like a lot of information to be exchanged between routers; however, link-state routing protocols initially discover their neighbors when they first boot up and synchronize their topology tables. After the neighbor discovery and topology synchronization, they send only periodic hello messages to let their neighbors know they are still functioning. This is significantly different from distance vector routing protocols that periodically exchange the entire routing table, which can contain a large amount of information, depending on the size of the network.

In addition, link-state routing protocols react much faster when a topology change occurs in the network. In fact, these protocols were initially created in response to the slow convergence issues that you typically encounter with distance vector routing protocols. The downfall to these routing protocols is the resources they consume in the router. Namely, maintaining and processing three tables consume quite a bit of memory and processor power. Link-state routing protocols are discussed in greater detail in Chapter 12, "Link-State and Hybrid Routing Protocols."

Advanced Distance Vector/Hybrid Routing Protocols

They say it usually takes three tries to get something absolutely right. The truth behind this saying is that you learn from the mistakes of the previous two attempts. Such is the case with advanced distance vector, often referred to as *hybrid* or *balanced hybrid* routing protocols. Because they take the best features and avoid the pitfalls of both distance vector and link-state routing protocols, hybrid routing protocols are a more proficient breed of routing protocols than their predecessors.

The Routing Table Revisited

Now that you have learned about the several types of routing sources including static routes and dynamic routing protocols, it's time to revisit the routing table and solidify how network entries are added and used in routing decisions. To help illustrate this process, refer to the `show ip route` output in Figure 10.12.

Notice that there are now several entries for directly connected networks, a static route, and several dynamic routing protocol entries from EIGRP, RIP, IGRP, and OSPF. For each dynamic routing protocol, there is the network and subnet mask that is being advertised by neighbor routers, followed by two numbers in brackets separated by a forward slash (/). The number to the left of the forward slash is the administrative distance of the routing protocol. The number to the right of the forward slash represents the metric that is being used by the routing protocol to determine the best path to the destination network. This information is immediately followed by the router from which it learned this information (thus the next hop address). The last item in the routing entry represents the interface packets must exit to reach those networks.

EXAM ALERT

You must be adept in deciphering the output of a routing table.

```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is not set

R    172.17.0.0/16 [120/1] via 192.168.1.10, Serial0/1
C    172.16.0.0/16 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
D       10.2.0.0/16 [90/2297856] via 192.168.1.10, Serial0/1
D       10.3.0.0/16 [90/2297856] via 192.168.1.10, Serial0/1
I       10.0.0.0/8 [100/8976] via 192.168.1.3 , Serial0/0
D       10.1.0.0/16 [90/2297856] via 192.168.1.10, Serial0/1
D       10.4.0.0/16 [90/2297856] via 192.168.1.10, Serial0/1
S       10.5.0.0/16 [1/0] via 192.168.1.10
O       10.4.0.1/32 [110/65] via 192.168.1.10, FastEthernet0/1
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.8 is directly connected, Serial0/1
```

FIGURE 10.12 Multi-source routing table output.

Assuming that several of the routing protocols advertised the same networks, how did these specific network entries come to be in the routing table? The obvious answer is that the interfaces, a static route, and multiple routing protocols were configured and the resultant table just appeared. However, to answer the question more specifically, each routing protocol determined which routes should be entered in the routing table based upon the lowest metric to those destinations. In the chance that one or more routing sources is trying to place a network entry in the routing table for exactly the same subnet, the routing protocol with the lowest administrative distance is chosen because it is the most trustworthy.

After the routing table is built, packets are routed to their destinations by examination of the destination IP address in an IP packet and associating the network in the routing table with that IP address. If there isn't a match for the network lookup the packet is forwarded to its default route. If the gateway of last resort is not set (as in Figure 10.12), the packet is dropped and an ICMP destination unreachable message is sent back to the source to indicate that the destination cannot be reached.

EXAM ALERT

Routing of packets is based upon the destination IP address in a packet. If the router does not have an entry for the packet's associated network, it sends an ICMP destination unreachable message back to the source.

In Figure 10.12's output, several entries for the 10.0.0.0 network are listed in the routing table. Interestingly enough, there is an IGRP entry for the 10.0.0.0 /8 network to go out serial 0/0 and four EIGRP-learned networks for 10.1.0.0 /16, 10.2.0.0 /16, 10.3.0.0 /16, and 10.4.0.0 /16, all destined for interface serial 0/1. Because the EIGRP networks are subnets of the major 10.0.0.0 network, which interface will the router use to route a packet destined, for example, for 10.1.0.3?

Cisco's routing logic answers this question by using a rule called the *longest match*. The longest match rule states that when a packet has multiple possible network entries to use, the more specific subnet is used over the less specific. In other words, the longer the number of bits in the subnet mask (thus the smaller subnet), the more chance it has of being the chosen network. In the routing table example, a packet destined for 10.1.0.3 would use the subnet with the longest prefix (subnet mask), which is the EIGRP route for 10.1.0.0/16 exiting interface Serial 0/1.

Routing Redistribution

You are likely to encounter in your Cisco travels certain situations in which you must run multiple routing protocols in your network. For instance, your company is in the process of merging with another company's network, and their routers are running a different routing protocol than yours. In addition, you may have to connect your Cisco router network to a non-Cisco routing infrastructure and you are using Cisco proprietary routing protocols.

In instances where you are running multiple routing protocols, it may be necessary to have networks advertised in one routing protocol injected into the other. Unfortunately, because routing protocols are so diverse in nature, they do not inherently interact or exchange information with each other when there are multiple routing protocols running in the network. The transferal of network information from one routing protocol into another is a manual configuration called *redistribution*.

The redistribution configuration is typically done at one or a couple of routers that sit on the boundary between each routing protocol, as illustrated in Figure 10.13. These devices run both routing protocols and must be manually configured to inject the networks learned from one routing protocol into the next. Redistribution can occur in one of two fashions:

- **One-way redistribution**—Networks from an edge protocol are injected into a more robust core routing protocol, but not the other way around. This method is the safest way to perform redistribution.
- **Two-way redistribution**—Networks from each routing protocol are injected into the other. This is the least preferred method because it is possible that suboptimal routing or routing loops may occur because of the network design or the difference in convergence times when a topology change occurs. Figure 10.13 is an example of two-way redistribution.

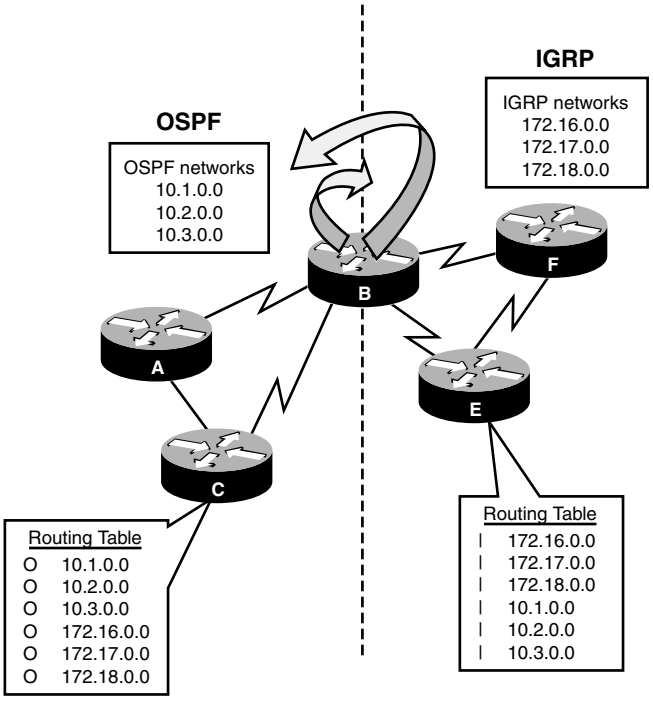


FIGURE 10.13 Two-way redistribution example.

EXAM ALERT

Remember that one-way redistribution translates networks from one routing protocol in another, but not vice versa. Two-way routing redistribution dispenses networks from each routing protocol into the other.

Chapter Summary

This chapter looked more closely at the operations involved in routing packets with Layer 3 devices such as routers and Layer 3 switches. You send packets from workstations on the local network to routing devices by configuring those devices with a default gateway IP address that matches the IP of your router. When the packet arrives at the router, it consults its routing table to determine whether the destination IP address in the IP packet has a match for the destination's network. If it does not have a matching entry, it looks to see whether the routing table has a default route. If no gateway of last resort is set, it drops the packet and sends an ICMP destination unreachable message back to the source. In instances where there are several matches for the destination network, it uses the entry that has the longest match.

The entries in the routing table can come from several routing sources. When the interface is operational and an IP address is assigned, they show up in the routing table as connected interfaces. Manual static route entries that were manually configured show up as an "S." Routing protocols choose their best network paths by calculating the lowest metric for their respective routing protocols. If multiple routing sources advertise the same subnet, the source with the lowest administrative distance is placed in the routing table.

The routing protocols can fall into several categories, based upon the characteristics that the protocols utilize. For instance, if a routing protocol does not advertise the subnet mask in its routing updates, it is a classful routing protocol. Classful routing protocols require the network design to have the same subnet mask in the design known as FLSM. In addition, these routing protocols cannot support discontiguous networks and automatically summarize network entries to the classful boundary when crossing interfaces in other major networks. When subnet masks are including the routing advertisements, these updates are said to be classless. Classless routing protocols support VLSM network designs, discontiguous networks, and require manual summarization of networks.

If the routing protocol is designed to route inside an autonomous system, that routing protocol is an IGP. EGP routing protocols, on the other hand, are designed to route between autonomous systems.

Finally, routing protocols can belong to one of the following three classifications:

- **Distance Vector**—The entire routing table is periodically sent to directly connected neighbors regardless of a topology change. These routing protocols manipulate the routing table updates before sending that information to their neighbors and are slow to converge when a topology change occurs.

- **Link-State**—All possible link states are stored in an independent topology table in which the best routes are calculated and put into the routing table. The topology table is initially synchronized with discovered neighbors followed by frequent hello messages. These routing protocols are faster to converge than distance vector routing protocols.
- **Hybrid**—By using the best characteristics from both link-state and routing protocols, these advanced routing protocols efficiently and quickly build their routing information and converge when topology changes occur.

Key Terms

- default gateway
- routing table
- connected interface
- hop
- routing protocols
- administrative distance
- static routes
- stub networks
- floating routes
- default route
- classful routing protocols
- classless routing protocols
- FLSM
- discontiguous networks
- VLSM
- route summarization
- supernet
- CIDR
- autonomous system
- IGP
- EGP
- distance vector routing protocols
- link-state routing protocols
- advanced distance vector/hybrid routing protocols
- longest match rule
- redistribution

Apply Your Knowledge

Exercises

10.1 Create a Static and Default Route

This exercise tests your configuration skills in configuring a static and default route.

Estimated Time: 5 minutes

1. Enter Privileged EXEC.
2. Enter Global Configuration.
3. Configure a static route for the 10.23.5.0/24 network using 192.168.64.2 as the next hop address.
4. Configure a floating static route for the 10.23.5.0/24 network using 192.168.60.3.
5. Configure a default route to exit out of your serial interface.

10.2 Create a Summary Route

Estimated Time: 5 minutes

This exercise ensures that you are able to accurately supernet smaller subnets into one summary route.

Given the following networks, what is the summary route you can use to advertise these individual subnets to your neighbor router as an aggregate entry?

172.16.0.0 /16

172.17.0.0 /16

172.18.0.0 /16

172.19.0.0 /16

1. Count the number of networks you want to summarize.
2. Determine an increment that is equal to or less than the number of networks.
3. Make sure your base networks start on incremental boundaries (128, 64, 32, and so on) for the number of networks you are summarizing.
4. Calculate the subnet mask by the number of bits you need to steal from the original subnet to equal that incremental value.

Review Questions

1. What are the Layer 2 and Layer 3 characteristics of a packet destined for a network on a remote segment?
2. Why would you use a static route versus a routing protocol?
3. What are the characteristics of distance vector routing protocols?
4. What are the characteristics of link-state routing protocols?
5. What is the difference between classful and classless routing protocols?

Exam Questions

1. Given the following output, on which interface will a packet destined for 192.168.1.34 /24 be routed?

```
RouterA>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/1
R    172.17.0.0/16 [120/1] via 192.168.1.10, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.8 is directly connected, Serial0/0
```

   - ❍ **A.** Serial 0/1
   - ❍ **B.** Serial 0/0
   - ❍ **C.** Fast Ethernet 0/0
   - ❍ **D.** None of the above

2. Your network designer, Denise, subnetted the major classful network of 192.168.2.0 into varying-sized subnets throughout your network. Which routing protocol category should not be your choice of routing protocol?

   - ❍ **A.** Classful
   - ❍ **B.** IGP
   - ❍ **C.** Link-state
   - ❍ **D.** ODR

3. Which of the following is not a characteristic of link-state routing protocols?

   - ❍ **A.** Fast convergence
   - ❍ **B.** Broadcasts routing table
   - ❍ **C.** Keeps track of neighbors in table
   - ❍ **D.** Knows all possible routes

4. Which of the following is not a subnet in the CIDR summary route 192.168.16.0 /21?

   - ❍ **A.** 192.168.16.0 /24
   - ❍ **B.** 192.168.20.0 /24
   - ❍ **C.** 192.168.24.0 /24
   - ❍ **D.** 192.168.23.0 /24

5. What is the consequence of using the following command?

   ```
   Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
   ```

   - ❍ **A.** The entry will show up in the routing table signified with an *R*.
   - ❍ **B.** This entry is configured in a Layer 2 switch to send traffic to a Layer 3 routing device.
   - ❍ **C.** 192.168.10.2 is the IP address of the router that advertised this network in the routing protocol update.
   - ❍ **D.** If there is not an exact match in the routing table, packets will be sent to 192.168.10.2.

6. What is the consequence of using the following command? (Choose 2.)

   ```
   Router(config)#ip route 192.168.20.4 255.255.255.0 10.1.1.1 3
   ```

   - ❍ **A.** The 3 at the end of the command signifies it is a floating static route.
   - ❍ **B.** The 3 at the end of the command signifies the hops to get to the destination.
   - ❍ **C.** The destination network is incorrect and this command will not work.
   - ❍ **D.** The default administrative distance for this command is 120.

7. The network entry for 192.168.2.0 /24 is being advertised by RIP and OSPF. Which routing protocol displays the subnet in the routing table and why?

- ❍ **A.** OSPF because it has a lower metric.
- ❍ **B.** RIP because it is classful.
- ❍ **C.** OSPF because it has a lower administrative distance.
- ❍ **D.** RIP because it has a higher administrative distance.

8. Which of the following is not a reason to use static routes?

- ❍ **A.** To minimize configuration in complex networks.
- ❍ **B.** To get finer control of routing decisions.
- ❍ **C.** Destination networks are stubs.
- ❍ **D.** To conserve bandwidth.

9. Given the following entries in a routing table, on which interface will a packet destined for 10.4.0.1 exit?

```
RouterA>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is not set

C    172.16.0.0/16 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
I       10.0.0.0/8 [100/8976] via 172.17.0.2, FastEthernet0/1
D       10.1.0.0/16 [90/2297856] via 192.168.1.10, Serial0/1
D       10.4.0.0/16 [90/2297856] via 192.168.1.10, Serial0/1
O       10.4.0.0/30 [110/65] via 192.168.2.10, Serial0/0
```

- ❍ **A.** Fast Ethernet 0/0
- ❍ **B.** Serial 0/1
- ❍ **C.** Serial 0/0
- ❍ **D.** None of the above

10. Given the following entries in a routing table, which of the following are true? (Choose 2.)

```
RouterA>show ip route
…Ouput Omitted…

Gateway of last resort is 192.168.2.10 to network 0.0.0.0

C    172.16.0.0/16 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
I       10.0.0.0/8 [100/8976] via 172.17.0.2, FastEthernet0/1
D       10.1.0.0/16 [90/2297856] via 192.168.1.10, Serial0/1
D       10.4.0.0/16 [90/2297856] via 192.168.1.10, Serial0/1
S*      0.0.0.0/0 [1/0] via 192.168.2.10, Serial0/0
```

- ❍ **A.** A packet destined for 192.168.100.2 will exit Serial 0/0.
- ❍ **B.** The metric for network 10.4.0.0/16 is 90.
- ❍ **C.** The metric for network 10.0.0.0/8 is 8976.
- ❍ **D.** The routing protocol for network 10.1.0.0 has an administrative distance of 100.

Answers to Review Questions

1. When a packet is destined for a remote network, the Layer 3 source address is the workstation or device that is sending the traffic. The destination Layer 3 address is the IP address of the destination device. At Layer 2, the source address is the MAC address of the sending workstation or device. The destination Layer 2 address, however, is the MAC address of the default gateway. The default gateway is the routing device on the local segment that is responsible for forwarding packets from the local segment to remote networks.
2. Static routes are used primarily in stub networks or when the administrator wishes to have complete control over the routing decisions of their routing devices. Routing protocols are used in complex networks with multiple paths to a destination. Unlike static routes, routing protocols can dynamically react to topology changes in the internetwork.
3. Distance vector routing protocols periodically send routing table updates to their directly connected neighbors regardless of whether there is a change in the topology. These routine routing updates contain the contents of the entire routing table.
4. Link-state routing protocols initially discover their neighbors and retain that information in a neighbor table. Information about all possible routes is exchanged between these neighbors and stored in a router's topology table. After the initial exchange of information, link-state routers periodically send hello messages as opposed to full routing updates. With the knowledge of all possible routes in the topology, the routers calculate the best route to each destination and place them in the routing table.

5. Classful routing protocols do not contain the subnet mask in the routing updates. Networks using classful routing protocols require that a FLSM design does not support discontiguous networks. Classless routing protocols updates contain the subnet mask that enables the network design to support VLSM and discontiguous networks.

Answers to Exam Questions

1. **D.** A packet destined for 192.168.1.34 /24 would require a network entry for 192.168.1.0 in the routing table. Because there isn't an exact match for that network, the router sends it out the interface specified in a default route. This router does not have a default route configured, so the packet will be dropped and an ICMP destination unreachable will be sent to the source. Answer A is incorrect because packets destined for the 10.0.0.0 /8 exit the serial 0/1 interface. Answer B is incorrect because packets destined for the 172.17.0.0 /16 exit the serial 0/0 interface. Answer C is incorrect because packets destined for the 172.16.0.0 /16 exit the Fast Ethernet 0/0 interface.

2. **A**. Because the network is designed with variable-length subnet masks, you should not use a classful routing protocol. B is incorrect because IGP routing protocols should be utilized inside your network. C is incorrect because link-state routing protocols support classless routing updates. D is incorrect because classless routing protocols support VLSM designs.

3. **B**. Link-state routing protocols do not broadcast their entire routing tables. They synchronize their topology table containing all possible routes with the neighbors they initially discover. Answers A, C, and D are all characteristics of link-state routing protocols.

4. **C**. Because the summary route stole three bits from the default Class C (/24), you are summarizing 2^3 or 8 networks. 192.168.16.0 is in an increment of 8, so that is the base network. The range of networks that are summarized extend to network 192.168.23.0 for a total of 8 networks. Answers A, B, and D all fit in the range of networks that are summarized by the 192.168.16.0 /21 summary route.

5. **D**. The default route configured specifies that packets should be routed to the 192.168.10.2 next hop if there is not a specific match in the routing table. Answer A is incorrect because static route entries show up with the letter *S* in the routing table. Answer B is incorrect because by default this is a routing command that can be configured only in Layer 3 devices. `IP default gateway` is the command to configure a gateway of last resort for Layer 2 switches. Answer C is false because static routes are not advertised to other routers.

6. **A, C**. The 3 at the end of the static route command overrides the default administrative distance of 1 for a static route. This is probably being used to create a floating static route in a redundant network. The command, however, does not work because you have an inconsistent subnet mask with the destination network. The network ID should reflect 192.168.1.0 or the subnet mask should be 255.255.255.252. Answer B is incorrect because the 3 represents the administrative distance. Answer D is incorrect because static routes have a default administrative distance of 1.

7. **C**. OSPF has a lower administrative distance than RIP (110 vs. 120), so that entry shows up in the routing table because the lower administrative distance is preferred over higher ones. Answer A is incorrect because the metric of OSPF applies only if the OSPF routing protocol has multiple pathways to the 192.168.2.0 network. Answer B is false because classful or classless is not a factor in decisions between routing sources. Answer D is incorrect routing protocols with lower administrative distances are trusted over routing protocols with higher administrative distances.
8. **A**. Static routes require more configuration in a complex network because you have to configure a static route for each destination in every router.
9. **C**. Because the OSPF entry has the longest match for the 10.4.0.1 network, you use that route out Serial 0/0. Answers B, C, and D are all valid reasons to use static routes.
10. **A, C**. This routing table indicates that a default route is configured. Because there isn't a match for 192.168.100.2 in the routing table, it is sent out Serial 0/0 as specified in the default route. The numbers in the brackets represent the administrative distance followed by the metric. Thus, the remaining correct statement is that the metric for the IGRP route for 10.0.0.0/8 is 8976. Answer B is false because the metric for the 10.4.0.0 /16 network is 2297856. Answer D is incorrect because the 10.1.0.0 /16 network is learned via EIGRP which has an administrative distance of 90.

Suggested Readings and Resources

1. Zinn, Alex. *IP Routing: Packet Forwarding and Intra-domain Routing Protocols*. Addison Wesley Professional, 2002.
2. Kruepke, Keith; Cernick, Paul; Degner, Mark. *Cisco IP Routing Handbook*. Hungry Minds, 2000.
3. Bruno, Anthony and Kim, Jacqueline. *CCDA Exam Certification Guide*. Cisco Press, 2004.
4. "Routing Protocols," www.firewall.cx.
5. "IP Routing," technology support on www.cisco.com.

CHAPTER ELEVEN

11 Distance Vector Routing Protocols

Objectives

This chapter covers the following Cisco-specified objective for the "Technology," "Implementation and Operation," "Planning and Designing," and "Troubleshooting" sections of the Cisco Certified Network Associate exam:

Evaluate the characteristics of routing protocols

Select an appropriate routing protocol based on user requirements

Configure routing protocols given user requirements

Troubleshoot routing protocols

- Each routing protocol is unique, based upon characteristics such as the content of its routing updates, the frequency of its routing updates, and its capability to converge in the face of a topology change.
- Because each routing protocol has varying characteristics, you must choose the right protocol based upon the users' requirements and the existing infrastructure and design.
- By knowing which networks are attached to a router, you can configure either RIP or IGRP to advertise those networks to their adjacent neighbors.
- Using the `show` and `debug` commands, you can determine whether a configuration is correctly configured and whether the routing protocols are operating as they should.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- Keep in mind the characteristics of distance vector routing protocols and how those characteristics apply to RIP and IGRP.
- Complete the Challenge Exercises and the Exercises at the end of the chapter. The exercises will solidify the concepts that you have learned in the previous sections.
- This chapter builds on the concepts discussed in Chapter 10. If you are not completely confident in your comfort with the fundamentals of routing protocols and their metrics, review Chapter 10 again before proceeding with this chapter.
- Complete the Exam Questions at the end of the chapter. They are designed to simulate the type of questions you will be asked in the CCNA exam.

Introduction

The last chapter looked at distance vector routing protocols from a sort of high-altitude overview. Now this chapter brings you closer so you can see the specific protocols that belong to this routing protocol class and explore the unique characteristics and functionality they provide. You will also learn how to configure those routing protocols to meet your administrative needs and how to verify and troubleshoot their operations.

Distance Vector Operations

Objective:

Evaluate the characteristics of routing protocols

To recap, distance vector routing protocols are legacy routing protocols that help routing devices determine the networks that are present in a topology. Using a routing algorithm, known as the Bellman-Ford algorithm, distance vector routing protocols periodically broadcast routing updates consisting of the routing table to directly connected neighbors on adjacent data links, regardless of whether a change has occurred in the topology. When those devices receive that update, they compare it with their existing routing table information. If the distance vector metric for an entry in the routing update is greater (higher) than a current entry in the routing table, it is discarded. If the metric is equal or less, it is added to the routing table with an updated metric to include the path to the advertising neighbor. This entry eventually is passed to the next routing device where the process occurs over again.

NOTE

Many routing protocols, when the metrics on more than one route received by an update are equal, put both entries in the routing table and perform load balancing (transferring packets over both alternate paths).

Because these neighbors base their decisions on information that is not learned first hand, distance vector routing protocol operations are often referred to as *routing by rumor*. In addition, each router in a distance vector routing topology has the same responsibility and function as the next router. In other words, distance vector routers contain flat relationships with each other.

EXAM ALERT

Distance vector routing protocols use the Bellman-Ford algorithm by broadcasting the entire routing table to directly connected neighbors regardless of whether a topology change occurs or not. The information in the update is added and recalculated before being sent to other neighbors.

Consider the example demonstrated in Figure 11.1, which uses a classful distance vector routing protocol such as RIP. Each router contains its directly connected networks in its routing table. Because the routing protocol is classful, the subnetted 192.168.1.0 network has a Fixed Length Subnet Mask (FLSM) design. In addition, the routing table entries contain the metric (hop count for this particular example) indicated by "0" because they are all connected. This is also followed by the interface that packets will exit to reach those networks. Without the use of static routes or routing protocols, the routers can never reach the networks that lie beyond their neighbor routers.

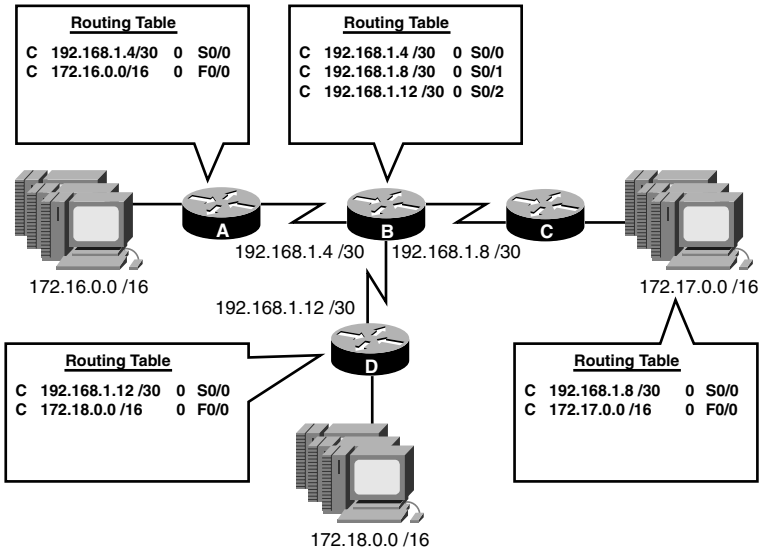


FIGURE 11.1 Distance vector routing initiation.

After you configure and enable a distance vector routing protocol, it advertises the networks in the routing table to its adjacent neighbors. For example, Router A broadcasts a routing update containing the 192.168.1.4 network as well as the 172.16.0.0 network to Router B. As soon as Router B receives that update, it compares the entries in its routing table with the information learned from Router A. Router B already knows about 192.168.1.4 as a directly connected network, so it disregards that entry because the directly connected network has a lower administrative distance than the routing protocol. Because the 172.16.0.0 network is new information, it adds that to its routing table with an updated metric of 1—the 172.16.0.0 network is one hop away through Router A. Similarly, when that entry is advertised to Routers C and D, the metric is updated again to 2 because it is two hops away (through Router B then Router A).

Likewise, Routers A, C, and D receive an update from Router B containing two new networks that will be added to their routing table as two hops away. This process continues until each router has an accurate depiction of all the networks in the domain, as exhibited in Figure 11.2;

in other words, the network will be converged. Despite having achieved full convergence, the routes will still advertise their routing table to their neighbors periodically even if there isn't a change in the topology.

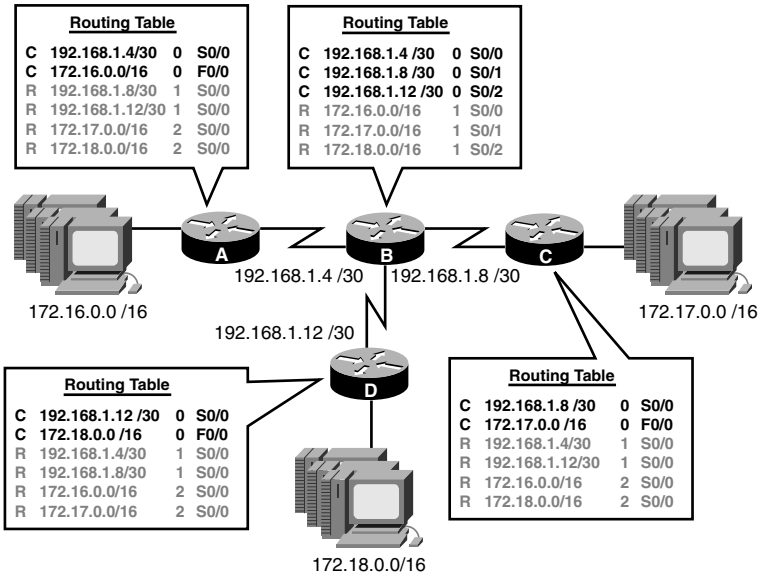


FIGURE 11.2 Distance vector routing converged scenario.

Routing Loops

Objective:

Evaluate the characteristics of routing protocols

One of the major downfalls with routing protocols is the possible occurrence of a routing loop. Routing loops are a stretch of the imagination these days because routing protocols have implemented many measures to mitigate them, but it is still important to examine the plausible historic events that necessitated the need for such measures. Additionally, there are still slim possibilities that these loops can occur regardless of the countermeasures in place.

To demonstrate a routing loop scenario, I will use the existing converged topology and introduce a link failure on Router A as illustrated in Figure 11.3. Notice the routing table in Router A changed to reflect only the remaining connected interface left since its serial link failed. Because the next hop to the protocol-learned networks is down, those entries are removed too. Likewise, Router B removes the connected interface as well as the network entry for 172.16.0.0 because that link and consequently the next hop to that network is down.

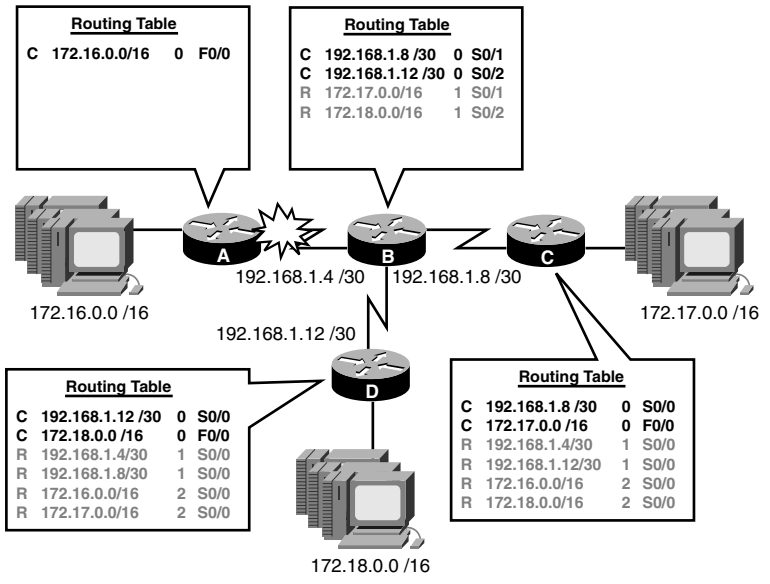


FIGURE 11.3 Link failure scenario.

Imagine in this scenario that Router D sends its periodic update to Router B before Router B can advertise the topology change in its update. When Router B receives the update, it compares the information with its own routing table as distance vector routing protocols typically do. The new subnet information learned in the routing update is added to the routing table. In this unfortunate case, Router B learns (again) about the 172.16.0.0 and the 192.168.1.4 networks and believes they can be reached through Router D (despite Router D originally having learned those routes via Router B). To boot, Router B will add its metric to get to Router D to reach the networks that don't even exist, as reflected in Figure 11.4.

Router B continues to update its neighbor routers periodically with the entries in its routing table. Unfortunately, the unreachable networks appear to be moving away because the hop count inevitably increases between the updates from Router B and Router D for infinity. All the while, poor Router C also is fed false information about these networks from Router B and also has to keep adjusting its metrics as shown in Figure 11.5.

With all three routers containing false information regarding those networks, any packets destined for the 172.16.0.0 and the 192.168.1.4 network are sent to Router D, who in turn, sends them right back to Router B, and so on. These packets will continue to bounce back and forth in the routing loop until the link becomes so saturated, traffic cannot flow between the two routers.

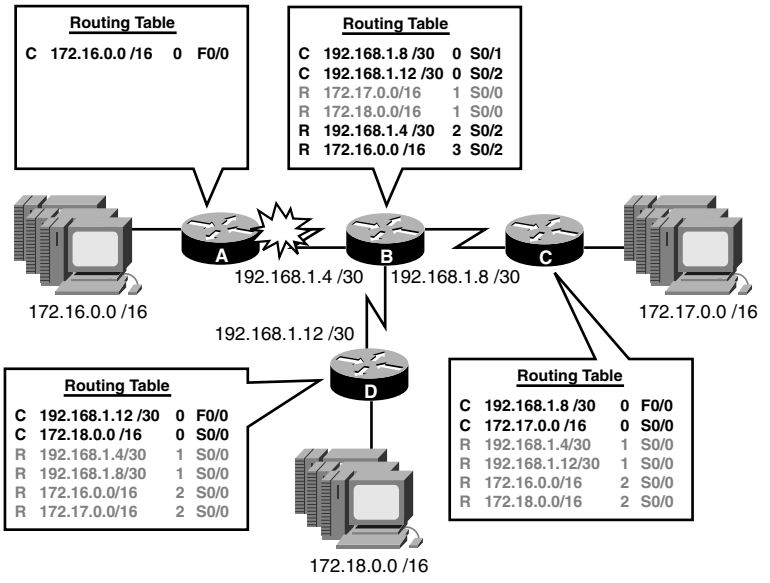


FIGURE 11.4 Incorrect update scenario.

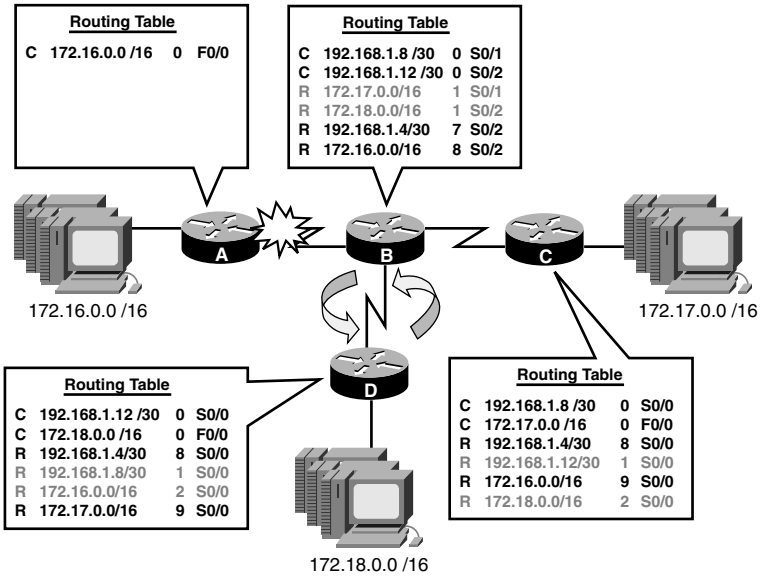


FIGURE 11.5 Routing loop.

Routing Loop Mitigation

To avoid routing loops, distance vector routing protocols have implemented several countermeasures within the routing protocol operations. The following sections describe the preventative measures that have been put in place to mitigate routing loops. For obvious reasons, the majority of these are integrated within the routing protocol and cannot be disabled.

EXAM ALERT

Make sure you remember and comprehend the ways distance vector routing protocols mitigate routing loops.

Count to Infinity

As demonstrated earlier, when routers are continuously passing updates to unreachable networks between each other, the metric continues to increase forever, which is known as *count to infinity*. The easiest way to mitigate this routing protocol side effect is to put a ceiling on the maximum hop count. Using this tactic, routers can determine a network to be unreachable after it reaches the maximum hop count allowed for that protocol. Table 11.1 lists the routing protocols and their maximum hop count values.

TABLE 11.1 Maximum Hop Counts

Protocol	Distance Vector/Link State/Hybrid	Maximum Hop Count
RIPv1	Distance Vector	15
RIPv2	Distance Vector	15
IGRP	Distance Vector	100/255
EIGRP	Hybrid	224
OSPF	Link State	Infinite

Notice that RIP version 1 and 2 both have a maximum hop count of 15, which drastically limits the size of the allowed RIP network. IGRP has a default maximum hop count of 100; however, it can be configured to support up to 255 hops. EIGRP, because it is has some distance vector routing protocol features, has a maximum hop count value of 224. OSPF is a link-state routing protocol that does not use or require a maximum hop count, so it can have an infinite number of hops.

EXAM ALERT

Be sure to remember the maximum hop counts for each protocol.

Split Horizon

Split horizon is similar to that old saying, "Don't ride out on the horse you rode in on." After hearing this little tidbit, if you were to turn around and say back to me that split horizon is similar to that old saying, "Don't ride out on the horse you rode in on," it would get redundant, confusing, and annoying pretty quickly. Such is the case with routing updates.

As you saw earlier, you can get into trouble when routers advertise networks back to the router from which they learned them. Split horizon fixes this dilemma by suppressing those networks in the routing updates being sent back to the source. In other words, split horizon does not advertise networks out the same interface as that from which it learned them.

Take the example shown in Figure 11.6. Because Router D learned about the 192.168.1.4, 192.168.1.8, 172.16.0.0, and 172.17.0.0 subnets from Router B, it does not advertise those networks back to Router B out Serial 0/0. In addition, because it heard Router B advertising the 192.168.1.12 network as well, it does not advertise that back out that interface either. Thus, the only network that Router D will still advertise to Router B is the 172.18.0.0 network because that subnet was not learned via serial 0/0. Now when the link fails on Router A, Router B will not receive a misleading update about the 192.168.1.4 and the 172.16.0.0 networks because Router D and Router C do not advertise those networks back to Router B.

NOTE

Contrary to common belief, when a router advertises a network in a routing update to its neighbors, it adds the metric automatically as shown in Figure 11.6.

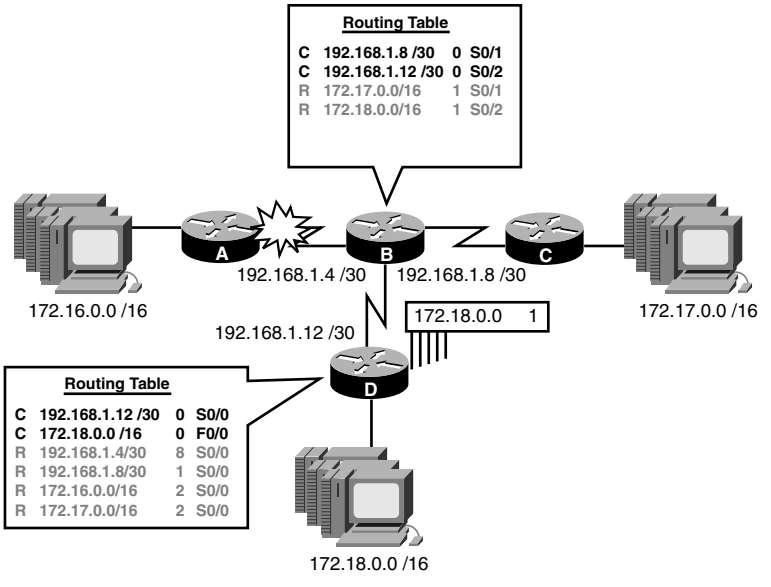


FIGURE 11.6 Split horizon updates.

EXAM ALERT

Make sure you understand the operations involved in split horizon.

Route Poison, Poison Reverse, and Hold-Down Timers

To avoid count to infinity routing loops, a maximum hop count is defined for a routing protocol so the metrics do not increment indefinitely in the event of a routing loop. With route poisoning, the router that recognizes the link failure poisons the affected networks by setting them to an infinite metric for that routing protocol. When that router sends this update to its neighbors, they are notified of the link failure and can update their routing table accordingly.

To illustrate the route poisoning concept, refer to Figure 11.7. Notice in this topology that a redundant route has been added between Router D and Router A. The resultant routing table for Router D now has a route to the 172.16.0.0 network through Router A because it is only one hop count as opposed to two hops through Router B. In addition, notice that Router D has equidistant hops to reach network 192.168.1.4. In this case, Router D keeps both routes in the routing table and load balances between both links for packets destined for that network. When the link fails between Router A and Router B, Router A and Router B set the affected networks to an infinite metric. In this example, because I am using RIP, the maximum hop count is 15, so 16 is an infinite metric.

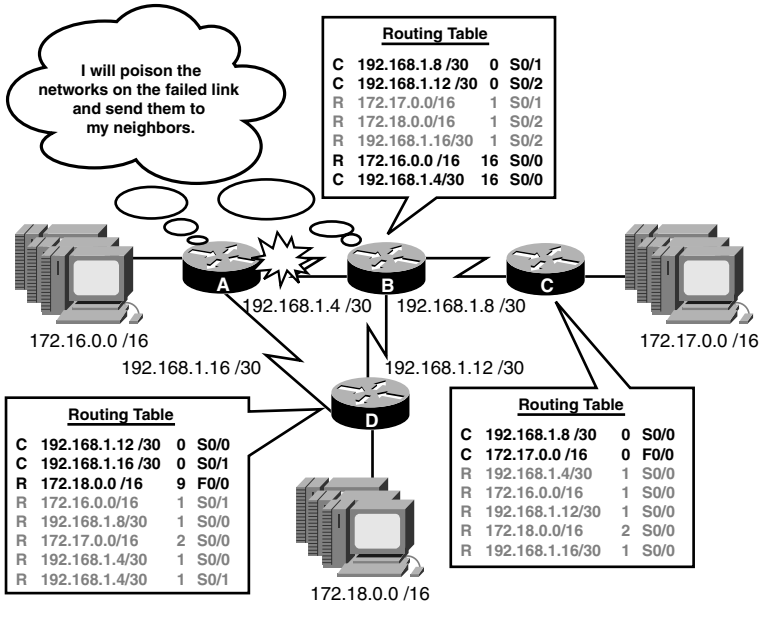


FIGURE 11.7 Route poisoning.

When Routers C and D receive these updates from their neighbors, they can advertise the poisoned network out all their interfaces. With poison reverse, the routers override the split horizon rule and even send the update back to the source, which proves useful as an acknowledgment that those devices are aware of the topology change. At the same time, when Routers C and D receive the poisoned update, they put that network in a "possible down" state in their routing table as illustrated in Figure 11.8. This is the work of the hold-down timer.

Hold-down timers are activated when a router receives a poisoned update from a neighbor indicating that a known network is now inaccessible. To ensure the router does not hastily listen to alternate routes causing yet another routing loop, the router ignores updates with a poorer metric than the original until the hold-down timer expires. This gives the rest of the topology ample time to react to the link change. In the event that an update is received with a better metric than the original route entry, the router discontinues the hold-down timer and uses that entry in its routing table.

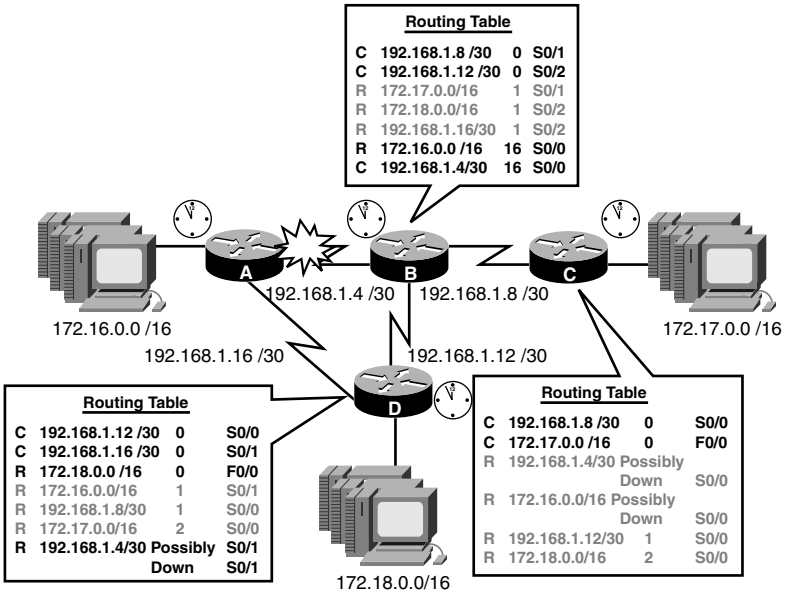


FIGURE 11.8 Hold-down timers.

In Figure 11.8, when Routers A and B poison their route entries and pass them to Routers C and D, those poisoned networks are put in a possible down state and the hold-down timer is activated. In that time, Router B may receive updates from Router D about the 172.16.0.0 network because Router D has an alternate route. However, Router D must wait for the hold-down timer to expire before using the alternate path. For this reason, distance vector routing protocols are considered the slowest routing protocols to converge.

Triggered Updates

One way distance vector routing protocols speed up their convergence while helping avoid routing loops at the same time is something called *flash* or *triggered updates*. Because one of the contributing causes of routing loops is the lack of update information reaching all devices quickly enough, triggered updates enable the router to send the update immediately after a link fails, as opposed to waiting for its periodic update time.

Invalid/Dead Timers

In place of a link failure, what do you suppose would happen if Router A had some operational failures or you removed or changed the routing protocol configuration or networks? Other routers in the domain would not be aware of this change because it isn't a link failure that they can detect and react to. To ensure that these networks are not circulating indefinitely in a routing system, routing protocols have invalid, or dead, timers. If a router stops receiving updates from a router after a set amount of time, that router is considered to be dead and the networks that learned from that router are invalid. Likewise, if a particular network stops advertising with a routing protocol, that entry becomes invalid after the dead timer ages out. This timer is reset every time an update is received from a neighbor for each network in the routing table. When the timer expires, the router poisons the route and advertises that topology change to its neighbors.

TIP

You can clear out aged entries in the routing table quickly by using the `clear ip route` command followed by the network you want to remove.

RIP

The first distance vector routing protocol that is discussed here is coincidentally one of the oldest routing protocols that is still used today. Circa 1988, Routing Information Protocol (RIP) for IP was defined in RFC 1058; however, its roots stem back to the 1970s at Xerox Corporation's Palo Alto Research Center. The following sections look at the characteristics and configurations involved with this resolute routing protocol.

RIP Characteristics

Objective:

Select an appropriate routing protocol based on user requirements

RIP is a fairly simple routing protocol in both characteristics and implementation. You already know that RIP uses hop count as its only metric, in which it can support up to 15 as a maximum. In instances where the metric is identical (for example, equal hop count) for a subnet, it load balances up to six equal paths (four by default). Like other distance vector routing protocols, RIP sends the contents of its routing table to its directly connected neighbors, regardless of whether there is a change or not in the topology. Particularly, RIP's update interval is every 30 seconds and its invalid timer is for 180 seconds. Thus, RIP broadcasts its routing table every 30 seconds and considers a neighbor or a network to be dead after six missed updates.

Because RIP does not advertise subnet masks in its routing updates, it is also a classful routing protocol. Recall that this requires every subnet of a major network to have the same (fixed length) subnet masks. In addition, RIP automatically summarizes subnetted networks to their default classful boundaries when sending the update over a different major network which, in turn, nullifies any support for a discontiguous network design.

As with many routing protocols, RIP requires manual redistribution if you want to advertise networks from a different routing source other than connected interfaces and other RIP-learned networks. One key exception to this is a default route. If you configure a static default route in a router that is running RIP, it automatically redistributes that default route in its routing updates to its neighbors without any additional configuration. The neighbors set that router as their gateway of last resort, assuming a static default route is not configured with a lower administrative distance. The routing table subsequently displays the learned 0.0.0.0/0 subnet as an RIP-learned network.

EXAM ALERT

Remember the characteristics of RIP for the exam.

RIP Configuration

Objective:

Configure routing protocols, given user requirements

The configuration for RIP is seamless as long as you remember these two simple rules:

- Advertise only your directly connected networks.
- Advertise only the classful network.

The first rule is imperative to keep in mind when configuring routing protocols. Remember that the point of the routing protocols is to advertise their known networks to each other so they can build their routing tables. With that being said, do not confuse the configuration of routing protocols with static routes. You do not specify a destination network with routing protocols as you would a static route. Instead, you specify local networks and let the routing protocols advertise them to each other.

Because RIP is a classful routing protocol, the second rule is self-explanatory. Regardless of whether you subnetted major networks into smaller subnets, you have to specify only the subnet to its classful boundary. In other words, you specify the network portion of the IP address and use zeros for the host bits. To recap, the classful boundaries are listed in Table 11.2, in which N represents the network and H represents the host.

EXAM ALERT

It is imperative to know and practice the two rules for configuring RIP.

TABLE 11.2 Classful Network Boundaries

Class	First Octet	Network
A	1–126	N.H.H.H
B	128–191	N.N.H.H
C	192–223	N.N.N.H

To configure RIP and advertise the directly connected classful networks, you must enter the configuration mode for routing protocols, using the `router` keyword in Global Configuration followed by the routing protocol you want to configure. After you are in the routing protocol configuration mode (signified by the `(config-router)#` prompt), you specify the directly connected classful networks by using the `network` command. If you need to remove a specific network from being advertised, you need to enter the RIP routing process again and type **`no`** followed by the keyword **`network`** and the network number you want to remove.

Using Figure 11.9 as an example, Routers A, C, and D each have two directly connected networks while Router B has three. To configure RIP to advertise the routing protocols, the configuration for Router A would look like the following:

```
RouterA(config)#router rip
RouterA(config-router)#network 172.16.0.0
RouterA(config-router)#network 192.168.1.0
```

TIP

If you accidentally configure a network at the incorrect classful boundary, the IOS configuration automatically changes your configuration statement(s) to reflect the classful network.

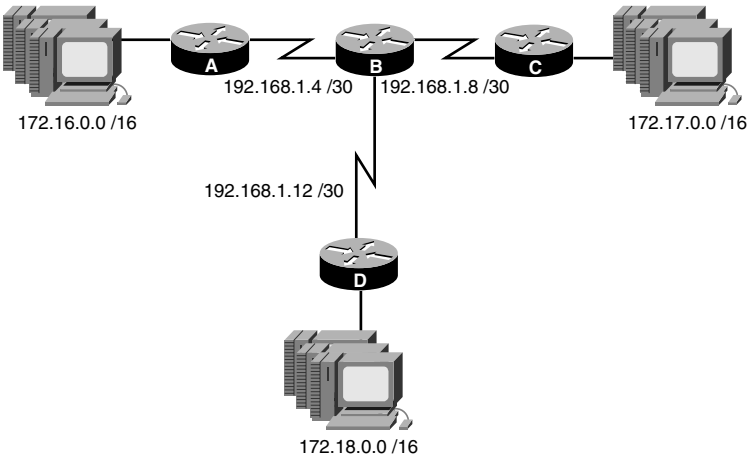


FIGURE 11.9 RIP configuration scenario.

EXAM ALERT

Be prepared to configure a routing protocol given a network topology. Even though there is the IOS support to autocorrect your mistakes when entering the networks as mentioned in the preceding Tip, do not rely on the exam to allow that as a correct answer.

Because Router A has the 172.16.0.0 network and the 192.168.1.4 network attached to it, the classful networks that are advertised are 172.16.0.0 because it is a Class B, and 192.168.1.0 because that network is a Class C. You do not need to include any other network statements because the routers will advertise each other's networks. After you define the networks with the `network` command, RIP begins to advertise and listen for updates on those interfaces that are contained in that classful network. For instance, if you did not configure the `network 192.168.1.0` statement in Router A, you would never be able to send and receive updates on the serial interface, which would entail that Router B would never learn of the 172.16.0.0 network and Router A would never learn of the other networks in the topology.

EXAM ALERT

Keep in mind that the routing protocol does not listen to or learn from advertisements on an interface unless you include their respective networks in the routing protocol process with the `network` command.

Router B has three directly connected 192.168.1.x networks, so how many statements do you think you must configure for Router B to participate in RIP updates? Despite having three networks, you must advertise the classful networks in the RIP configuration; thus, you require only one statement for the 192.168.1.0 network that will, in essence, encompass all three subnets. To see the configurations for each router in this topology, direct your attention to Figure 11.10.

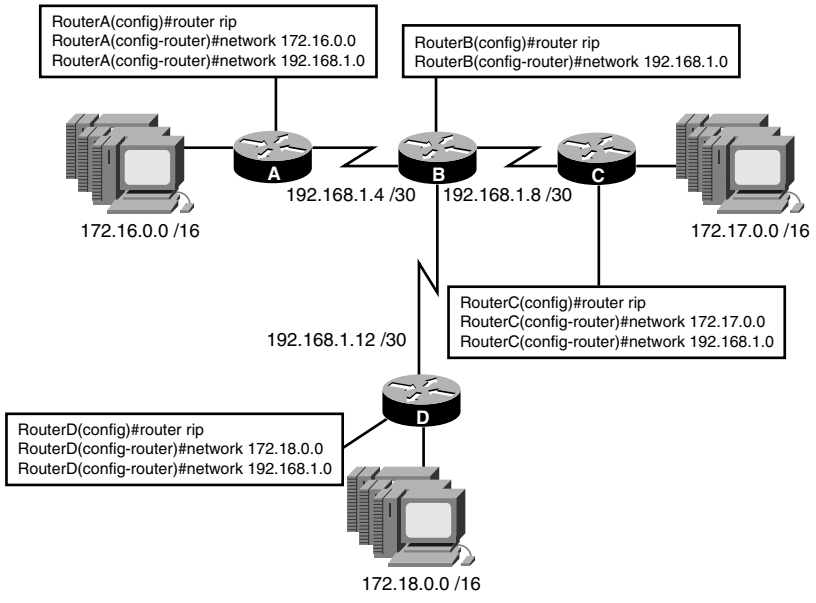


FIGURE 11.10
Completed RIP configuration scenario.

If you want to change the number of allowed equal paths to load balance with RIP, you can use the `maximum-paths` command in the routing process. For example, if you wanted to change the maximum paths to 6 equal paths, the configuration would look like the following:

```
RouterA(config)#router rip
RouterA(config-router)#maximum-paths 6
```

TIP

To disable load balancing over multiple equal paths, set the maximum paths to 1.

RIPv2 Characteristics

Objective:

Select an appropriate routing protocol based on user requirements

In an attempt to keep up with modern needs from a routing protocol, RIP version 2 was created in 1994 to address many of the shortcomings of its predecessor. Many of the characteristics are similar to RIPv1; nonetheless, RIPv2 had some significant improvements:

- **Multicast Updates**—Rather than broadcast its routing updates, RIPv2 uses a reserved multicast address of 224.0.0.9 to communicate with other RIPv2 neighbors. By using a multicast address, it does not waste the processing resources of non-RIP devices because only RIPv2 devices process messages to that address.

- **Classful or Classless Support**—RIPv2 is classful by default, but can be configured as a classless routing protocol, which allows for subnet masks to be sent in the routing updates. The implication of this enhancement entails that RIPv2 can support VLSM and discontiguous network designs.
- **Authenticated Updates**—To ensure the origin of the routing update and protect from attackers spoofing routing updates, RIPv2 allows update authentication in which the passwords must match in all routers to validate the routing update.

EXAM ALERT

Be sure to remember the enhancements that RIPv2 holds over RIPv1.

RIPv2 Configuration

Objective:

Configure routing protocols given user requirements

The configuration for RIPv2 is practically identical to RIPv1. In other words, you still must enter the RIP routing process with the `router rip` command and still must advertise the directly connected classful networks. To enable RIPv2, you have to type the command, **`version 2`**, in the routing process as follows:

```
RouterA(config)#router rip
RouterA(config-router)#version 2
RouterA(config-router)#network 172.16.0.0
RouterA(config-router)#network 192.168.1.0
```

By default, RIPv2 is classful. To configure this enhanced routing protocol to support classless routing updates, the only entry you need to configure is the `no auto-summary` command in the routing process as shown here:

```
RouterA(config)#router rip
RouterA(config-router)#no auto-summary
```

RIP Verification

Objective:

Troubleshoot routing protocols

To verify RIP, you can use an assortment of `show` commands, each equally contributing to a wealth of information about the RIP routing protocol you configured. For instance, `show`

`running-config` is an easy pick to show your configuration for RIP and the networks that you have configured. It is also a useful starting point if you are troubleshooting an existing implementation of RIP and suspect missing or misconfigured network statements.

To ensure that RIP updates are being received from neighbors, `show ip route` proves the network configuration is functioning because you will see RIP entries appear in the routing table as follows:

```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is not set

R    172.17.0.0/16 [120/1] via 192.168.1.6, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
R    172.18.0.0/16 [120/1] via 192.168.1.6, Serial0/0
     192.168.1.0/30 is subnetted, 3 subnets
R       192.168.1.8 [120/1] via 192.168.1.6, Serial0/0
R       192.168.1.12 [120/1] via 192.168.1.6, Serial0/0
C       192.168.1.4 is directly connected, Serial0/0
```

The RIP entries are identified in the routing table with the letter *R* followed by the default administrative distance and the hop count in brackets. The IP 192.168.1.6 is the next-hop address to reach those networks out of Serial 0/0.

Finally, to see detailed information regarding all the IP routing protocols configured on a routing device, use the `show ip protocols` to see a plethora of information, as illustrated in Figure 11.11. In this output, you can see the timers involved with the routing protocol, including the update interval of 30 seconds and the invalid and hold-down timers. In addition, you can see which networks you are routing. This is useful for administrators who do not have access to Privileged EXEC (therefore are not able to use the `show running-config` command) to verify which networks are being advertised.

```
RouterA#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 19 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface         Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0   1     1 2
    Serial0/0         1     1 2
  Routing for Networks:
    172.16.0.0
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.6           120      00:00:15
  Distance: (default is 120)

RouterA#
```

FIGURE 11.11 `show ip route` RIP entries.

Troubleshooting RIP

Troubleshooting routing protocols always begins with verification of the routing configuration and status by using the `show` commands discussed in the last section. You can also test whether you have IP connectivity by pinging or you can test the route packets will take by using the `traceroute` command. However, if you need to get into the trenches, so to speak, and verify the updates as they are being sent and received, you need to use real-time troubleshooting tools entailing the `debug` command.

TIP

If you forget which debug processes you have running, you can issue the `show debug` command to list all the processes you are currently debugging.

To actively see real-time updates as they are being sent and received for RIP, use the Privileged EXEC command, `debug ip rip`, as demonstrated in the three sections in Figure 11.12.

In the first section, labeled 1, the router is receiving an update from a neighbor with the IP address 192.168.1.6. If there are any new subnets learned from this update, they ultimately are placed in the routing table, using 192.168.1.6 as the next-hop address and Serial 0/0 as the exiting interface because that is where this information was learned. Notice in this section that there are no subnet masks received in the update, solidifying that fact that you are running a classful routing protocol, RIPv1.

```
RouterA#debug ip rip
RIP protocol debugging is on
RouterA#
00:26:27: RIP: received v1 update from 192.168.1.6 on Serial0/0
00:26:27:      192.168.1.8 in 1 hops                                    1
00:26:27:      192.168.1.12 in 1 hops
00:26:27:      172.17.0.0 in 2 hops
00:26:27:      172.18.0.0 in 2 hops
00:26:41: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (172.16.0.1)
00:26:41: RIP: build update entries
00:26:41:       network 172.17.0.0 metric 3                             2
00:26:41:       network 172.18.0.0 metric 3
00:26:41:       network 192.168.1.0 metric 2
00:26:41: RIP: sending v1 update to 255.255.255.255 via Serial0/0 (192.168.1.5)
00:26:41: RIP: build update entries                                     3
00:26:41:       network 172.16.0.0 metric 1
RouterA#undebug all
All possible debugging has been turned off
```

FIGURE 11.12 `debug ip rip` output.

Section 2 is the local router broadcasting (255.255.255.255) an update out its Fast Ethernet 0/0 interface. Most importantly, notice how the router increments the hop count by 1 before sending it out to any neighbors on its LAN. Also, take note of the 192.168.1.0 entry that is being advertised out this interface. Because the interface has an IP address of 172.16.0.1, which is not in the same major network, this router automatically summarized its subnetted entries to 192.168.1.0.

The information shown in section 3 is proof that split horizon is enabled and working on this router. This is evident because the router does not send any entries that it received in the first section of Figure 11.12. Recall that split horizon inhibits a router from advertising networks back out the interface from which it received that information. Because the 192.168.1.8, 192.168.1.12, 172.17.0.0, and 172.18.0.0 networks were received in the router's Serial 0/0 interface, they cannot be sent back out that interface.

EXAM ALERT

Be sure you are able to decipher the output of a `debug ip rip` command.

Challenge

Given the following design in Figure 11.13, you are going to configure RIP on Router A to be able to communicate with the remainder of the pre-configured network.

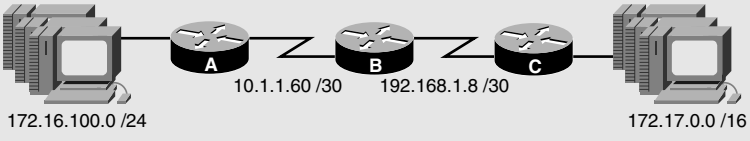


FIGURE 11.13 RIP configuration challenge.

1. Remember to remove any existing static routes. Why?
2. Enter the configuration process for RIP.
3. Advertise Router A's networks.
4. What will Router B do with the update from Router A?
5. What will the networks look like when Router B sends them on to Router C?
6. Configure Router A to run RIP version 2.
7. Configure Router A to be classless.
8. What will the update from Router A look like now?

Challenge Answer

You must first remove any static routes because they have a lower administrative distance than RIP. The configuration in steps 2 and 3 would look like the following:

```
RouterA(config)#router rip
RouterA(config-router)#network 172.16.0.0
RouterA(config-router)#network 10.0.0.0
```

Despite having subnetted the major networks in our topology, you must advertise the directly connected classful networks. When Router B receives that update, it adds the 172.16.0.0 entry into its routing table (because 10.1.1.60 is already directly connected) with a metric of 1 and uses Router A's serial interface as the next hop. The entry is not 172.16.100.0 because Router A auto-summarizes that network when exiting its WAN interface because that is on a different major network. When Router B sends that entry to Router C, it is sent as 172.16.0.0 with a metric (hop count of 2).

To configure Router A for RIPv2 and make it classless, you must add the following configurations:

```
RouterA(config)#router rip
RouterA(config-router)#version 2
RouterA(config-router)#no auto-summary
```

With this configuration, Router A does not automatically summarize the 172.16.100.0 network and it sends the subnet mask along to Router B. If B is running RIPv2 also, it keeps the network in its subnetted form of 172.16.100.0/24.

IGRP

Shortly after RIPv1 was standardized, Cisco created its own proprietary distance vector routing protocol that addressed many of the shortcomings and oversimplifications with RIP. Introduced in the mid-1980s, Interior Gateway Routing Protocol (IGRP) was created by Cisco in the hopes that despite being proprietary, it would rapidly be accepted and become the de facto routing protocol used in networks. The following sections expound on the improved features that IGRP offers over RIP.

IGRP Characteristics

Objective:

Select an appropriate routing protocol based on user requirements

One of the most notable improvements that IGRP offers over RIP is the use of a robust composite metric. Specifically, IGRP uses bandwidth and delay by default as its metric to determine the best routing path to a destination. In addition, you can configure IGRP to include

additional metrics such as reliability, load, and MTU. By using this more robust composite metric (as opposed to using hop count), routers can accurately determine the best path to take to a destination. Speaking of hop count, IGRP can support larger networks than RIP because its maximum hop count is 100 by default, and can be configured up to 255.

EXAM ALERT

Remember that IGRP uses bandwidth and delay by default, but can be configured to include reliability, load, and MTU for its composite metric.

For example, given the example in Figure 11.14, RIP would take the T1 link as the best route to reach 172.17.0.0 because it has the lowest number of hops. IGRP, on the other hand, considers the bandwidth of the links and determines that the bottom path is the optimal route because the ethernet links combined are still faster than a single TI of 1.54Mbps.

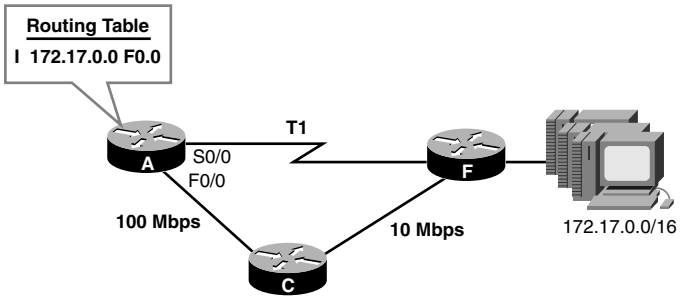


FIGURE 11.14 IGRP composite metric in action.

IGRP's update interval is 90 seconds as compared to RIP's 30 seconds. This decreases the amount of utilization and bandwidth required to send these updates because they do not occur as frequently as RIP. In the rare case that a Cisco router should fail, or more likely its neighbor routers stop advertising a network, IGRP waits 270 seconds before considering the network to be invalid. When a router wants to poison the route, it sets the metric to IGRP's infinite metric value of 4,294,967,295.

As you will see, because IGRP metrics can vary considerably depending on the bandwidth and delay of the links to the destination, IGRP also can support load balancing up to six unequal paths (as opposed to RIP's equal paths). The only downfall for IGRP, unfortunately, is that because of its proprietary nature, IGRP must be implemented in an all-Cisco network.

TIP

IGRP is no longer supported in version 12.3.

IGRP Configuration

Objective:

Configure routing protocols given user requirements

IGRP must follow the same configuration guidelines as RIPv1. Namely, it must advertise the directly connected networks; and because IGRP is also classful, the networks configured must be at a default classful boundary. A key element that differs in the RIP configuration is the inclusion of an autonomous system (AS) number in the routing process configuration. This AS number is an arbitrary number between 1 and 65535 that you or your network administrator assigns to your network. It is imperative that you make this number match in all your router configurations or the routers will ignore the routing updates.

EXAM ALERT

Be sure that the autonomous system number must match in every router that you configure or else the updates will be ignored.

Figure 11.15 displays an example of an IGRP topology using the chosen autonomous system number 100. To configure Router A, the configuration is similar to the RIP configuration except that you must specify the AS number after the `router igrp` command, as illustrated here:

```
RouterA(config)#router igrp 100
RouterA(config-router)#network 172.16.0.0
RouterA(config-router)#network 192.168.100.0
```

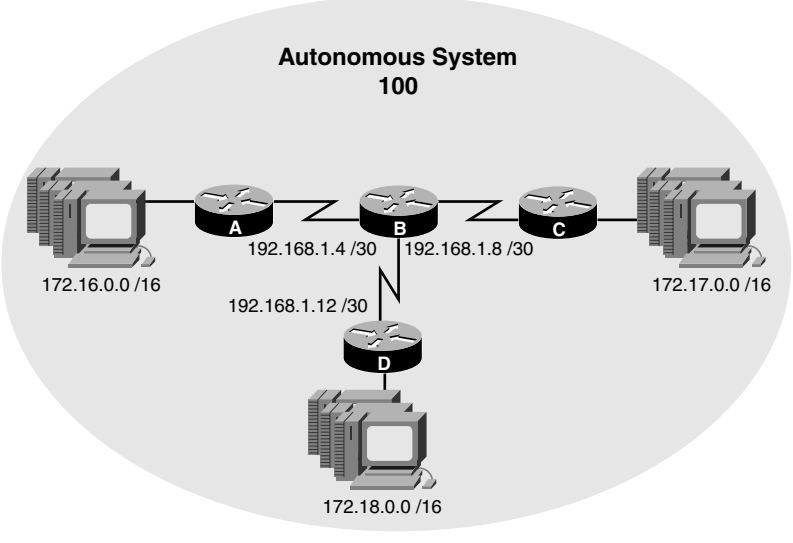


FIGURE 11.15 IGRP configuration scenario.

In Routers B, C, and D, the configuration must have the same autonomous system number or else the updates from neighbor routers are ignored.

The Bandwidth Bandwagon

Because IGRP utilizes bandwidth as one of its metrics in determining the best path to a destination, it is imperative that the routers accurately depict the bandwidth that is currently on their interfaces. Because the ethernet and Fast Ethernet interfaces automatically define the bandwidth of their interfaces, you do not have to worry about any additional configurations on the LAN interfaces.

WAN interfaces, such as serial, asynchronous serial, and HSSI, can have varying speeds depending on the WAN circuits to which they are connected. For instance, it is possible to have a 64Kbps link connected to one serial interface and T1 connected to another. By default, the Cisco IOS automatically assumes that any circuit connected to a serial interface is T1 (1544Kbps) speed, so how are you to tell the IGRP of a link speed that is less than T1? The answer is by using the `bandwidth` interface command followed by the bandwidth in Kbps as discussed in Chapter 7, "Basic Cisco Configurations." By specifying the actual bandwidth on the interface, IGRP incorporates that information in its metrics and can make accurate routing decisions based upon the proper speeds of the links.

Unequal Path Load Balancing

One of the outstanding features of IGRP is its capability to load balance up to six unequal paths (four by default). To achieve this remarkable feat, you must configure a multiplier based upon the lowest composite metric to a destination. The command for this multiplier is the `variance` command, which is configured in the IGRP routing process.

For instance, Figure 11.16 illustrates a simplified topology with the composite metrics to reach 172.17.0.0. In its default state, IGRP would choose the router through Router B because that has the lowest cumulative composite metric to reach the destination network. Because the path through B and C has a metric of 80, and the path through D and E has a metric of 160, you can specify a variance of 2, which acts as a multiplier of the lowest metric (80 in this case). The configuration for this would look like the following:

```
RouterA(config)#router igrp 100
RouterA(config-router)#variance 2
```

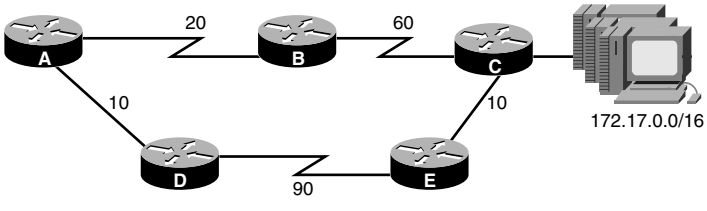


FIGURE 11.16 Unequal path load balancing with variance command.

TIP

The variance multiplier does not have to be an exact multiplication. If the multiplied value happens to go over the highest composite metric to a destination, it still load balances over any path that is included in the range.

IP Default-Network

Unlike RIP, IGRP does not automatically redistribute default routes to downstream neighbors in its routing updates. As an alternative, you can configure a default network that informs downstream neighbors to reach the network specified as a gateway of last resort. This does not, however, configure a default route or a gateway of last resort in the router that it is configured.

The syntax to configure a default network is the `ip default-network` command in global configuration. The network that you specify must already be a subnet that is present in the routing table. Downstream neighbors will set their network as their gateway of last resort and determine the fastest way to reach it via their routing protocol. For example, if you wanted to use the 192.168.1.0 network in your routing table as a gateway of last resort for downstream neighbors receiving your IGRP updates, the configuration would resemble the following:

```
RouterA(config)#ip default-network 192.168.1.0
```

IGRP Verification

Objective:

Troubleshoot routing protocols

The commands used to verify the RIP configuration (`show running-config`, `show ip route`, and `show ip protocols`) are exactly the same commands to use when verifying IGRP. For instance, the following is the output of the `show ip route` command with IGRP entries present in the routing table:

```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route
```

```
Gateway of last resort is not set

I    172.17.0.0/16 [100/16576] via 192.168.1.6, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
I    172.18.0.0/16 [100/16576] via 192.168.1.6, Serial0/0
     192.168.1.0/30 is subnetted, 3 subnets
I       192.168.1.8 [100/8976] via 192.168.1.6, Serial0/0
I       192.168.1.12 [100/8976] via 192.168.1.6, Serial0/0
C       192.168.1.4 is directly connected, Serial0/0
```

This time, the IGRP routes appear with the letter *I* to designate networks that were learned via neighbor routers using IGRP. Once again, the numbers in the brackets signify the administrative distance (100 for IGRP), followed by IGRP's composite bandwidth and delay metric to reach the destinations.

The `show ip protocols` once again display the timers and the networks that are being advertised by the routing protocol, as shown in Figure 11.17. In addition, the output of this command also displays the K weight values that determine which metrics are used in the calculation of the best path (which equals out to bandwidth + delay by default because the other K values are 0). The `show ip protocols` for IGRP also display the default values for the maximum hop count of IGRP (100) and the variance multiplier (1 = no unequal load balancing).

```
RouterA#show ip protocols
Routing Protocol is "igrp 100"
  Sending updates every 90 seconds, next due in 49 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing: igrp 100
  Routing for Networks:
    172.16.0.0
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.6           100     00:01:04
  Distance: (default is 100)
```

FIGURE 11.17 `show ip protocols` IGRP output.

Troubleshooting IGRP

Once again, your troubleshooting should begin with the `show` commands described in the previous section, as well as with the `ping` and `traceroute` commands. In addition, IGRP has a set of `debug` commands that can be used to display the routing information to your management session. As with all debugging commands, please use these commands with extreme caution and verify your router's current utilization with the `show processes` command before you debug routing updates.

The `debug ip igrp transactions` command is similar to the output of the `debug ip rip` command in that it shows a detail of all the routing updates begin sent and received. Once again, you can see in Figure 11.18 that IGRP is classful because there are no subnet masks

contained in the updates. In addition, split horizon is suppressing the router from advertising the networks learned from the neighbor router back out of serial 0/0.

```
RouterA#debug ip igrp transactions
IGRP protocol debugging is on
RouterA#
05:52:02: IGRP: sending update to 255.255.255.255 via FastEthernet0/0 (172.16.0.1)
05:52:02:       network 172.17.0.0, metric=8576
05:52:02:       network 172.18.0.0, metric=8976
05:52:02:       network 192.168.1.0, metric=8476
05:52:02: IGRP: sending update to 255.255.255.255 via Serial0/0 (192.168.1.5)
05:52:02:       network 172.16.0.0, metric=110
05:52:04: IGRP: received update from 192.168.1.6 on Serial0/0
05:52:04:       subnet 192.168.1.8, metric 8976 (neighbor 501)
05:52:04:       subnet 192.168.1.12, metric 8976 (neighbor 501)
05:52:04:       network 172.17.0.0, metric 8576 (neighbor 1100)
05:52:04:       network 172.18.0.0, metric 8976 (neighbor 501)
RouterA#undebug all
All possible debugging has been turned off
```

FIGURE 11.18 `debug ip igrp transactions` output.

If the output from your `show processes` command indicates that your router is highly utilized, you might want to use the `debug ip igrp events` command instead. This command gives only a summary of the updates that are being sent and received, such as those shown in Figure 11.19, so it is not as taxing for the router to display.

```
RouterA#debug ip igrp events
IGRP event debugging is on
RouterA#
05:53:17: IGRP: received update from 192.168.1.6 on Serial0/0
05:53:17: IGRP: Update contains 2 interior, 2 system, and 0 exterior routes.
05:53:17: IGRP: Total routes in update: 4
05:53:20: IGRP: sending update to 255.255.255.255 via FastEthernet0/0 (172.16.0.1)
05:53:20: IGRP: Update contains 0 interior, 3 system, and 0 exterior routes.
05:53:20: IGRP: Total routes in update: 3
05:53:20: IGRP: sending update to 255.255.255.255 via Serial0/0 (192.168.1.5)
05:53:20: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
05:53:20: IGRP: Total routes in update: 1
RouterA#undebug all
All possible debugging has been turned off
```

FIGURE 11.19 `debug ip igrp events` output.

Chapter Summary

This chapter discussed the two main distance vector routing protocols, RIP and IGRP. Both routing protocols are susceptible to routing loops and have several countermeasures in place to help mitigate these anomalies. For instance, both routing protocols have a maximum hop count to ensure that routing loops do not cause routers to increment the metric for infinity, and define a reasonable limit on the size of the network to which the routing protocol can scale. Split horizon contributes in the mitigation of routing loops by ensuring that routers do not advertise networks out the same interface as that on which those networks were learned. When a link fails, distance vector routing protocols poison the affected routes by setting them to an infinite metric and immediately shoot them out as a flash or triggered update. The split horizon rule is overridden in this instance to send a notice that the link is possibly down. The link remains in that state (unless it receives an update that has a better metric than the original network entry) until the hold-down timer expires. After the hold-down timer lapses, the router can use routes with less favorable metrics than the original.

Table 11.3 is a summary of the characteristics of both versions of RIP and IGRP.

TABLE 11.3 RIP and IGRP Comparison

	RIPv1	RIPv2	IGRP
Classful/Classless	Classful	Both	Classful
Algorithm	Bellman-Ford	Bellman-Ford	Bellman-Ford
Metric	Hops	Hops	Composite (Bandwidth+Delay)
Maximum Hop Count	15	15	100/255
Infinite Metric	16	16	4,294,967,295
Update/Invalid	30/180	30/180	90/270
Updates	Broadcast	Multicast (224.0.0.9)	Broadcast
Load Balancing	Equal Paths	Equal Paths	Unequal Paths

To configure RIP and IGRP, you must enter the routing process first with the `router` keyword in Global Configuration mode followed by the routing protocol. In the case of IGRP, you must also specify an autonomous system number that must match in all routers under your administrative control. After you are in the routing process, you advertise the networks with the `network` command followed by the directly connected classful networks.

To verify the routing process for RIP and IGRP, you can use the `show ip route` command to view the IP routing table and examine whether networks have been learned from the routing protocol. In addition, `show ip protocols` displays the networks you are advertising in the local router, as well as the timers for each IP routing protocol.

When performing real-time troubleshooting, you can use the `debug ip rip` command for RIP and `debug ip igrp transactions` or `debug ip igrp events` for IGRP. Be sure that

you do not use these commands on a production router that is reporting high CPU utilization from the `show processes` output.

Key Terms

- Bellman-Ford algorithm
- count to infinity
- route poison
- poison reverse
- hold-down timers
- triggered updates
- RIP
- RIPv2
- IGRP
- autonomous system number
- variance

Apply Your Knowledge

Exercises

11.1 Configure IGRP Router A

In this exercise and the next, you will configure IGRP between two routers.

NOTE

This exercise assumes you have two non-production routers with a DCE to DTE serial cable or simulated software. If you do not have these on hand, write out what the configurations would look like.

Estimated Time: 20 minutes

1. Enter Privileged EXEC on Router A.
2. Enter Global Configuration.
3. Configure and enable the ethernet interface on Router A to have an IP address of 192.168.1.1/24.
4. Configure and enable the serial interface on Router A to have an IP address of 10.1.1.1/30.
5. Configure the clock rate (if this is the DCE) for 64000 bits per second.
6. Configure a bandwidth statement to reflect this speed on the serial interface.
7. Enter the routing process for IGRP, using 7 as the AS number.
8. Advertise the directly connected classful networks.

11.2 Configure IGRP Router B

Now that Router A is configured, you must configure its neighbor, Router B, to send and receive routing updates.

Estimated Time: 20 minutes

1. Enter Privileged EXEC on Router B.
2. Enter Global Configuration.
3. Configure and enable the ethernet interface on Router B to have an IP address of 172.16.30.1/24.
4. Configure and enable the serial interface on Router B to have an IP address of 10.1.1.2/30.
5. Configure the clock rate (if this is the DCE) for 64000 bits per second.
6. Configure a bandwidth statement to reflect this speed on the serial interface.
7. Enter the routing process for IGRP, using 7 as the AS number.
8. Advertise the directly connected classful networks.

11.3 Verify Routing

If configured correctly, you should be able to verify your IGRP routing in this exercise.

1. In both Router A and Router B, do a `show ip protocols` to verify the networks that you are advertising.
2. Do a `show ip route` and verify you have an IGRP entry in your routing table from your neighbor.
3. If statements are missing, troubleshoot the routing process by using the `debug ip igrp transactions`.

Review Questions

1. What are the mitigation methods distance vector routing protocols use to avoid routing loops?
2. What are the characteristics of RIP?
3. What additional features are present in RIPv2 that are not present in RIP?
4. What are the characteristics of IGRP?
5. What are the fundamental configuration steps for RIP and IGRP?

Exam Questions

1. Given the following output, which of the following is a true statement?

```
CstmrARtr#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

R    1.0.0.0/8 is possibly down, routing via 192.168.1.9, Serial0
C    172.17.0.0/16 is directly connected, Ethernet0
R    172.16.0.0/16 [120/1] via 172.17.0.2, 00:00:19, Ethernet0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.8 is directly connected, Serial0
```

   - ❍ **A.** The 172.16.0.0 has an administrative distance of 1.
   - ❍ **B.** The 1.0.0.0 network is in a hold-down state.
   - ❍ **C.** The configuration for this router to advertise RIP should have a network 172.16.0.0 and a network 1.0.0.0 statement.
   - ❍ **D.** None of the above.

2. Given the following exhibit, what statement is false regarding the 0.0.0.0/0 network?

```
CstmrARtr#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is 192.168.1.9 to network 0.0.0.0

R    1.0.0.0/8 [120/1] via 192.168.1.9, 00:00:21, Serial0
C    172.17.0.0/16 is directly connected, Ethernet0
R    172.16.0.0/16 [120/1] via 172.17.0.2, 00:00:02, Ethernet0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.8 is directly connected, Serial0
R*   0.0.0.0/0 [120/1] via 192.168.1.9, 00:00:21, Serial0
```

- ❍ **A.** The 0.0.0.0 network was statically configured in this router.
- ❍ **B.** The gateway of last resort is the 192.168.1.9 router.
- ❍ **C.** The default route was advertised to the local router via RIP.
- ❍ **D.** The default route was automatically redistributed in Router 192.168.1.9.

3. Based upon the following output, which network may not show up in the routing table?

```
RouterA#debug ip rip
RIP protocol debugging is on
RouterA#
00:26:27: RIP: received v1 update from 192.168.1.6 on Serial0/0
00:26:27:      192.168.1.8 in 12 hops
00:26:27:      192.168.1.12 in 15 hops
00:26:27:      172.17.0.0 in 14 hops
00:26:27:      172.18.0.0 in 16 hops
```

- ❍ **A.** 172.17.0.0
- ❍ **B.** 192.168.1.8
- ❍ **C.** 192.168.1.12
- ❍ **D.** 172.18.0.0

4. Which two commands enable a distance vector routing protocol to be classless? (Choose 2.)

- ❍ **A.** `version 2`
- ❍ **B.** `variance 2`
- ❍ **C.** `no auto-summary`
- ❍ **D.** `router classless`

5. Which command enables unequal load balancing over all three links with the following metrics: Network A-234, Network B-23, and Network C-601?

- ❍ **A.** `variance 10`
- ❍ **B.** `variance 3`
- ❍ **C.** `variance  30`
- ❍ **D.** `variance 25`

6. Given the following two configurations, what would be the result?

```
RouterA(config)#router IGRP 200
RouterA(config-router)#network 172.17.0.0
RouterA(config-router)#network 192.168.34.0

RouterB(config)#router IGRP 100
RouterB(config-router)#network 172.18.0.0
RouterB(config-router)#network 192.168.34.0
```

   - ❍ **A.** Router A will add the 172.18.0.0 network to its routing table.
   - ❍ **B.** Router B will not add the 192.168.34.0 network because it is advertising it to Router A.
   - ❍ **C.** The routing updates will contain the subnet masks.
   - ❍ **D.** Router A and Router B will ignore each other's updates.

7. Given the following output of a `debug ip igrp transactions`, which of the following is false?

```
00:46:56: IGRP: received update from 192.168.1.6 on Serial0/0
00:46:56:       subnet 192.168.1.8, metric 8976 (neighbor 501)
00:46:56:       subnet 192.168.1.12, metric 8976 (neighbor 501)
00:46:56:       network 172.17.0.0, metric 8576 (neighbor 1100)
00:46:56:       network 172.18.0.0, metric 8976 (neighbor 501)
00:46:32: IGRP: sending update to 255.255.255.255 via Serial0/0 (192.168.1.5)
00:46:32:       network 172.17.0.0, metric=8576
00:46:32:       network 172.18.0.0, metric=8976
00:46:32:       exterior 192.168.1.0, metric=8476
00:46:32:       network 172.16.0.0, metric=110
00:46:32:       subnet 192.168.1.12, metric 8976
```

   - ❍ **A.** Split horizon is enabled.
   - ❍ **B.** The metric uses bandwidth + delay in its calculation to determine the best path to the destination network.
   - ❍ **C.** The routing protocol used is classful.
   - ❍ **D.** The routes in the update are not poisoned.

8. Which command should you implement before doing any `debug` commands?

   - ❍ **A.** `show running-config`
   - ❍ **B.** `show processes`
   - ❍ **C.** `undebug all`
   - ❍ **D.** `copy running-config startup-config`

9. Given the following output of a `debug ip rip`, which of the following is true?

```
00:57:27: RIP: received v2 update from 192.168.1.6 on Serial0/0
00:57:27:      192.168.1.8/30 via 0.0.0.0 in 1 hops
00:57:27:      192.168.1.12/30 via 0.0.0.0 in 1 hops
00:57:27:      172.17.0.0/16 via 0.0.0.0 in 1 hops
00:57:27:      172.18.0.0/16 via 0.0.0.0 in 1 hops
```

- ❍ **A.** The routing updates are broadcast to their neighbors.
- ❍ **B.** The router automatically summarizes these networks.
- ❍ **C.** Networks 172.17.0.0 and 172.18.0.0 have an infinite metric.
- ❍ **D.** The `no auto-summary` command is used in RIPv2.

10. Which characteristic does not go with its respective routing protocol?

- ❍ **A.** 180 invalid timer—RIP
- ❍ **B.** Classful by default—RIPv2
- ❍ **C.** Default metric is bandwidth, delay, reliability, load, and MTU—IGRP
- ❍ **D.** Default maximum hop count of 100—GRP

11. What command configures a gateway of last resort to be sent to downstream neighbors in IGRP updates?

- ❍ **A.** `ip route 0.0.0.0 0.0.0.0 serial 0`
- ❍ **B.** `redistribute default`
- ❍ **C.** No command necessary. It is done automatically.
- ❍ **D.** `ip default-network`

Answers to Review Questions

1. Since distance vector routing protocols are susceptible to routing loops, they have incorporated several countermeasures to help mitigate any routing loop anomalies. For instance, all distance vector routing protocols have a maximum hop count to avoid counting-to-infinity. In addition, split horizon prevents routers from advertising networks out the same interface in which they were learned. Upon learning about a failing network, routers poison the route by setting it to an infinite metric and send a triggered update to the router's neighbors. The router will not process new inferior information about the failed network until the hold-down timer expires to ensure the failed network does not get accidentally reinstated.

2. RIP is a classful distance vector routing protocol that uses hop count as its metric (maximum of 15). RIP broadcasts the contents of the routing table to its directly connected neighbors every 30 seconds.

3. RIPv2 supports classless routing updates if the `no auto-summary` command is used. In addition, RIPv2 updates are sent as multicasts and can be authenticated using a MD5 password.

4. IGRP is a classful distance vector Cisco proprietary routing protocol that uses a composite metric (bandwidth + delay) to determine the optimal path to a destination. IGRP also supports unequal path load balancing by using the `variance` command.

5. To enable RIP and IGRP, you must enter the routing process by using the keyword `router` followed by the routing protocol. In the case of IGRP, you must also specify the autonomous system number which must match in all routers in the routing domain. Once in the routing configuration process, you must advertise the directly connected classful networks attached to the router by using the `network` command followed by the classful network.

Answers to Exam Questions

1. **B**. Because the routing table update shows the 1.0.0.0/8 network as possibly down, it is currently in a hold-down state and waiting for the hold-down timer to expire before accepting a route with a higher metric. Answer A is incorrect because the AD is 120 and the hip count is 1. C is false because those network entries were learned via RIP, not advertised. D is incorrect, since B is correct.

2. **A**. Because the default route has an R statement next to it, it was redistributed automatically by the neighbor at 192.168.1.9. If it was statically configured, it would have an S indication next to the route. Answers B, C, and D are true statements since the 0.0.0.0 route was redistributed and advertised via RIP by the router with the IP address of 192.168.1.9.

3. **D**. Because the 172.18.0.0 has an infinite metric for RIP being advertised, it is most likely a poisoned route or a router that is not showing up in the routing table. Answers A, B, and C will show up in the routing table since their hop count is does not exceed the maximum hop count for RIP (15).

4. **A, C**. The only distance vector routing protocol that can be classless is RIPv2. The command to enable RIPv2 is `version 2`. To make it classless, you use the no `auto-summary` command. Answer B is incorrect because the `variance` command is used to load balance over unequal paths. Answer D is not a valid command.

5. **C**. Because the lowest metric to the destinations is 23, and the highest is 601, a multiplier of 30 enables metric values from 23 to 690 (30×23). Answer A is incorrect, because the multiplier will only load balance over links with a metric up to 230. Answer B is incorrect, because the multiplier will only load balance over links with a metric up to 69. Answer D is incorrect, because the multiplier will only load balance over links with a metric up to 575.

6. **D**. The autonomous system number must match in both devices or the routers will ignore each other's updates. Answer A is incorrect because Router A is not advertising the 172.18.0.0 network. Answer B is incorrect because Router B will already have the 192.168.34.0 network in its routing table since Router B is advertising this directly connected network. Answer C is false because IGRP is a classful routing protocol.

7. **A**. Because the router is advertising updates back through the same interface as that through which they were learned, split horizon must be disabled. Answer B is true because IGRP uses bandwidth + delay by default as its metric. C is also true because IGRP is a classful routing protocol. D is a true statement because the metrics do not equal 4,294,967,295.

8. **B**. Before running any `debug` commands, you should check your router's current and past utilization with the `show processes` command. Answer A does not have any effect on the debug process. Answer C will turn off any debugging after the debugging process has been initiated. Answer D does not have any effect on the debugging process.

9. **D**. The update is indicative of a RIPv2 update that has been configured as classless with the no `auto-summary` command. This is true because the updates contain the subnet masks. Answer A is false because RIPv2 multicasts its updates to 224.0.0.9. B is false because the `no auto-summary` command disables automatic summarization. C is incorrect because an infinite metric for RIPv2 is 16.

10. **C**. IGRP by default uses bandwidth + delay as its metric; however, it can be configured to use reliability, load, and MTU. Answer A is true because RIP has an invalid timer of 180 seconds. Answer B is also true because RIPv2 is classful by default. Answer D is true because IGRP's maximum hop count is 100 by default.

11. **D**. To send a default route with IGRP, you can use the `ip default-network` command in Global Configuration and specify a network entry that exists in your routing table. Answer A is incorrect because a static default route is not redistributed automatically, as is the case with RIP. Answer B is not a valid command. C is false because this process is not an automatic one.

Suggested Readings and Resources

1. Zinn, Alex. *IP Routing: Packet Forwarding and Intra-domain Routing Protocols*. Addison Wesley Professional, 2002.

2. Kruepke, Keith; Cernick, Paul; Degner, Mark. *Cisco IP Routing Handbook*. Hungry Minds, 2000.

3. Bruno, Anthony and Kim, Jacqueline. *CCDA Exam Certification Guide*. Cisco Press, 2004.

4. "Routing Protocols," www.firewall.cx.

5. "RIP, IGRP, RIPv2," technology support on www.cisco.com.

CHAPTER 12

Link-State and Hybrid Routing Protocols

Objectives

This chapter covers the following Cisco-specified objectives for the "Technology," "Implementation and Operation," "Planning and Designing," and "Troubleshooting" sections of the CCNA exam:

Evaluate the characteristics of routing protocols

Select an appropriate routing protocol based on user requirements

Configure routing protocols given user requirements

Troubleshoot routing protocols

- Each routing protocol is unique, based upon characteristics such as the contents of its routing updates, the frequency of its routing updates, and its capability to converge in the face of a topology change.
- Because each routing protocol has varying characteristics, you must choose the correct protocol based upon the users' requirements and the existing infrastructure and design.
- By knowing which networks are attached to your router, you can configure either OSPF or EIGRP to advertise those networks to their known neighbors.
- Using the `show` and `debug` commands, you can determine whether a configuration is configured correctly and whether the routing protocols are operating as they should.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- The concepts mentioned in this chapter are the essentials to understand for the CCNA exam. Additional features and configurations entailed with these routing protocols are covered in the Building Scalable Cisco Internetworks exam for the CCNP. If you're researching them in other information sources, be sure not to get too engrossed in these additional features.
- This chapter requires a firm understanding of subnetting. Please review Chapter 4 and ensure that you have mastered this topic before tackling wildcard masks in this chapter.
- Complete the Challenge Exercises and the Exercises at the end of the chapter. The exercises will solidify the concepts that you have learned in the previous sections.
- This chapter makes mention of the concepts discussed in Chapter 10. If you are not completely confident in your comfort with the fundamentals of routing protocols and their metrics, review Chapter 10 again before proceeding with this chapter.
- This chapter revisits route summarization that was discussed in Chapter 10. Be sure you are familiar with supernetting before attempting to read this chapter.
- Complete the Exam Questions at the end of the chapter. They are designed to simulate the type of questions you will be asked in the CCNA exam.

Introduction

Distance vector routing protocols are ideal for small networks in which there are routers with slow processing power and limited memory resources. Today's enterprises require significantly larger networks that can scale way beyond the limits of distance vector routing protocols. As the networks grow larger, routing protocols must also be able to react to topology changes faster to ensure that all devices are aware of a change in a reasonable amount of time. Link-state and balanced hybrid/advanced distance vector routing protocols were designed to overcome the scalability and convergence speed restrictions that hindered distance-vector routing protocols. This chapter looks at how the innovators of these two classes of routing protocols, OSPF and EIGRP, achieve these feats and shows you how to implement and customize them in your configurations.

Link-State Operations

Objective:

Evaluate the characteristics of routing protocols

Recall that distance vector routing protocols used the Bellman-Ford algorithm, which entailed routing devices advertising directly connected networks that are sent to any neighbor listening on adjacent segments. When they received the updates, they would manipulate their routing tables and advertise the subsequent information to their directly connected neighbors. One of the major downfalls with this algorithm is that the updates contain second-hand information from other routers and in which the best pathway is chosen according to another device's perception of the network. This would be similar to following directions to a destination based upon your friend's sister's boyfriend's recollection of getting to that destination over his preferred roads and highways.

Link-state routing protocols use the Dijkstra Shortest Path First (SPF) algorithm, which is a complex and processor-intensive mathematical calculation in determining optimal paths. How this differs from distance vector routing algorithms is that the calculations are actually done based upon all possible routes to a destination that link-state routing protocols store in their topology tables. The best route that is chosen from the topology table for any given network is placed in the router's routing table.

Routers receive this topology information from the neighbors they discovered by listening for Link-State Advertisements (LSAs) from other routers. In fact, link-state routing protocols establish a relationship with these neighbors and track them in yet another table, called the *neighbor table*, before even sending update information.

EXAM ALERT

Remember link-state routing protocols have to maintain three tables: the topology table, the neighbor table (sometimes referred to as an adjacency table), and the routing table.

The updates that are exchanged between the routers not only contain the subnets that their neighbors know about, but all information about their link-states, including the status of the links and the metrics for each subnet they are aware of. Knowing all the possible links and their associated metrics to reach them, the router can make first-hand decisions about which is the best path for it to take to reach each destination. To reuse the analogy, now you would learn about the all possible paths to the destination from your friend, your friend's sister, her boyfriend, MapQuest, and so on, and base your decision on the best path, using all that information from your point of reference.

After a router sends that topology information to its neighbors, it does not need to continuously send them that information over and over again as distance vector routing protocols require. Instead, link-state routing protocols send small hello LSAs every so often just to ensure to neighbors that the router is still alive and ticking.

In the event of a topology change, a link-state update (LSU) is flooded to all routers, immediately alerting them of the topology change. In fact, link-state routers that receive this topology change notification flood the link-state update to their neighbors before processing and recalculating the change to update their own routing tables with the new information. Thus, there is no need for loop prevention measures as you witnessed with distance vector routing protocols because link-state routing protocols propagate this information and converge exponentially faster.

Because link-state routing protocols can scale to such large sizes, they can segment the routing domain into smaller systems, known as areas, so devices do not have to maintain an excessive amount of information in their topology tables. What's more, the routers that send information between these divisions summarize the subnets located inside the area connected to them to the rest of the autonomous system. By minimizing the routing update traffic and overhead, you can speed up convergence and confine instability to a single area. Because the routers that perform this route summarization have a special function over the rest of the routers in the autonomous system, link-state routing protocols are hierarchical by design.

EXAM ALERT

Know that areas are used in link-state routing protocols to speed up convergence and confine instability by route summarization.

OSPF

Objective:

Select an appropriate routing protocol based on user requirements

The most widely used link-state routing protocol today is an IETF standard routing protocol called Open Shortest Path First (OSPF). Developed in 1988, this routing protocol was created to overcome the limitations that RIP presented for large-scale networks. The following sections look at the fundamentals of OSPF and show you how to apply them in your configuration.

OSPF Characteristics

OSPF is unique among the routing protocols that are discussed in this book. This is true from its operations all the way down to the configuration. Notably, one of the more intriguing aspects of this routing protocol is that it is completely classless. With the subnet masks accompanying the networks in the routing updates, routers are aware of all the individual subnets that exist. The upside to this knowledge is that you do not have to concern yourself overly with discontiguous network designs and you can implement VLSM addressing throughout the topology. The unfortunate downside of knowing all the subnets is that the topology database can grow to be quite large, depending on the size of the autonomous system. Not only does this knowledge exhaust the memory resources in your routers, but any change in the links associated with those subnets causes a flood of updates, consequently causing each router to run the SPF algorithm again. If your autonomous system consists of 1000 routers, each one has to expend the processing resources to flood the update and rerun its algorithmic calculations based upon the residual topology. If the link is continuously going up and then down (known as *flapping*), each of the 1000 routers continually floods updates and reruns its Dijkstra SPF algorithm, which could exhaust a router's resources and detrimentally affect the router's capacity to function.

OSPF Areas

OSPF mitigates the need for excessive topology databases and update traffic overhead by segmenting an OSPF autonomous system into smaller areas. As mentioned before, routers that transmit information from one area to another can be configured to summarize the subnets being advertised to other areas. In this situation, routers in other areas need to keep only summarized entries in their topology table, minimizing the amount of memory required. In the event that a link goes down within the area, only devices within that area need to be notified because the rest of the OSPF autonomous system is aware of only the summarized route. With that update confined within that area, other routers in different areas do not receive an update and do not have to flood and recalculate the information in the update.

For instance, Figure 12.1 demonstrates an OSPF autonomous system in which you have created three areas. Routers C and E have the responsibility of summarizing the subnets in their areas to the rest of the OSPF autonomous system. This hierarchy in routing ensures that any link failure that occurs in the areas they are summarizing does not go beyond those routers. Because these hierarchical routers are sitting on the border between two areas, they are called Area Border Routers (ABRs).

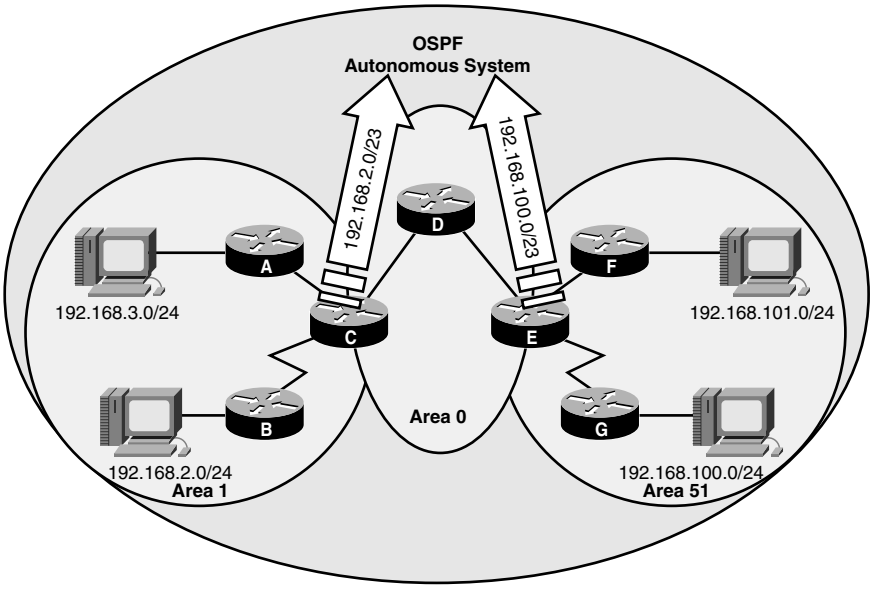


FIGURE 12.1
OSPF AS with areas.

Backbone Area

Notice that at the center of the OSPF autonomous system in Figure 12.1 is Area 0, to which Area 1 and Area 51 are attached. This is not by coincidence, but rather by design. Area 0, also known as the *backbone area*, is an essential part of an OSPF design because as the name states, this is the area in which traffic from one area must transit to reach another area. If your network design requires only a single area, that area must be Area 0.

Any area that is created must somehow be connected to the backbone area. Because this area is truly an information highway interconnecting all other areas, it typically consists of robust routers called *backbone routers* that are either completely inside or have an interface that connects to Area 0. Traffic originating in one area is sent to the backbone ABR for that area, which in turn ultimately passes the traffic to the destination backbone ABR and finally to the destination router inside the remote area. Because these links inside the backbone carry excessive traffic, the backbone routers are typically interconnected with high-speed interlinks such as Fast or Gigabit Ethernet.

EXAM ALERT

Remember that Area 0 is also commonly known as the backbone area. All areas that are created must connect back to Area 0.

Stub Area

Recall that the term *stub* in networking refers to networks that contain a single pathway in or out. Accordingly, a stub area is an area that contains only one pathway in or out of that area. The IETF created this concept of a stub area as a measure to decrease the topology database even further for routers that are inside a stub area.

NOTE

Because the backbone area is a transit area that interconnects other areas, it can never be configured as a stub.

Once again, the ABR router takes the credit for this reduction in OSPF overhead, as shown in Figure 12.2. If the area is configured on all routers inside that area as a stub area, the ABR replaces all the networks it learns from the rest of the OSPF autonomous system with a default route and advertises that to the routers inside the stub area. This makes logical sense because the routers inside the stub area are using that ABR as a gateway of last resort to leave their area.

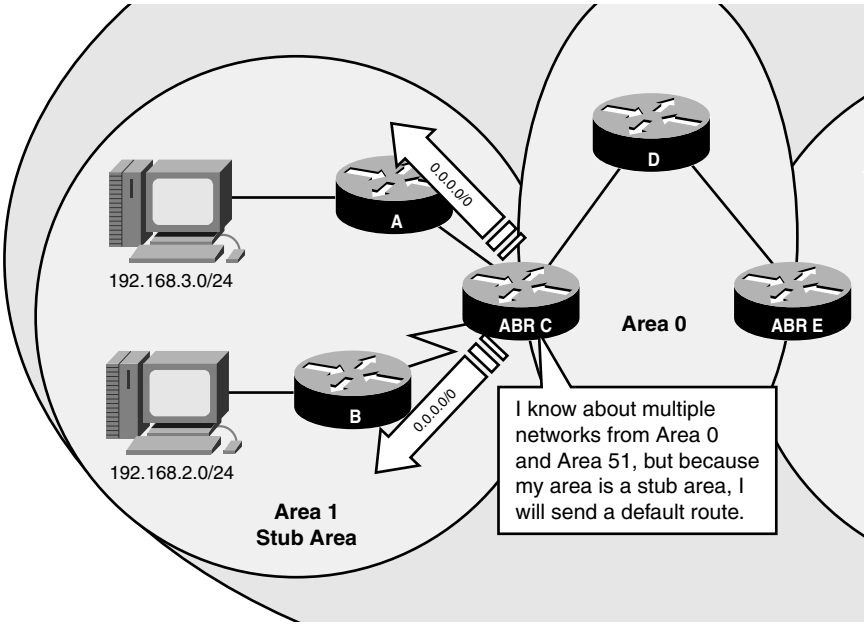


FIGURE 12.2
Stub area.

OSPF Metrics

When OSPF routers run the Dijkstra algorithm to calculate the best route to reach destination subnets, they use the lowest cumulative cost to reach that network. The path cost is calculated by taking 10^8, divided by the bandwidth in bps. Table 12.1 lists some of the common path costs associated with their respective bandwidths.

TABLE 12.1 Cost Values Based on Bandwidth

Bandwidth	OSPF Cost
56Kbps	1785
64Kbps	1562
T1 (1.544Mbps)	64
Ethernet (10Mbps)	10
Fast Ethernet (100Mbps)	1
Gigabit Ethernet (1000Mbps)	1

EXAM ALERT

Be prepared to calculate the cost for any given link speed.

Notice that when you reach and exceed Fast Ethernet speeds of 100Mbps, the cost is still 1. For that reason, you can configure OSPF to use a different reference for the bandwidth that is higher than 10^8 to account for links of that magnitude.

Router ID

Unlike most routing protocols, OSPF routers identify each other with something known as a *router ID*. The router ID is a 32-bit unique number in which the router is known to the OSPF autonomous system. This ID is determined in the following order:

1. Highest IP address assigned to an active logical interface at the start of the OSPF process.
2. If no logical interface is present, the highest IP address of an active physical interface at the start of the OSPF process.

NOTE

When I say "highest IP address," I am talking about the numerical value of the IP address, not the class of the IP address.

EXAM ALERT

Be sure to know how to determine a router's router ID based upon the IP addresses of the router's interfaces.

Take notice that if there is a logical interface the IP address overrides any physical IP address for the router ID, even if it is a lower value. So what do I mean by a logical interface? Cisco routers include the capability to create logical or virtual interfaces called *loopback interfaces*. The advantage of using these virtual interfaces is that, unlike physical interfaces, loopback interfaces cannot go down unless the router is malfunctioning or turned off.

EXAM ALERT

For the exam, keep in mind that loopback interfaces are logical interfaces that cannot go down unless the router is malfunctioning or turned off.

OSPF Topologies

The nature in which OSPF operates varies greatly depending on the type of topology to which an OSPF interface is connected. Such operations as hello and dead timers, neighbor discovery methods, and OSPF update overhead reduction are ultimately dictated by the OSPF interface's topology. The three main type of topologies are the following:

- **Broadcast Multi-access**—These topologies denote multiple devices accessing a medium in which broadcasts and multicasts are heard by all devices sharing that medium (for example, ethernet).
- **Non-broadcast Multi-access**—NBMA topologies are similar to broadcast multi-access topologies (multiple devices accessing a medium), except that devices cannot hear each other's broadcasts because the medium is separated by other routers, such as with Frame Relay.
- **Point-to-Point**—On a point-to-point link, there are only two devices on a shared network link.

To demonstrate the point, consider how OSPF timers operate in different topologies. For instance, in broadcast multi-access and point-to-point links, the hello and dead interval is 10 and 40 seconds, respectively. Remember, these hello messages are not full routing updates like distance vector routing protocols. The hello messages contain minimal information to identify the sending device to other neighbor routers to ensure that their dead timers do not expire and cause a topology change.

Because NBMA network topologies such as Frame Relay typically comprise slower links, the default timers for these topologies are 30 seconds for hello messages and 120 seconds for the dead timer. The hello messages are not sent as often in NBMA topologies to ensure that OSPF routers are not needlessly consuming bandwidth on the WAN links.

DR/BDR Elections

Another significant topology-related function of OSPF is the election of a Designated Router (DR) and a Backup Designated Router (BDR) in broadcast and non-broadcast multi-access topologies. Routers in these topologies undergo these elections to reduce the amount of update overhead that can be incurred when a link state changes.

For example, in Figure 12.3, all the routers in Area 7 are connected to a switch, which is indicative of a broadcast multi-access topology. If the link connected to Area 0 on ABR Router B were to fail, OSPF protocol dictates that it flood the update to all the neighbors in its neighbor table. When Router B sends that update to all the routers in the topology, all devices hear that because they are all connected to the same switch. However, recall that after the other routers receive that update, they have to alert all their neighbors—once again, all the routers connected to the switch. This time, multiple routers send the update and cause excessive traffic on the switched network to devices that are already aware of the update. If you have a large number of routers in the topology, this update traffic can consume quite a bit of unnecessary bandwidth and processor utilization. In point-to-point links, it is not necessary to have a DR or BDR election because only two routers are on the segment and there is no threat of excessive update traffic.

EXAM ALERT

Remember that DRs and BDRs are elected only on broadcast and non-broadcast multi-access networks.

When a DR and BDR are elected (in case the DR fails), routing updates are minimized because the update is sent only to the DR and the BDR. The DR then is responsible for updating the rest of the topology. The election is determined by the following:

1. **Highest interface priority**—An arbitrary number you can configure on an interface-by-interface basis. The default is 1. A value of 0 renders the device ineligible for DR and BDR election.
2. **Highest Router ID**—In the event of a tie, the highest Router ID is the tiebreaker.

EXAM ALERT

Be sure to keep in mind for the exam that DR and BDR elections are decided by the highest interface priority, followed by the highest Router ID in the event of a tie.

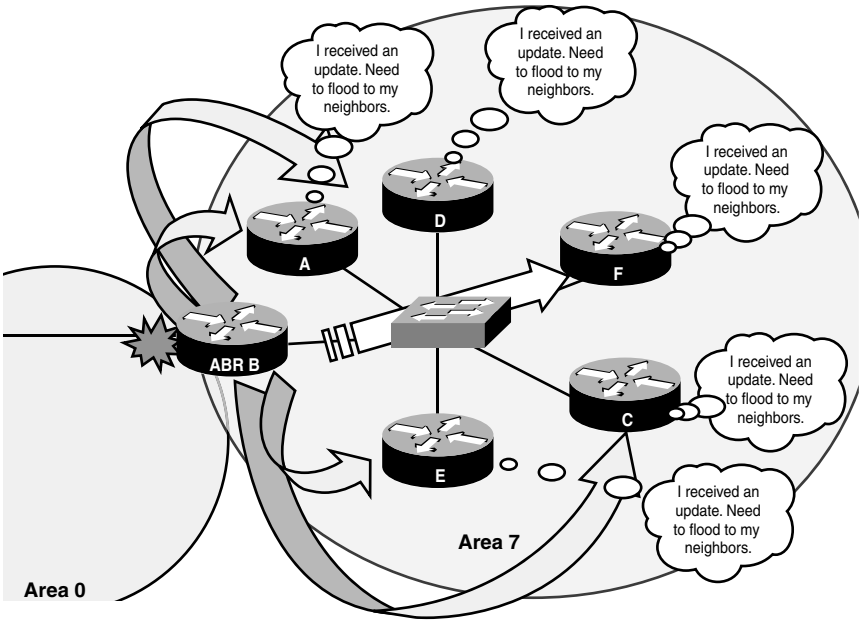


FIGURE 12.3 Broadcast multi-access topology updates.

TIP

This election is based upon the assumption that all devices start the OSPF process at the same time. Realistically, the first router that comes online is the DR and the second is the BDR. If you need to set another router as the DR, you must take the current DR and BDR offline or restart the OSPF process to force the election.

Figure 12.4 demonstrates the election process between several routers in a broadcast multi-access topology. Because Router D's interface priority is highest, that router becomes the DR for that segment. Router F, with the second highest priority, becomes the BDR in case Router D is turned off or crashes. Now if a link fails, the update is sent to Router D, which in turn updates the rest of the topology.

One missing piece of this OSPF puzzle is how the devices manage to send updates to the DR and BDR routers only if they are all connected in the same topology. The answer lies in the manner in which OSPF routers propagate LSAs and LSUs. Rather than broadcast this information as RIPv1 and IGRP do, OSPF sends updates to two different reserved multicast addresses. The multicast address, 224.0.0.6, is reserved for the DR and BDR. When a router needs to send an update in a broadcast or non-broadcast topology, it sends the LSU to 224.0.0.6, which only the DR and BDR process. The DR then sends the LSU to the multicast address of 224.0.0.5, which is the address to which all OSPF routers are listening for updates and hello messages.

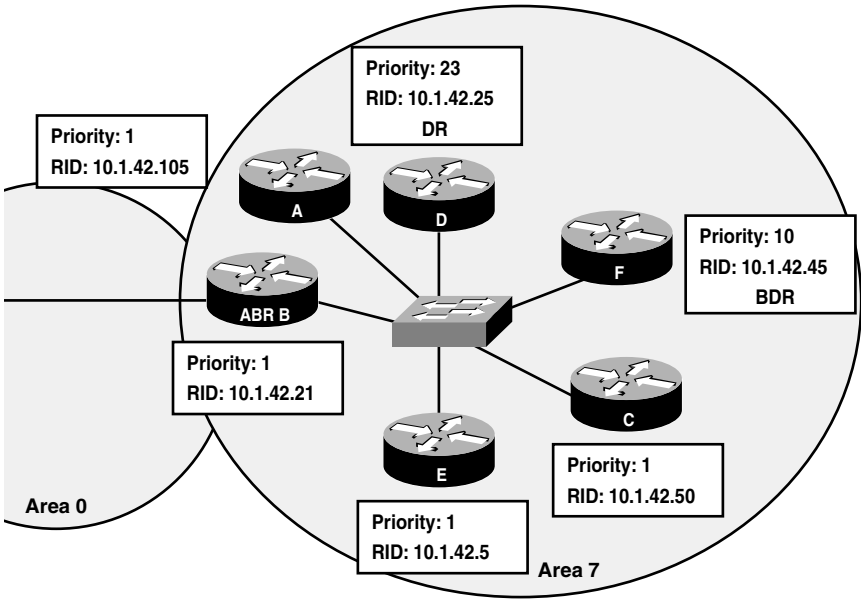


FIGURE 12.4
DR and BDR elections.

So now when Router B detects the link failure, it multicasts its LSU to 224.0.0.6, which only Router D and Router F process. Because Router D is the DR, it disseminates the update to everyone else in the topology by sending the update to 224.0.0.5.

OSPF Initialization

Recall that link-state routing protocols establish who the router's neighbors are before exchanging updates. This process is actually quite intricate and depends on several factors being in place. To clarify, let's look into what happens when an OSPF router comes online.

After the OSPF process is started in a router, it sends a hello message out all interfaces that are configured to participate in OSPF. The hello LSAs are sent to the multicast address of 224.0.0.5 so that all devices running OSPF will process it. Information contained in the hello messages includes the following: Router ID, hello/dead intervals, known neighbors, area ID, priority, DR address, BDR address, authentication password (similar to RIPv2), and stub area flags (if area is configured as a stub area).

A router that receives this hello message adds that neighbor to its neighbor table only if the hello/dead intervals, area ID, authentication password, and stub flag match its configuration. If these values match, the router sends a hello message back, which includes the Router ID of new router in the neighbor list. At that point, the original router adds that router to its neighbor table. This process occurs until the router discovers all the neighbors on its links.

EXAM ALERT

Remember that the hello/dead intervals, authentication password, stub flag, and area ID must match in the hello LSAs to form a neighbor relationship.

It is important to note that no update information has been exchanged at this point. If the topology has a DR elected (indicated in the hello messages it received), it synchronizes its topology table with that router because the DR always has the most current information. If the topology is a point-to-point connection, the two routers synchronize with the neighbor on the other side of the link. After the topology tables are synchronized, it is said that the devices have formed an adjacency. Now that the router has all possible routes in the topology table, it can run the Dijkstra algorithm to calculate the best routes to each subnet.

Introduction to Configuring OPSF

Objective:

Configure routing protocols given user requirements

One of the first steps you should take when configuring OSPF is to configure loopback interfaces to ensure that your Router ID will match the IP address of the loopback interface when the OSPF routing process is started. To create a virtual loopback interface, you configure it like a normal interface, as shown in the following example:

```
Router(config)#interface loopback 0
Router(config-if)#ip address 10.1.42.1 255.255.255.255
```

The interface number for the loopback interface is arbitrary because the interface is virtual. Also, notice the subnet mask used in the loopback interface is 255.255.255.255 or a /32. This is known as a *host mask* and is typically used on loopback interfaces because there is no need to use an entire subnet on a virtual interface that doesn't connect to anything.

EXAM ALERT

Keep in mind for the exam that loopback interfaces typically have a subnet mask of 255.255.255.255, known as a host mask.

To start the OSPF process for configuration, you use the `router` keyword followed by `ospf` just as you have in the past with other routing protocols. In the case of OSPF, however, you must specify a process ID after the `router ospf` keywords. The process ID is an arbitrary number ranging from 1–65535, in which the router can track whether you have multiple instances of OSPF running in your router. Unlike the autonomous system number used in IGRP, this process ID does not need to match in all router configurations.

EXAM ALERT

Remember that the process ID is a locally significant number between 1 and 65535 that is used to track multiple instances of OSPF that might be running on the router. It does not have to match in all other router configurations.

Wildcard Masks

Before you go further with the explanation of the OSPF configuration, you need to understand the means by which OSPF advertises the classless networks in the configuration. Because you no longer have the luxury of putting a classful subnet in the `network` statement, you need to have some way of telling the router what specific IP subnets are to be applied to the OSPF routing process. OSPF (as well as EIGRP and access lists) use something called a *wildcard mask* to identify to the IOS how much of an IP address should be applied to a criteria in a configuration statement. That criteria differs depending on which configuration statements the wildcard mask is using.

NOTE

Wildcard masks are revisited in Chapter 13, "Access Lists," with access lists.

In the case of OSPF, the wildcard mask is used to define what portion of the IP in a `network` statement is to be associated with the routing process. If the IP addresses assigned to interfaces matches the scope of the addresses defined with the IP address and wildcard mask criteria in the `network` entry, then OSPF is enabled on those interfaces and their subnets are advertised in routing updates.

Wildcard masks are represented as 32-bit numbers separated in four octets, just like IP addresses and subnet masks. Each bit in the wildcard mask corresponds back to the same bit position in the IP address to identify whether that bit should be applied to the criteria. Specifically, if the bit value in a wildcard mask is a 0, the corresponding bit in the IP address is checked and applied to the criteria. Conversely, a 1 in a wildcard mask bit signifies that the corresponding bit in the IP address can be ignored. Using these 0s and 1s, you are basically telling the IOS to perform pattern matching against the IP address that precedes the wildcard mask and apply the portion that matches to the conditions in the configuration statement.

For example, if you wanted to apply a wildcard mask to a specific IP address, every bit in the wildcard mask must be a 0 (0000000.0000000.0000000.0000000) because each corresponding bit in the IP address is being applied to the criteria. So, for example, if you wanted to specify the IP address of 10.1.4.2, the corresponding wildcard mask for that specific IP would be 0.0.0.0 in decimal. On the contrary, if you wanted to apply the criteria to any IP (therefore,

you do not care whether any of the corresponding bits match), you would need to have a wildcard mask composed of all 1s (11111111.1111111.11111111.11111111, or 255.255.255.255 in decimal). Technically it does not matter which IP address precedes this wildcard mask because you are applying any value, so it is common to use an IP address of 0.0.0.0 with the 255.255.255.255 wildcard mask.

In cases such as those with OSPF, you need to use wildcard masks to specify a specific IP subnet. For instance, given an IP subnet of 192.168.1.0 /24, you know that you want to apply the criteria to the first 24 bits in the IP address. Because the last octet of the IP subnet can be any value from 0–255, you don't want to apply any of those bits to your criteria. The resultant wildcard mask will ultimately be composed of the first three octets in the wildcard mask, containing all 0s to match the 192.168.1, and the last octet containing all 1s. Thus, the 192.168.1.0 /24 subnet would be identified as 192.168.1.0 0.0.0.255 in the configuration statement.

That may seem fairly cut and dry, but how do you apply a wildcard mask to a subnet such as 192.168.1.4 /30? You know right off that the first three octets will have all 0s, but you can't say you don't care about all 8 bits in the last octet because you want to apply this criteria only to those IPs in the 192.168.1.4 255.255.255.252 subnet (192.168.1.4-192.168.1.7). As shown in Figure 12.5, by breaking down the last octet into binary, you can see how to align the corresponding bits in the wildcard mask. Namely, the first six bits in the last octet must be exactly the same values that are in the IP address to give you a decimal value of 4. The last two bits can be any combination of 1s or 0s because they will ultimately give you the values of 192.168.1.4, 192.168.1.5, 192.168.1.6, and 192.168.1.7. Because the first six bits must match, and the last two do not matter, the wildcard mask in binary for the last octet is 00000011, or 3 in decimal. So, to specify the 192.168.1.4 /30 subnet, your statement would look like 192.168.1.4 0.0.0.3.

	.128	64	32	16	8	4	2	1
IP: 192 168.1.4	. 0	0	0	0	0	1	0	0
SM:255.255.255.252	. 1	1	1	1	1	1	0	0
WCM: 0.0.0.3	. 0	0	0	0	0	0	1	1

FIGURE 12.5 Wildcard mask breakdown.

TIP

An easier way to determine a wildcard mask for an entire subnet is by subtracting the subnet mask from 255.255.255.255. For example, 255.255.255.255 – 255.255.255.252 = 0.0.0.3. In addition, the wildcard mask is always one less than the increment of the subnet in the octet where the subnet falls. For instance, a subnet of 255.255.255.252 has an increment of 4. So the wildcard mask in the last octet (because the /30 subnet falls in the last octet) is one less than the increment, or 0.0.0.3.

Notice in Figure 12.5 that the wildcard mask happens to be the inverse of the subnet mask. For this very reason, the wildcard mask is sometimes referred to as the *inverse mask*. This is the case for all wildcard masks that correspond to an entire subnet.

EXAM ALERT

You will be expected to be able to determine a wildcard mask given an IP address or an entire subnet for several concepts throughout the CCNA exam. It is imperative that you practice and master these calculations and be able to recognize an incorrect configuration if presented with a troubleshooting scenario.

OSPF Network Configuration

Reverting back to the matter of configuring OSPF, you left off with entering the OSPF routing process by typing something similar to the following:

```
Router(config)#router ospf 4
```

Recall that the number `4` in this example is the process ID and does not have to match in all routers. Because you are in the routing process (indicated by the `Router(config-router)#` prompt) for OSPF, you are ready to specify the classless networks that are to participate in OSPF. As you do with other routing protocols, you start off by using the keyword `network`, but from there you go a different direction. At this point, you need to specify an IP address or IP subnet, followed by the wildcard mask to identify which interfaces are participating in the OSPF process. Immediately following the IP and wildcard mask is the keyword `area` followed by the OSPF area number where the router's interface is located. For example, if you have an IP address of 192.168.1.1 with a subnet mask of 255.255.255.0 connected to area 0, you would configure it something like the following:

```
Router(config)#router ospf 4
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

EXAM ALERT

Be sure you understand the syntax involved in starting the OSPF process and assigning networks to that process.

Because you use the wildcard mask in the OSPF configuration, you actually have multiple ways to specify an interface and its subnet in the OSPF routing process. Using the same example, you could use any of the following configurations in Table 12.2 to place that interface in area 0.

TABLE 12.2 Alternate `network` Statements

Command	Explanation
`Router(config-router)#network 192.168.1.1 0.0.0.0 area 0`	The interface with the IP address of 192.168.1.1 and its subnet will be advertised in OSPF.
`Router(config-router)#network 192.168.0.0 0.0.255.255 area 0`	Interfaces and their subnets starting with 192.168 will be advertised in OSPF.
`Router(config-router)#network 192.0.0.0 0.255.255.255 area 0`	Interfaces and their subnets starting with 192 will be advertised in OSPF.
`Router(config-router)#network 0.0.0.0 255.255.255.255 area 0`	All interfaces and their subnets will be advertised in OSPF.

EXAM ALERT

Because there are so many ways you can advertise the networks with OSPF, the exam will be looking for one specific way. If not otherwise specified, specify the entire subnet for each interface.

In the example demonstrated in Figure 12.6, you are shown the configuration for two of the routers in the multi-area OSPF autonomous system. First, notice that Router B and Router D do not have matching Router IDs; these values are significant locally only to those routers to keep track of multiple instances of OSPF that might be running. Router D has both interfaces in the backbone area, so you specify each subnet, using the appropriate wildcard mask, and identify the networks to be in Area 0. Notice the configuration parameters are similar in Router B except the interface that has the 192.168.1.8 subnet assigned to it is in Area 51. With that network placed in a different area, that router is now configured to be an ABR.

Additional OSPF Commands

As you already know, OSPF is loaded with additional features and capabilities that make this routing protocol extremely adaptable. Throughout the course of your Cisco career, you may find yourself needing to configure additional parameters to fit the needs of your network. This section covers a few of the many configurations that OSPF offers.

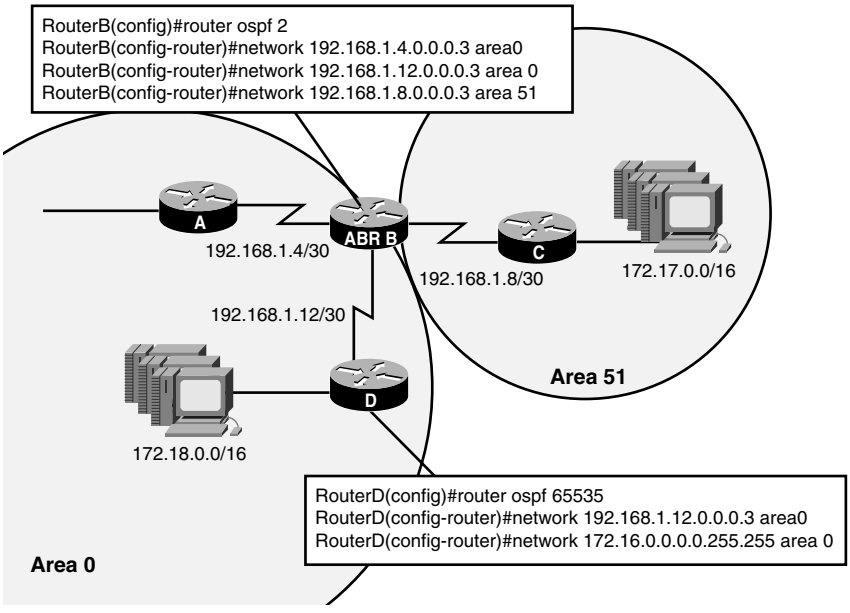


FIGURE 12.6
Multi-area OSPF configuration example.

For instance, in instances where you want to designate your area as a stub to decrease the amount of routing information stored in the topology database, you can use the `area` command in the routing process to identify that area as a stub:

```
Router(config-router)#area 51 stub
```

TIP

Remember, the stub flag was one of the required fields to form a neighbor relationship, so be sure you configure this for all routers that touch that area.

Because OSPF does not have automatic summarization, you have to configure these routers manually to summarize a set of networks. For example, if you wanted to summarize the 192.168.1.4 /24–192.168.1.7 /24 subnets in Area 51, you would use the `range` keyword in the area configuration, as in the following:

```
Router(config-router)#area 51 range 192.168.1.4 255.255.252.0
```

OSPF also has several commands that are actually configured on the interfaces as opposed to in the routing process. For example, if you wanted to manipulate the cost of an interface to make a network favorable over another or to force the router to load balance, you can use the `ip ospf cost` command as shown here:

```
Router(config)#interface serial 0/0
Router(config-if)#ip ospf cost 2
```

On interfaces that are connected to broadcast and non-broadcast multi-access topologies, it is highly recommended that you change the priority in those routers that you want to force the DR and BDR election. By default, the priority is 1, but you can change that manually by using the `ip ospf priority` command as follows:

```
Router(config)#interface serial 0/0
Router(config-if)#ip ospf priority 3
```

Verifying OSPF

Objective:

Troubleshoot routing protocols

Because there are so many aspects of OSPF, you have a considerable number of `show` commands at your disposal to verify OSPF operations. As before, you can use the `show running-config` to verify the local configuration of your routing protocol. In the case of OSPF, this is useful to ensure that you configured the network and wildcard mask correctly, as well as associated the network with the correct area. In addition, `show ip protocols` once again shows you information regarding the networks that you are advertising with OPSF.

Recall that OSPF maintains three separate tables in its routing process: the routing table, the neighbor table, and the topology table. You are already familiar with the `show ip route` command to view the routing table and verify whether you are receiving OPSF networks from the neighbors, as illustrated here:

```
RouterA>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * -
➥candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set
O IA 172.17.0.0/16 [110/74] via 192.168.1.6, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
O       172.18.0.1/16  [110/65] via 192.168.1.6, Serial0/0
     10.0.0.0/32 is subnetted, 1 subnets
C       10.1.42.1 is directly connected, Loopback0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.4 is directly connected, Serial0/0
```

The 172.17.0.0 and 172.18.0.0 networks in this example were learned via OSPF through the Serial 0/0 interface. Notice that the 172.17.0.0 entry has an IA (inter-area) indicator that signifies that this network was learned from an ABR and the network resides in another area.

To see a listing of the neighbors that were discovered through LSA hello advertisements, you can look in the neighbor table of your router by using the `show ip ospf neighbor` command as follows:

```
RouterA>show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.42.100      10   FULL/DR         00:00:39    192.168.1.6     Serial0/0
```

The Neighbor ID is actually the Router ID of the neighbor that is being advertised in neighbor's hello messages. The `Pri` field indicates the priority configured on your neighbors' interfaces. Because the default priority is 1 and this neighbor has a priority of 10, that router happens to be the DR for that segment as shown in the State field. The other possible values for this state could be BDR or DROTHER (not a DR or BDR), depending on whether those routers won the election on that segment.

The `show ip ospf database` command shows the third table that is maintained by OSPF: the topology table. This table lists all the network entries and the advertising routers for those entries. From this table, the SPF algorithm is run and the routes with the lowest cumulative cost are put in the routing table. Below, you can see the output of the `show ip ospf database summary` command because the information is presented in a more intelligible output:

```
RouterA>show ip ospf database summary

       OSPF Router with ID (10.1.42.1) (Process ID 1)

                Summary Net Link States (Area 51)

  Routing Bit Set on this LSA
  LS age: 537
  Options: (No TOS-capability, DC)
  LS Type: Summary Links(Network)
  Link State ID: 172.17.0.0 (summary Network Number)
  Advertising Router: 10.1.42.100
  LS Seq Number: 80000001
  Checksum: 0x7863
  Length: 28
  Network Mask: /16
        TOS: 0  Metric: 10
```

Here you can see the 172.17.0.0 network you learned from the neighbor router, 10.1.42.100, and the cost of the link associated with that network.

NOTE

In a larger-scale example, there could be hundreds of these networks that have been learned from other routers in the OSPF area and in other areas as well.

The final show command for OSPF is actually extremely useful when you want to gather information regarding the network topologies that are connected to the router's interfaces. The `show ip ospf interface` command yields a wealth of information such as the local router's Router ID, interface topology type, link cost and priority, the Router ID for the DR and BDR on the segment, hello/dead intervals, and a count of how many neighbors and adjacencies formed, as you can see in Figure 12.7.

```
RouterA>show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet Address 172.16.0.1/16, Area 51
  Process ID 1, Router ID 10.1.42.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.42.1, Interface address 172.16.0.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0 is up, line protocol is up
  Internet Address 192.168.1.5/30, Area 51
  Process ID 1, Router ID 10.1.42.1, Network Type NON_BROADCAST, Cost: 64
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.1.42.100, Interface address 192.168.1.6
  Backup Designated router (ID) 10.1.42.1, Interface address 192.168.1.5
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:07
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.42.100  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

FIGURE 12.7 `show ip ospf interface` output.

EXAM ALERT

The `show ip ospf neighbor` and the `show ip ospf interface` commands can show you which router is the DR and which is the BDR.

Troubleshooting OSPF

At the risk of sounding like a broken record, you should begin your troubleshooting by using the show commands discussed in the previous section to ensure your configurations are correct. Some of the more common problems that occur with OSPF configurations are simple mistakes such as those that occur with incorrect `network` statements (incorrect network ID, wildcard mask, or area) or forgetting to configure each router as a stub in a stub area.

In cases where the configuration checks out, OSPF also has the capability of debugging routing information in real-time if you use the `debug ip ospf events` command. This command is useful if you are trying to troubleshoot occurrences such as routers that cannot form a neighbor relationship. In the following example, you can see that a hello message has been received from 10.1.42.100. Notice that there is not any real routing information in these hello messages because OSPF does not send entire routing updates in its hello LSAs.

```
RouterA#debug ip ospf events
OSPF events debugging is on
00:57:13: OSPF: Rcv hello from 10.1.42.100 area 51 from Serial0/0 192.168.1.6
00:57:13: OSPF: End of hello processing
```

Challenge

Now it is time to test your OSPF configuration skills. In this challenge, you will configure a new OSPF router given the following parameters:

Fast Ethernet Interface IP: 172.16.100.65 /27 Area 0

Serial Interface IP: 192.168.100.9 /30 Area 1

Router ID: 10.1.1.1 /32

1. The first step is to ensure that the Router ID is configured before you configure the OSPF router process.
2. Configure the OSPF router process using an ID of 65535.
3. Advertise the entire Fast Ethernet subnet and place it in the backbone area.
4. Advertise the entire Serial subnet and place it in Area 1.
5. Configure Area 1 as a stub.
6. Navigate to the Fast Ethernet interface and make sure your router becomes the DR by setting the priority to 2.

Challenge Answer

Based upon the parameters specified, your router configuration should resemble the following:

```
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
 exit
router ospf 65535
 network 172.16.100.64 0.0.0.31 area 0
 network 192.168.100.8 0.0.0.3 area 1
 area 1 stub
exit
interface FastEthernet0/0
 ip ospf priority 2
```

To configure the Router ID, you have to assign the IP address of 10.1.1.1 with a host mask of 255.255.255.255 to a virtual loopback interface so that it is chosen over the physical interfaces. After the OSPF process has begun, you need to advertise both subnets attached to the interfaces. The network ID for the Fast Ethernet interfaces is 172.16.100.64. The wildcard mask for a subnet of 255.255.255.224 is 0.0.0.31 (255.255.255.255–255.255.255.224). Likewise, the network ID for 192.168.100.9 is 192.168.100.8 with a wildcard mask of 0.0.0.3 (255.255.255.255–255.255.255.252).

Balanced Hybrid Operations

Objective:

Evaluate the characteristics of routing protocols

Balanced hybrid routing protocols are sometimes referred to as *advanced distance vector routing protocols*. The rationale behind this logic is that these routing protocols use similar metrics and have a maximum hop count as distance vector routing protocols. However, balanced hybrid routing protocols discover neighbors and put them in a neighbor table before exchanging routing information, as well as keep lists of all possible routes in a topology table, just as link-state routing protocols do. By taking the best attributes from both classes of routing protocols, they have the pick of the litter, so to speak, which enables these routing protocols to be considered some of the more elite routing protocols.

EIGRP

The biggest contender for routing protocol stardom is a Cisco proprietary routing protocol called Enhanced Interior Gateway Routing Protocol. As the name states, EIGRP is an enhanced version of Cisco's distance vector routing protocol, IGRP. In the next sections, you will look at exactly how this routing protocol is not only an enhanced version IGRP, but is actually one of the fastest converging protocols that exist today.

EIGRP Characteristics

Objective:

Select an appropriate routing protocol based on user requirements

EIGRP shares certain distance vector routing protocol attributes as its predecessor, IGRP. For example, EIGRP uses a maximum hop count (224 maximum) to limit any count to infinity problems. What's more, it also uses the same composite metrics as IGRP (bandwidth + delay by default, but can support reliability, load, and MTU) and can load balance up to six unequal paths. One significant difference in these metrics, however, is that EIGRP multiplies the metric by 256, giving it a more robust 32-bit metric over IGRP's 24-bit metric. Finally, EIGRP also uses the concept of an autonomous system number in its configuration and updates such as the case with IGRP. They are so similar, in fact, that EIGRP automatically redistributes networks learned from IGRP if their autonomous system numbers match.

EXAM ALERT

Remember that EIGRP uses a 32-bit composite metric, has a maximum hop count of 224, and automatically redistributes IGRP networks if the AS number matches.

At this point, EIGRP breaks away from its predecessor to incorporate certain features from link-state routing protocols. For instance, EIGRP discovers its neighbors and builds a topology table by sending hello messages as a multicast to the reserved multicast address of 224.0.0.10. After the neighbors are discovered, they synchronize their topology databases and send hello messages afterwards to keep their dead timers from expiring. The timers differ depending on the topology, just as you saw with OSPF. Specifically, point-to-point and broadcast topologies have a 5-second hello interval and 15-second dead timer, whereas nonbroadcast multi-access topologies such as Frame Relay have a 60-second hello interval and 180-second dead timer.

Cisco, however, did not stop there with the features of this balanced hybrid routing protocol. They developed a new routing algorithm called the Diffusing Update Algorithm, or DUAL, that ensures a 100% loop-free routing environment that can converge in the face of a topology change in a split second. EIGRP also has the capability of routing not only IP, but also IPX and AppleTalk routed protocols in your network if you have an older Novell or Macintosh environment.

EXAM ALERT

It is important to remember that EIGRP can route IP, IPX, and AppleTalk routed protocols.

NOTE

If you are routing IP, IPX, and AppleTalk with EIGRP, it keeps a routing, neighbor, and topology table for each routed protocol. That means it has to maintain nine tables, which consumes a lot of memory and processor resources.

Another additional useful characteristic of EIGRP is its capability to distinguish between internally learned networks and those networks that were redistributed into EIGRP. External networks get tagged when being redistributed so EIGRP knows not to trust those networks over native EIGRP networks. EIGRP assigns the external networks an administrative distance of 170 and the internal networks an administrative distance of 90.

EXAM ALERT

Be sure to remember that internal networks have an AD of 90 and external networks have an AD of 170.

Last but not least, EIGRP is classful by default, but can be configured to be classless similar to RIPv2. By disabling automatic summarization, you can support VLSM designs and discontiguous networks, as well as manually summarize networks at any bit boundary you want.

EXAM ALERT

In the exam, keep in mind that EIGRP is classful by default, but can support VLSM and discontiguous networks if configured as classless.

Once again, a significant downfall to this routing protocol is that all your routers must be Cisco routers (not that that is a bad thing) to support this proprietary routing protocol.

Successor and Feasible Successor Routes

The secret to EIGRP's rapid convergence is found in EIGRP's topology table. Just like OSPF, EIGRP stores all possible routes in the database and calculates the best path to each subnet, based upon the lowest cumulative composite metric. Those best routes are known as the *successor routes*.

EIGRP keeps track of the composite metric for every subnet that is being advertised to it by neighbor routers, known as the *advertised distance*. The router also tracks that advertised distance plus the composite metric to reach that advertising router from the local router, known as the *feasible distance*. The lowest feasible distance to a particular subnet becomes the successor route and is the path that is also placed in the routing table.

Where EIGRP sets it self apart from OSPF is that it keeps an ace up its sleeve, so to speak. If the conditions are correct, EIGRP keeps a backup route in its topology table known as the *feasible successor*. In the event that a successor route fails, the feasible successor becomes the successor route and is placed in the routing table in about one second.

The feasible successor route is chosen only if the route will not cause a loop when activated and if it the advertised distance from a neighbor is less than the existing successor route's feasible distance. In other words, the feasible successor must have an advertised metric that is less than the metric of the route in the routing table. For example, to reach Network X, imagine your local router's successor route might have a feasible distance of 8000. If any neighbor propagated an advertised distance for it to reach Network X of 7999 or less, then its route is a feasible successor. If the advertised distances are 8000 or more, then the route will be in the topology table, but will not be a candidate for a feasible successor.

EXAM ALERT

The successor route is the primary route in the topology table and is also placed in the routing table. The feasible successor is the second best or backup route, located only in the topology table.

DUAL Algorithm in Action

You already know that the feasible successor route in the topology table will be used if the primary successor route fails. So what is to happen if there isn't a feasible successor, as illustrated in Figure 12.8? In this exhibit, you see a glimpse of Router D's topology table for the 172.17.0.0 /16 subnet. The *P* next to the network stands for passive state, which in EIGRP terms is actually a good thing. Underneath, you see two possible routes through Router A and through Router B with numbers in parenthesis separated by a forward slash. The number on the left represents the advertised distance from the neighbor router, whereas the number on the right represents the feasible distance to reach that subnet through that advertising router. Because the path through Router B has the lowest feasible distance, that is the successor route, which is also placed in the routing table. The route through Router A has an advertised distance of 9700, which is not less than the successor route's feasible distance (3700), so it cannot be a feasible successor.

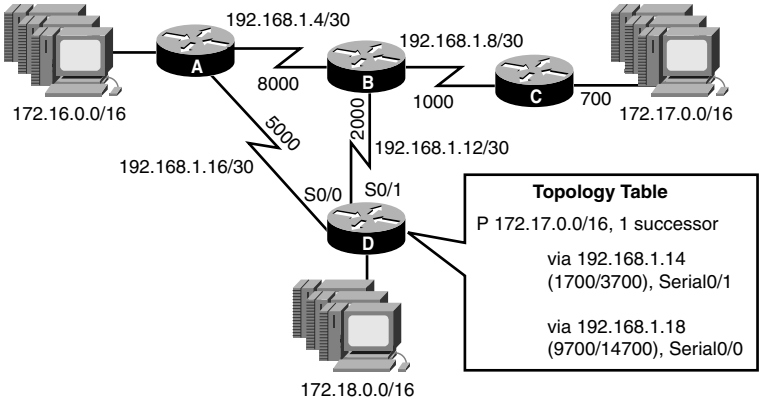


FIGURE 12.8 Passive EIGRP topology.

Now let's see what happens when the successor route to Router B fails, as shown in Figure 12.9. Without a feasible successor route to 172.17.0.0, Router D puts that network into an active state. The network is active because the router begins to actively query its directly connected neighbors whether they have a route to the affected network. This is considerably different and less resource intensive than OSPF because the router is only asking its neighbors, as opposed to flooding the update throughout the area.

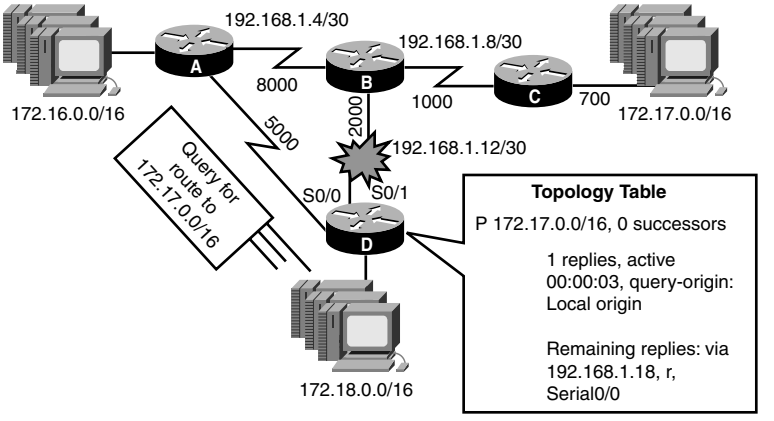


FIGURE 12.9 Active EIGRP topology.

EXAM ALERT

Remember that passive states are normal functioning routes; however, active states signify the subnet is being actively queried.

When Router A responds to Router D's query, it adds that entry into its topology table, which, in turn, will be the new successor route and be placed in the routing table. To ensure a loop-free environment, Router D has to wait for all queries to come back before implementing the new route. That is why EIGRP routers start what is known as a *Stuck In Active* (SIA) timer, which is the length of time it will wait for a response back from a query. The default SIA timeout is 180 seconds.

EIGRP Configuration

Objective:

Configure routing protocols given user requirements

One of the greatest aspects of EIGRP is that you get all this advanced functionality with minimal configuration effort required. In fact, the configuration for EIGRP is something of a cross between IGRP and RIPv2's configurations.

Just as you did for IGRP, you start the routing process for EIGRP by using the `router` keyword followed by `eigrp` and the autonomous system number. Once again, this number must match in all routers that are configured for EIGRP. In addition, as mentioned before, if there are routers that are configured for IGRP with the same autonomous system number, EIGRP automatically redistributes those IGRP subnets.

When in the routing process, you use the `network` keyword once again, followed by the directly connected classful networks because EIGRP is classful by default. You can change EIGRP into a classless routing protocol by typing the `no auto-summary` command as you did with RIPv2. The

following example configuration demonstrates adding the 172.16.0.0 and the 10.0.0.0 networks to the EIGRP process for autonomous system number 100. In addition, EIGRP is configured to be classless (`no auto-summary`) and to load balance over unequal paths (`variance` command):

```
Router(config)#router eigrp 100
Router(config-router)#network 172.16.0.0
Router(config-router)#network 10.0.0.0
Router(config-router)#no auto-summary
Router(config-router)#variance 2
```

TIP

When running EIGRP as a classless routing protocol, you can specify the wildcard mask after the network ID as you did with OSPF.

After you configure the routing protocol to be classless, you are capable of supporting VLSM, discontiguous networks, and route summarization at any bit level. With automatic summarization turned off, however, that means you must manually configure EIGRP route summaries. The command to do this is the `ip summary-address eigrp` command, which is actually configured on the interface on which the summarized route will be advertising the summary route, as follows:

```
Router(config)#interface serial 0/0
Router(config-if)#ip summary-address eigrp 192.168.4.0 255.255.254.0
```

EIGRP Verification

Objective:

Troubleshoot routing protocols

As with all of the routing protocols, the `show ip protocols` command displays the networks being advertised, the administrative distance of the routing protocol, and the routing sources for EIGRP-learned networks, as follows:

```
RouterA#show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.1.0/24 for FastEthernet0/0
      Summarizing with metric 2169856
```

```
    172.16.0.0/16 for Serial0/0
  Routing for Networks:
    172.16.0.0
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)          5      00:00:07
    192.168.1.6           90      00:00:01
  Distance: internal 90 external 170
```

As the case with OSPF, you can look at the three tables that EIGRP maintains for each routed protocol. To see the IP routing table, as before, use the `show ip route` command to verify that you are receiving EIGRP entries which are signified by the letter "D":

```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * -
➥candidate default
       U - per-user static route, o - ODR, P - periodic downloaded
➥static route
       T - traffic engineered route

Gateway of last resort is not set

D    172.17.0.0/16 [90/2195456] via 192.168.1.6, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
D EX 172.19.0.0/16 [170/2169856] via 192.168.1.6, Serial0/0
D    172.18.0.0/16 [90/2297856] via 192.168.1.6, Serial0/0
     10.0.0.0/32 is subnetted, 1 subnets
C       10.1.42.1 is directly connected, Loopback0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.4/30 is directly connected, Serial0/0
```

Notice in the preceding `show ip route` example, there is an entry for 172.19.0.0 with an `EX` indicator next to it. You may have already guessed by looking at the administrative distance in the brackets (170) that this is an external EIGRP route that was learned through another routing source being redistributed into EIGRP. Because it is not native to EIGRP, it is trusted less than an internally learned route.

To see a listing of your EIGRP neighbors that were discovered through listening to the 224.0.0.10 multicast address, the command is `show ip eigrp neighbors`, as follows:

```
RouterA#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                        (sec)         (ms)       Cnt Num
0   192.168.1.6             Se0/0         11 00:16:27   36   216  0  7
```

The final table, the topology table, can be viewed with the `show ip eigrp` topology command. Here you can see all the possible routes, determine who the successor routes are, learn whether you have any feasible successors for each subnet, and learn whether those subnets are in an active or passive state:

```
RouterA#show ip eigrp topology
IP-EIGRP Topology Table for process 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 192.168.1.4/30, 1 successors, FD is 2169856
         via Connected, Serial0/0
P 172.16.0.0/16, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 172.17.0.0/16, 1 successors, FD is 2195456
         via 192.168.1.6 (2195456/281600), Serial0/0
P 172.18.0.0/16, 1 successors, FD is 2297856
         via 192.168.1.6 (2297856/128256), Serial0/0
P 172.19.0.0/16, 1 successors, FD is 2169856
         via 192.168.1.6 (2169856/256), Serial0/0
```

NOTE

Notice that the syntax for viewing the topology table for EIGRP is `show ip eigrp topology` as opposed to OSPF's `show ip ospf database`.

EIGRP Troubleshooting

It wouldn't be a troubleshooting section without me reminding you that verifying the routing protocol configuration and process should be the first step before engaging in any debug commands. With that said, EIGRP has the capabilities of performing real-time debugging with the `debug ip eigrp` command, as follows:

```
RouterA#debug ip eigrp
03:43:46: IP-EIGRP: Processing incoming UPDATE packet
03:43:46: IP-EIGRP: Int 172.17.0.0/16 M 2195456 - 1657856 537600
➥SM 281600 - 256000 25600
03:43:46: IP-EIGRP: Int 172.18.0.0/16 M 2297856 - 1657856 640000
➥SM 128256 - 256 128000
03:43:46: IP-EIGRP: Int 172.19.0.0/16 M 2169856 - 1657856 512000
➥SM 256 - 256 0
03:43:46: IP-EIGRP: Int 172.17.0.0/16 metric 2195456 - 1657856 537600
03:43:46: IP-EIGRP: Int 172.18.0.0/16 metric 2297856 - 1657856 640000
03:43:46: IP-EIGRP: Int 172.19.0.0/16 metric 2169856 - 1657856 512000
```

Chapter Summary

This chapter rounded out your routing protocol classes as you delved into the modern link-state and balanced hybrid routing protocols. Table 12.3 is a summary of the characteristics of link-state routing protocol, OSPF, and the balanced hybrid routing protocol, EIGRP.

TABLE 12.3 OSPF and EIGRP Comparison

	OSPF	EIGRP
Classful/Classless	Classless	Both
Algorithm	Dijkstra SPF	DUAL
Metric	Cost (10^8/Bandwidth bps)	32-bit Composite
Maximum Hop Count	None	224
Areas or Autonomous System Configuration	Areas	Autonomous Systems
Hello/Dead Time	10/40, 30/120	5/15, 60/180
Cisco or IETF	IETF	Cisco
Updates	Multicast (224.0.0.5, 224.0.0.6)	Multicast (224.0.0.10)
Load Balancing	Equal Paths	Unequal Paths
Routed Protocols	IP	IP, IPX, AppleTalk

Because the OSPF Router ID is determined by the highest virtual IP address followed by the highest physical IP, it is recommended that the first step you should pursue when configuring OSPF is to create a loopback interface. To start the OSPF routing process, use the `router` keyword in global configuration, followed by the routing protocol and the OSPF process ID. This process ID is a locally significant number between 1 and 65535 that does not need to match in all router configurations. After you are in the routing process, you advertise the networks with the `network` command, followed by the network ID and the wildcard mask for that classless subnet. This is immediately followed by the `area` keyword and the area to which you want to associate that network.

By using areas, you can minimize topology and routing tables by creating route summaries on the ABR routers that are in between two areas. This also helps contain any topology changes to that area because other areas are not aware of those individual subnets. You can also create a stub area that instructs the ABR to send a default route to the routers inside the stub area instead of the subnets from other areas. Because Area 0 is the transit backbone area to which all other areas must connect, it cannot be a stub area.

OSPF also performs elections in broadcast and non-broadcast topologies to reduce update overhead. The DR and BDR are elected based upon the highest interface priority followed by the Router ID as a tiebreaker. Updates are sent to the DR and BDR, who listen on the 224.0.0.6 reserved multicast address. The update is then propagated to the rest of the segment with the 224.0.05 multicast address, to which all OSPF devices are listening.

EIGRP configuration consists of specifying the autonomous system number in the `router eigrp` command, which must match in all routers. If IGRP routers are configured in the network with the same AS number, EIGRP automatically redistributes them into EIGRP and gives them an administrative distance of 170 because they are external routes. When in the routing process for EIGRP, the directly connected classful networks are advertised. You can make EIGRP classless by using the `no auto-summary` command.

OSPF and EIGRP can be verified with the `show ip protocols` and `show ip route` commands, as with other routing protocols. In addition, you can view the neighbor table by using the `show ip ospf neighbor` for OSPF and `show ip eigrp neighbors`. You can view all the possible networks learned via OSPF's neighbors by looking at its topology table with the `show ip ospf database` command. EIGRP, on the other hand, shows you all the routes as well as the successor and any feasible successor routes in the topology table if you use the `show ip eigrp topology` command. The successor route is the primary route, which is placed in the routing table, and the feasible successor route is viable only if the advertised distance to a subnet is less than the feasible distance for the local router.

Finally, you also have the means of seeing real-time updates and hello messages in your routing protocols if you use the `debug ip ospf` command for OSPF and `debug ip eigrp` for EIGRP.

Key Terms

- Dijkstra SPF algorithm
- topology table
- LSAs
- neighbor table
- areas
- LSUs
- flapping
- ABRs
- backbone area
- backbone routers
- router ID
- loopback interface
- broadcast multi-access topology
- non-broadcast multi-access topology
- Point-to-Point Topology
- DR
- BDR
- OSPF priority
- adjacency
- host mask
- process ID
- wildcard mask
- DUAL
- successor routes
- advertised distance
- feasible distance
- feasible successor routes
- SIA timer

Apply Your Knowledge

Exercises

12.1 Configure EIGRP Router A

In this exercise and the next, you will configure EIGRP between two routers.

NOTE

This exercise assumes you have two non-production routers with a serial cross-over cable or simulated software. If you do not have these on hand, write out what the configurations would look like.

Estimated Time: 20 minutes

1. Enter Privileged EXEC on Router A.
2. Enter Global Configuration.
3. Configure and enable the ethernet interface on Router A to have an IP address of 192.168.1.1/24.
4. Configure and enable the serial interface on Router A to have an IP address of 10.1.1.1/30.
5. Configure the clock rate (if this is the DCE) for 64000 bits per second.
6. Configure a bandwidth statement to reflect this speed on the serial interface.
7. Enter the routing process for EIGRP, using 102 as the AS number.
8. Advertise the directly connected classful networks.
9. Make EIGRP classless by using the `no auto-summary` command.

12.2 Configure EIGRP Router B

Now that Router A is configured, you must configure its neighbor, Router B, to send and receive routing updates.

Estimated Time: 20 minutes

1. Enter Privileged EXEC on Router B.
2. Enter Global Configuration.

3. Configure and enable the ethernet interface on Router B to have an IP address of 172.16.30.1/24.
4. Configure and enable the serial interface on Router B to have an IP address of 10.1.1.2/30.
5. Configure the clock rate (if this is the DCE) for 64000 bits per second.
6. Configure a bandwidth statement to reflect this speed on the serial interface.
7. Enter the routing process for IGRP, using 102 as the AS number.
8. Advertise the directly connected classful networks.
9. Make EIGRP classless by using the `no auto-summary` command.

12.3 Verify Routing

If configured correctly, you should be able to verify your EIGRP routing in this exercise.

1. In both Router A and Router B, do a `show ip protocols` to verify the networks that you are advertising.
2. Do a `show ip route` and verify that you have an EIGRP entry in your routing table from your neighbor.
3. Verify the neighbor was discovered by using the `show ip eigrp neighbors` command.
4. Make sure your route is the feasible successor and it is in a passive state in the topology table by using the `show ip eigrp topology`.

Review Questions

1. What is the OSPF Router ID and how is it determined?
2. What is the significance of a Designated Router and what are the surrounding circumstances that are necessary for a router to become a DR?
3. What is the purpose of an OSPF area?
4. How does the DUAL algorithm use the contents of the topology table to ensure rapid convergence?
5. What are the basic configuration steps for using OSPF and EIGRP routing protocols?

Exam Questions

1. David, your Cisco co-worker, shows you the following output from a `debug ip ospf events` command:

```
RouterA#debug ip ospf events
OSPF events debugging is on
00:30:53: OSPF: Rcv hello from 10.1.42.100 area 51 from
➥Serial0/0 192.168.1.6
00:30:53: OSPF: Mismatched hello parameters from 192.168.1.6
00:30:53: Dead R 40 C 120, Hello R 10 C 30  Mask R 255.255.255.252
➥C 255.255.255.252
```

   He mentioned that he knows that the *R*s stand for received and the *C*s stand for configured. However, he can't figure out why he cannot get OSPF to work. What should you tell him?

   - ❍ **A.** OSPF needs to have the classful networks advertised.
   - ❍ **B.** Area 51 is an invalid area number.
   - ❍ **C.** Check the OSPF timers.
   - ❍ **D.** 10.1.42.100 needs to be a DR.

2. Given the following outputs, which of the following is false?

```
RouterA>show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet Address 172.16.0.1/16, Area 51
  Process ID 1, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.42.1, Interface address 172.16.0.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
```

   - ❍ **A.** This router will be listening for updates on multicast address 224.0.0.6.
   - ❍ **B.** 10.1.1.1 is not a loopback IP address.
   - ❍ **C.** The router interface is not connected to the backbone area.
   - ❍ **D.** This router will be listening for LSA hellos on 224.0.0.5.

3. Given the following customer requirements, which routing protocol would you recommend?

Requirements: fast convergence, IP only, large network, VLSM support needed, Cisco and Nortel routers.

- ❍ **A.** RIPv2
- ❍ **B.** IGRP
- ❍ **C.** EIGRP
- ❍ **D.** OSPF

4. Based upon the following output, which two are true? (Choose 2.)

```
RouterA#show ip eigrp topology
IP-EIGRP Topology Table for process 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 172.17.0.0/16, 1 successors, FD is 2195456
         via 192.168.1.6 (2195456/281600), Serial0/0
         via 192.168.1.31 (2297856/128256), Serial0/1
```

- ❍ **A.** The route for 172.17.0.0 is down and is being queried.
- ❍ **B.** Router 192.168.1.31 has a composite metric of 2297856 to get to 172.17.0.0.
- ❍ **C.** Router 192.168.1.6 has an administrative distance of 2195456.
- ❍ **D.** There is no feasible successor to 172.17.0.0.

5. Given the following outputs, why is OSPF not working correctly?

```
RouterA#show running-config
interface FastEthernet0/0
 ip address 172.16.0.1 255.255.0.0
!
interface Serial0/0
 ip address 192.168.1.5 255.255.255.252

RouterA#configure terminal
RouterA(config)#router ospf 9
RouterA(config-router)#network 172.16.0.0 0.0.255.255 area 0
RouterA(config-router)#network 192.168.1.0 0.0.0.4 area 0
```

- ❍ **A.** There is an incorrect network ID and wildcard mask.
- ❍ **B.** The area needs to be configured as a stub area.
- ❍ **C.** You need the `no auto-summary` command to make it classless.
- ❍ **D.** The autonomous system number doesn't match other router configurations.

6. Given the following output, what will the OSPF Router ID be for this router if you configure it for OSPF?

```
RouterA>show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        172.16.0.1      YES NVRAM  up                    up
Serial0/0              192.168.1.5     YES NVRAM  up                    up
Loopback0              10.1.42.1       YES NVRAM  administratively down down
```

   - ❍ **A.** OSPF does not require a Router ID because this router has a broadcast topology.
   - ❍ **B.** 172.16.0.1
   - ❍ **C.** 10.1.42.1
   - ❍ **D.** 192.168.1.5

7. What is the cost for a 512Kbps link for OSPF?

   - ❍ **A.** 156
   - ❍ **B.** 512
   - ❍ **C.** 10
   - ❍ **D.** 64

8. What is the effect of the following configuration?

```
 RouterA#show running-config
interface FastEthernet0/0
 ip address 10.1.0.1 255.255.0.0
!
interface Serial0/0
 ip address 10.100.25.2 255.255.255.252
!
interface Serial0/1
 ip address 10.10.45.102 255.255.255.252
!
router ospf 234
 network 10.0.0.0 0.255.255.255 area 10
```

   - ❍ **A.** Only interface Fast Etherent 0/0's subnet will be associated into OSPF area 10.
   - ❍ **B.** Only interface Serial 0/0's subnet will be associated into OSPF area 10.
   - ❍ **C.** Only interface Serial 0/1's subnet will be associated into OSPF area 10.
   - ❍ **D.** None of the above.

9. What will be the result of the following two configurations on two separate routers?

```
RouterA(config)#router eigrp 29
RouterA(config-router)#no auto-summary
RouterA(config-router)#network 172.21.0.0 0.0.255.255
RouterB(config)#router igrp 29
RouterB(config-router)#network 172.18.0.0
```

   - ❍ **A.** Network 172.17.0.0 will have an administrative distance of 170 in Router A.
   - ❍ **B.** IGRP and EIGRP will not work because EIGRP is classless.
   - ❍ **C.** Only EIGRP routes will show because it has a lower administrative distance than IGRP.
   - ❍ **D.** The 29 is the process ID and is only locally significant.

10. Which characteristic does not apply to EIGRP and OSPF?

   - ❍ **A.** The timers for hello/dead are different depending on the topology.
   - ❍ **B.** Both routing protocols support VLSM, router summarization, and discontiguous networks by default.
   - ❍ **C.** Both routing protocols have a routing table, neighbor table, and topology table.
   - ❍ **D.** Both routing protocols discover neighbors by sending hellos to a multicast address.

Answers to Review Questions

1. The OSPF Router ID is what the router uses to know the rest of the OSPF routing domain. The highest IP address of the logical loopback interfaces is used at the startup of the OSPF routing process to determine the OSPF Router ID. If no loopback interfaces are configured or enabled, the router uses the highest IP address of an active physical interface.
2. The Designated Router is elected as broadcast and non-broadcast multi-access networks to minimize the amount of routing update overhead. On each network segment, the router with the highest interface priority (default is 1) is elected to be the DR, and the router with the interface with the second-highest priority is the BDR. In cases where the interface priorities are tied, the highest Router ID is used as a tiebreaker.
3. OSPF areas serve as a way to segment an OSPF routing domain into smaller routing systems to reduce the amount of routing overhead and confine topology changes. Area 0 is known as the backbone area, to which all other areas must connect.
4. The DUAL algorithm keeps track of the advertised distance and the feasible distance for each network in the topology table. The lowest feasible distance to a destination is known as a successor route and is the network that is put in the routing table. If the router receives an update that has an advertised distance less than the successor route's feasible distance, that entry becomes the feasible successor, which is used in case the successor route fails.

5. To configure OSPF and EIGRP, you must enter the routing process, using the `router` keyword followed by the routing protocol. In the case of OSPF, you must also specify a process ID to locally identify the instance of OSPF. The valid range of OSPF process IDs is between 1 and 65535 and does not need to match in all router configurations. On the other hand, EIGRP requires that you specify an autonomous system number that does have to match in all router configurations.

   After you are in the routing process, you advertise the connected networks with the `network` command. EIGRP configurations require that you enter the directly connected classful network(s) after the `network` keyword. Conversely, OSPF configurations require that you specify the network ID followed by the wildcard mask. Following the wildcard mask, you must also use the `area` keyword, followed by the area to which that network belongs.

Answers to Exam Questions

1. **C**. For OSPF to form a neighbor relationship, the hello/dead timers, stub flag, authentication password, and area ID must match. Because the output shows the received timers are different from the configured, the timers must be misconfigured. Answer A is incorrect because OSPF is a classless routing protocol. Answer B is incorrect because Area 51 is an area within the acceptable ranges of 0–65535. Answer D is incorrect because 10.1.42.100 does not need to be a DR to send hello messages.

2. **B.** The Router ID is chosen based upon the highest active virtual loopback address. If no loopback is present, then the highest physical IP address is chosen when the OSPF process starts. Answer A is true because the output indicates that this router's interface is the DR, which listens to 224.0.0.6. Answer C is true also because this interface is connected to Area 51, not Area 0. Answer D is correct because all OSPF routers (including the DR and BDR) listen to hellos on 224.0.0.5.

3. **D**. Given the customer requirements, D is the only viable option. Answers A and B aren't good choices because they require fast convergence. Answer C is tempting, but the fact that they have Nortel routers cancels out EIGRP and IGRP because they are Cisco proprietary.

4. **B, D.** The topology table shows that 192.168.1.31 is advertising (advertised distance) a metric of 2297856. Because that advertised distance is larger than the feasible distance of the successor route (281600), it cannot be a feasible successor. Answer A is incorrect because the subnet is not in an active state. Answer C is tricky because this number with the slash is not the administrative distance, as you would see in a routing table. It is the advertised distance followed by the feasible distance.

5. **A.** The network ID for Serial 0/0's subnet should be 192.168.1.4, and the wildcard mask for a 255.255.255.252 subnet mask is 0.0.0.3. Answer B is false because the type of area has no bearing on this configuration. Answer C is false because OSPF does not require a command to make it classless. Answer D is false because OSPF does not use autonomous system numbers.

6. **D.** Typically, the 10.1.42.1 address would be the correct Router ID for OSPF; however, the output shows it as administratively down. Because that interface isn't active, the highest active physical IP address is used (192.168.1.5). Answer A is false because all OSPF routers use a Router ID. Answer B is incorrect because it is not the highest active IP address. Answer C would be correct if the interface were not administratively shutdown.

7. **A**. To calculate OSPF cost, you take 10^8/bandwidth in bps. Thus, 100000000/512000 = 195. Answer B is the cost for a link speed of 640Kbps. Answer C is the cost for 10Mbps Ethernet. Answer C is the cost for a T1.

8. **D.** Because the wildcard mask is configured to allow any network starting with 10.x.x.x to be in the OSPF routing process, all interfaces are applied in this configuration. Answers A, B, and C are incorrect because the wildcard mask encompasses all three of the networks assigned to the interfaces.

9. **A**. EIGRP automatically redistributes IGRP networks as long as the AS number matches. When that occurs, the network is tagged as external, which has an administrative distance of 170. Answer B is incorrect because IGRP and EIGRP can interoperate if their autonomous system numbers match. Answer C is false because the EIGRP automatically redistributes the IGRP networks when the autonomous system numbers match. The 29 is the EIGRP and IGRP autonomous system number, making D an incorrect answer.

10. **B**. EIGRP is not classless by default. You must configure the `no auto-summary` command for it to support VLSM, router summarization, and discontiguous networks. Answer A is a true statement because OSPF and EIGRP both have different hello/dead intervals, depending on the topology to which the interfaces are connected. Answer C is true because EIGRP and OSPF both have a routing, topology, and neighbor table. Answer D is true because OSPF and EIGRP both discover neighbors by sending hello messages to a multicast address.

Suggested Readings and Resources

1. Zinn, Alex. *IP Routing: Packet Forwarding and Intra-domain Routing Protocols*. Addison Wesley Professional, 2002.

2. Kruepke, Keith; Cernick, Paul; Degner, Mark. *Cisco IP Routing Handbook*. Hungry Minds, 2000.

3. Bruno, Anthony and Kim, Jacqueline. *CCDA Exam Certification Guide*. Cisco Press, 2004.

4. Malhotra, Ravi. *IP Routing*. O'Reilly, 2002.

5. Sportack, Mark. *IP Routing Fundamentals (The Cisco Press Fundamental Series)*. Cisco Press, 1999.

6. "Routing Protocols," www.firewall.cx.

7. "OSPF, EIGRP," technology support on www.cisco.com.

CHAPTER 13

Access Lists

Objectives

Describe the types and functions of access lists as they relate to Cisco routers

Configure standard and extended access lists for security purposes

Verify access list configuration and operation

- Access lists are key configuration items in a Cisco router. Despite their name, they are not reserved for only security purposes. This chapter discusses the variety of uses and styles of access lists available on Cisco routers.
- The two most common types of access lists are IP Standard and Extended. This chapter discusses the configuration and application of each of these.
- A misplaced access list can devastate a Cisco network. Understanding the verification commands covered in this chapter are a key to troubleshooting and solving access list issues.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- Spend plenty of time looking over the configuration examples. Understanding the configuration of access lists is paramount to understanding many of the upcoming chapters and exam objectives.

Introduction

A packet slides smoothly across the ethernet cable, gliding through a switch as it heads to its final destination: the company accounting server. Nobody in the network suspects that this is no normal packet. Behind all the source and destination header information lies a specially engineered code designed to unleash a denial of service attack when processed by the unsuspecting Windows 2003 Server platform. Just one more router to pass through and the deed will be done. Let's pick up the dialog here:

Incoming router Ethernet interface: bang, bang! (*a loud knock is heard*)

Router processor (*yelling)*: "Source and destination please!"

Malicious packet (*in a scandalous voice*): "Yeah, I'm 10.6.9.2 headed to 10.56.100.10 on port 137…make it snappy."

* *gunshot rings out, malicious packet falls to the ground* *

Router processor (*scraping the crumpled bits into a bucket*): "Your type isn't welcome in these parts…punk."

You have just been witness to one of the most well-known uses of an access list: network traffic control. This function enables you to turn a common router into a fairly sophisticated firewall (the Dirty Harry dialog does require an IOS upgrade, however). As you might imagine, a cornerstone function like this is not only relevant for the CCNA exam, but also for Cisco network deployments worldwide.

Access List Concepts

When you look at the term *access list*, the only word that stands out is *access*. Of course, this immediately causes any technology-minded person to conjure thoughts of controlling traffic, firewalls, and intrusion detection. Although this may have been Cisco's initial intention when they created the concept of access lists, nowadays access lists are used for a plethora of functions on any Cisco device. When you hear the term *access list*, don't focus on the word *access*; rather, focus on the word *list*.

An access list is nothing more than an ordered list of `permit` and `deny` statements. Every time the router needs to refer to the list for some reason, it reads it at the top and works its way down. You can picture it like a bouncer at an upscale drinking establishment. He may have the following list in his hand:

Deny Joshua Smith

Deny Benjamin Newport

Permit people with brown hair

The bouncer is then told to screen people as they attempt to enter the establishment. Now, when the first patron attempts to enter the building, the following transcript occurs:

Bouncer: "Is your name Joshua Smith?"

Patron: "No."

Bouncer: "Is your name Benjamin Newport?"

Patron: "No."

Bouncer: "Do you have brown hair?"

Patron: "Yes."

Bouncer: "You may enter our establishment."

The next person that attempts to enter the building is subjected to exactly the same list of questions in exactly the same order. Now this leads to a major question about this story: What if someone attempted to enter the building who did not have the name Joshua Smith or Benjamin Newport, but also did not have brown hair? That person is denied. No questions asked. This is one of the cornerstone facts of access lists on a Cisco device: *If you have not been explicitly permitted, you are implicitly denied.*

EXAM ALERT

Access lists always have an implicit `deny` statement at the end of the list. This statement is never displayed and cannot be seen through any `show` command. In an access list, if you have not been explicitly permitted, you are implicitly denied.

The implicit `deny` statement is hidden at the end of all access lists, and its order cannot be changed. However, the ordering of access lists elsewhere is of great importance. It can affect everything about your access list. For example, what if in the question, "Do you have brown hair?" was listed first in the bouncer's access list? In that case, Joshua Smith or Benjamin Newport may have been permitted because they had brown hair, even though they were explicitly denied elsewhere in the list. A router stops processing an access list after an initial match statement is found. Let's leave the bouncer example behind for now and begin applying these concepts to networking.

Suppose you had defined the following access list (this is not correct syntax; rather, it is a conceptual view):

Permit host 192.168.1.50

Deny network 192.168.1.0/24

Permit host 192.168.1.100

<implicit deny>

This list would permit the host 192.168.1.50, as it intended. However, the host 192.168.1.100 would never be permitted because it is listed after the second statement in the list, which denies the entire Class C 192.168.1.0/24 subnet.

CAUTION

Depending on the IOS version you are using, there may be different ways the IOS formats access lists. In older IOS versions, the access list is arranged exactly as you enter it into the command line and cannot be reordered unless you completely erase the access list and re-create it. In modern IOS versions, the Cisco router can automatically reorder the list if you make an obvious mistake, as shown in the prior access list. In the newest versions of the IOS, the Cisco router assigns sequence numbers to each entry, allowing the addition, removal, and reordering of any line in the access list. (This is an awesome feature, which is covered later in the chapter during the discussion of named access lists.)

EXAM ALERT

For the CCNA exam, assume that the router is using an older version of the IOS that is arranged exactly as you enter it into the command line and cannot be reordered unless you completely erase the access list and re-create it.

Throughout the rest of this chapter, it is assumed that the IOS version is the same as it is on the CCNA exam. This means there is no automatic reordering of the list, lines cannot be individually removed, and the only additions that can be made are lines that are inserted at the end of the access list (this is the default when configuring the access list).

After all this, keep in mind that these are only the guidelines for creating an access list. Remember: An access list is just a list of `permit` and `deny` statements. The way in which you apply the access list defines the *function* of the access list. If you apply the access list inbound or outbound on a router interface, then the router begins to filter packets according to the instructions in the access list. If you apply the access list to your Network Address Translation (NAT) configuration, then the access list defines what IP addresses are permitted to be translated to an Internet-valid address. If you apply the access list to a dial-on-demand configuration, then the access list defines what devices or network traffic types are allowed to bring up a dial-up interface (such as a modem). I hope I am getting the point across: *An access list is nothing more than a list of* `permit` *and* `deny` *statements. How you apply it dictates what function the access list really serves.*

Functions of an Access List

At this point, we have discussed a few access list uses in passing; however, the truth is that you will rarely encounter a major function of a Cisco router that does not require an access list in some way. For the CCNA exam, you should be aware of the following access list functions:

- Packet filtering
- Quality of service (QoS)
- Dial-on-demand routing (DDR)
- Network Address Translation (NAT)
- Route filtering

EXAM ALERT

Although you may be required to understand some of the common applications of access lists on the CCNA exam, you will be required only to demonstrate proficiency in configuring access lists for packet filtering, DDR, and NAT.

Packet Filtering

Of course, packet filtering is the most well-known application of access lists. This access list application enables you to turn your router into a basic firewall. By using these foundation IOS features, you can begin filtering traffic inbound or outbound from any interface on your router. Depending on the type of access list you use, you can filter traffic based on the source address (standard access list) or based on the source and destination address, along with protocol and port number (extended access list).

CAUTION

As soon as you apply an access list for packet filtering inbound or outbound on an interface, the router must begin comparing every packet against the access list. Depending on the size and matching criteria of your access list, this can cause significant processor load.

Quality of Service

With the emerging technology of Voice over IP (VoIP), it has become necessary to give unequal treatment to network traffic. For example, if a router is receiving a considerable amount of Web surfing traffic (HTTP) and a VoIP telephone call attempts to come through, the VoIP conversation should receive prioritization over the HTTP traffic to ensure high-quality voice conversations; even if it means dropping a few of the HTTP packets. This is the concept of Quality of Service (QoS). The QoS matching methods rely extensively on access lists to define what types of traffic are prioritized over others. In this case, you see access lists in the view that they are *permitting* traffic to be prioritized and *denying* others from gaining network priority.

Now, not all QoS methods seek the good of the traffic they match. There is a QoS method called *traffic policing* that limits the bandwidth available to a certain application. For example, a network may have problems with users using peer-to-peer file sharing applications, such as Napster, Kazaa, or Morpheus, and depleting the Internet connection bandwidth. In this case, a QoS policing policy can be defined to limit the bandwidth available to these application types. Here's where the access list irony can be seen: The access list matches these applications (permits) and then restricts the amount of bandwidth they can use. The applications that are not matched (denied) do not have any bandwidth restrictions placed on them. In this access list function, from the application's point of view, it is better to be denied than permitted. Are you beginning to see that an access list is just a list of statements? How you apply that access list determines the effect it has on the network traffic.

Dial-on-Demand Routing

Dial-on-demand routing encompasses any type of temporary (not always on) connection. Despite their "legacy" stereotype, dial-up connections are here to stay because no other connection type has proved to be as reliable as the circuit switched technology. Although many people immediately think of modem connections, ISDN BRI and PRI services also fit this profile. In recent years in the United States, the number of ISDN BRI connections has dropped drastically because the emergence of cheaper connections that use DSL and cable modem technology. However, the number of ISDN connections overseas is enormous.

EXAM ALERT

Because of the continued popularity of dial-on-demand technology for overseas and backup connections, a good understanding of the Cisco configuration of dial-on-demand technology is required for the CCNA exam.

Now you might wonder…what does dial-on-demand routing have to do with access lists? Well, in this case, access lists do not define what traffic is permitted across the dial-on-demand connection; rather, it defines what traffic is interesting enough to bring up the line. If you ever saw the movie *Wayne's World* in the early 90's, there is a moment where the singer Alice Cooper walks by Wayne and Garth. Immediately, they fall to the ground yelling, "We're not worthy!" In the same sense, you will create an access list that defines traffic that is "worthy" to dial the connection. Some ISDN connections charge a per-minute cost for being connected, so it may pay off to limit dial-up connections to certain traffic sources or packet types before the line is engaged.

Network Address Translation

Network Address Translation (NAT) has been in widespread use for over a decade, and yet still never ceases to amaze me. There is perhaps no other configuration that gives you as much satisfaction in "beating the system" as NAT (other than using your neighbor's wireless access point, of course). NAT theoretically allows more than 60,000 internal hosts to share a single, registered, public IP address to access the Internet. This has overcome the current public IP address shortage and extended the life of TCP/IP version four for years beyond what many thought possible.

EXAM ALERT

Because of the overwhelming popularity of NAT deployments, it is one of the newest topics to be added to the CCNA exam.

The way access lists are used in NAT is similar to the way they were used in dial-on-demand routing. The access lists define what source addresses are "worthy enough" to be transmitted. A `permit` statement in the access list applied to a NAT configuration says, "This host (or subnet) is permitted to be translated with NAT." A `deny` statement in the same access list says, "This host (or subnet) is *not* permitted to be translated with NAT." A `deny` statement does not prevent traffic from being sent; rather, it denies it from being translated with NAT before it is sent.

Route Filtering

The final access list application covered in this text is route filtering. The routing protocols discussed so far, such as RIP, IGRP, EIGRP, and OSPF, all make it their mission to pass all known network routes to neighboring routers. In some network situations, this could cause a problem. Perhaps you don't want the router to pass *all* routes to *every* router on your network. For example, you might have some edge routers that connect to a partner company or an Internet-based peer. You could protect your network by using an access list to filter the routes that are sent and received to and from this peer.

A configuration known as a *distribute list* is used most often to apply the access list used for this function. In order to set this up, you would configure an access list permitting only the networks you would like to send or receive (or denying the networks you would not like to send or receive, depending on your strategy). As discussed before, creating the access list does absolutely nothing, functionally speaking; it must be applied to take action. In the case of route filtering, you would apply the access list under router configuration mode, `Router(config-router)`, for the routing protocol you would like to filter, by using the `distribute-list <access_list_number> <in|out>` syntax. Access list numbers are used to

identify the access list you are referencing. For example, if I wanted to keep my routing protocol from sending the routes I have listed as "deny" routes in access list #50, I would use the syntax:

```
Router(config-router)# distribute-list 50 out
```

If I wanted to keep my router from receiving the routes I had listed as "deny" routes in access list #50, I would use the syntax:

```
Router(config-router)# distribute-list 50 in
```

Standard Access Lists

Cisco provides two primary categories of IP-based access lists: standard and extended. Standard access lists can permit or deny traffic based only on the source IP address. For example, I can set up an access list that says the host `192.168.1.1` is denied. However, if I use a standard access list to accomplish this, I can never say what destination the host is denied from reaching or what protocol it is denied from using; I can say only that they are denied. Period. Therefore, the interface on the router where you apply the standard access list can make all the difference. The benefits of using standard access lists are the simplicity and resource usage. Because the standard access lists filter based only on the source IP address, the router processor and memory resources are not as taxed as they are when you use an extended access list.

Configuration of Standard Access Lists

Whenever you decide to begin configuring any type of access list, remember this wisdom from the Cisco elders: Context-sensitive help is your friend. If you have not yet become accustomed to entering a question mark after each step of your configuration, now is the perfect chance to gain that familiarity. In these initial examples, the question mark is entered after each command to find out what arguments the router expects next.

The standard access list is created from Global Configuration mode with the `access-list` command, so that's where this example begins:

```
Neo(config)#access-list ?
  <1-99>            IP standard access list
  <100-199>         IP extended access list
  <1100-1199>       Extended 48-bit MAC address access list
  <1300-1999>       IP standard access list (expanded range)
  <200-299>         Protocol type-code access list
  <2000-2699>       IP extended access list (expanded range)
  <700-799>         48-bit MAC address access list
  dynamic-extended  Extend the dynamic ACL absolute timer
```

Just by looking at the categories of `access-list`, you can tell what protocols this router supports. In this case, the router supports the IP-only feature set. Otherwise, you would see access list categories for each protocol (such as IPX/SPX, Appletalk, or Decnet). Notice the number ranges for each access list; the type of access list you are going to create depends on what number you type after the `access-list` command. If you were to type **`access-list 25`**, the syntax that followed would be that of a standard access list because you chose a number between 1 and 99. Likewise, if you were to enter the command **`access-list 135`**, the syntax that followed would be that of an extended access list because you chose a number between 100 and 199.

EXAM ALERT

Knowing that access list numbers 1–99 represent standard access lists and 100–199 represent extended access lists increases your chances of passing the CCNA exam by at least 1.2%.

In addition to dictating the type of access list that will be created, the access list number represents your access list as a whole. As the name "access *list*" implies, each access list number can contain many individual statements. For example, you could create access list 4, which contains 3000 specific lines dictating what source IP addresses are permitted and denied.

Even though each access list can contain many statements, if you have a router with an extremely complex configuration, you could run out of access lists. For this reason, Cisco created the expanded access list ranges for both standard (1300–1999) and extended (2000–2699) access lists, as shown in the prior syntax. This ensures that routers will never run out of IP access list numbers again. The configuration example continues by using access list number 25:

```
Neo(config)#access-list 25 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
```

The first decision you need to make about this access list entry is whether the statement will permit or deny. Remember, at the bottom of every access list is the invisible implicit `deny`, so you need to permit at least one thing. Imagine that you want to permit the host 10.1.1.5:

```
Neo(config)#access-list 25 permit ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address
```

You are now given the option to either enter an IP address, use the `any` keyword to match any source host address, or to use the `host` keyword to match a single host address. You might ask the question at this point, "So do I enter the IP address 10.1.1.5 here, or the keyword `host`?"

You can enter either one. Try entering the IP address first, and then the example returns to the `host` command:

```
Neo(config)#access-list 25 permit 10.1.1.5 ?
  A.B.C.D  Wildcard bits
  log      Log matches against this entry
```

Because the `host` keyword was not used, the router is now prompting for the correct wildcard bits. This may bring back bad memories of the OSPF routing protocol, which is another major router configuration that relies on wildcard masks (also called inverse masks) to specify OSPF interface(s). Just to review, a wildcard mask is exactly the opposite of a subnet mask. The zero bits (0) of a wildcard mask say, "Look at these," whereas the one bits (1) of a wildcard mask say, "I don't care." For example, if you entered the IP address 172.16.0.0 with a wildcard mask 0.0.255.255, the router would look at the 172.16 digits (because they matched the binary zeros in the wildcard mask) and would not care about the 0.0 digits (because they matched the binary ones in the wildcard mask). This means that the address 172.16.90.100 would match because all the router cares about is that the address starts with 172.16. This now brings us back to the configuration. You need to create a wildcard mask that matches exactly the IP address 10.1.1.5. It would be safe to say that you want the router to look at every single octet of that IP address, so the appropriate wildcard mask would be 0.0.0.0. Here's a look at the complete line of syntax:

```
Neo(config)#access-list 25 permit 10.1.1.5 0.0.0.0 ?
  log  Log matches against this entry
  <cr>
```

Notice that the only options context-sensitive help gives you is to enter the `log` command (which writes a record to the router log file anytime this entry is matched) or to press Enter. If you choose the latter, you enter your first line into an access list. Let's work through the syntax one more time to add a second statement to the access list. This time, you want to permit the entire 192.168.77.0/24 subnet:

```
Neo(config)#access-list ?
  <1-99>       IP standard access list
  <100-199>    IP extended access list
  <1000-1099>  IPX SAP access list
  <1100-1199>  Extended 48-bit MAC address access list
  <1200-1299>  IPX summary address access list
  <1300-1999>  IP standard access list (expanded range)
  <200-299>    Protocol type-code access list
  <2000-2699>  IP extended access list (expanded range)
  <300-399>    DECnet access list
  <400-499>    XNS standard access list
  <500-599>    XNS extended access list
  <600-699>    Appletalk access list
  <700-799>    48-bit MAC address access list
  <800-899>    IPX standard access list
```

```
  <900-999>    IPX extended access list
  rate-limit   Simple rate-limit specific access list
```

Notice the IOS on the Neo router has been upgraded to a version that supports a few more protocols than the prior IOS version. You will now continue on through this configuration of permitting the entire 192.168.77.0/24 subnet, using context-sensitive help to guide you through each additional piece of syntax.

```
Neo(config)#access-list 25 ?
  deny    Specify packets to reject
  permit  Specify packets to forward

Neo(config)#access-list 25 permit ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address

Neo(config)#access-list 25 permit 192.168.77.0 ?
  A.B.C.D  Wildcard bits
  log      Log matches against this entry
  <cr>

Neo(config)#access-list 25 permit 192.168.77.0 0.0.0.255 ?
  log  Log matches against this entry
  <cr>

Neo(config)#access-list 25 permit 192.168.77.0 0.0.0.255
Neo(config)#
```

The second line has just been added to access list 25. Notice that the wildcard mask 0.0.0.255 tells the router to look at the 192.168.77 (the first three octets of zero bits in the wildcard mask), and to ignore the last octet (because of the one bit in the last octet of the wildcard mask). You can now use a couple of `show` commands to verify your work: `show ip access-lists` or `show running-config`.

```
Neo#show ip access-lists
Standard IP access list 25
    permit 10.1.1.5
    permit 192.168.77.0, wildcard bits 0.0.0.255


Neo@show running-config
Building configuration...
<…output omitted…>
access-list 25 permit 10.1.1.5
access-list 25 permit 192.168.77.0 0.0.0.255
```

Initially, it looks as if the router lost the wildcard mask that was added for the 10.1.1.5 host. The Cisco router removes the 0.0.0.0 because an IP address without the wildcard mask is assumed to be an individual host anyway.

EXAM ALERT

Some IOS versions completely remove the wildcard mask as shown in the text, whereas other, newer IOS versions insert the `host` keyword, such as in the following:

```
access-list 25 permit host 10.1.1.5
```

To be safe on the CCNA exam, always use either the wildcard mask or the `host` keyword when configuring your access list in a simulation. Never just type in an IP address and press Enter. Although this may work on real Cisco equipment, the test simulations may deduct points.

Placement of Standard Access Lists

As mentioned before, you can create access lists all day on your router and no functional change will ever occur. Access list take effect only when you apply them in some way. This chapter focuses on applying access lists for security purposes. Access lists can be placed inbound or outbound on any router interface. When applying `access-list` for security, remember this mantra:

One access list…

…per protocol,

…per interface,

…per direction

You must take these rules into account when deciding how to engineer the access list. Here is what the mantra means: You must design a single access list to include all the possible `permit` and `deny` statements you need for each protocol (such as TCP/IP or IPX/SPX, not subprotocols such as TCP or UDP) on a single interface for the inbound or outbound direction. You are allowed to apply only one access list number inbound and one access list outbound.

Finally, keep this in mind before you apply an access list: The access list goes into effect *immediately* when applied. Before you apply the access list, check the access list thoroughly to make sure you have allowed enough traffic to pass through. The most common mistake made by network administrators is to create an access list and quickly list the items they want to deny. They then apply this to an interface, forgetting about the implicit deny at the end of the access list. The access list then acts as a "deny all" statement for the interface, effectively shutting down the communication on that interface. If this is done in a production network, it can have devastating effects.

The other common mistake is to make changes to an access list while it is applied to an interface. Although this can be done successfully, it is not recommended. The changes go into effect immediately after you press the Enter key, not giving you the time you need to take the entire access list into consideration.

NOTE

Many Cisco administrators create their access lists in a text editor such as Notepad, which enables you to reorder the statements as you see fit before the access list is created and applied.

With all these cautions in place, the syntax to apply the access list to the interface is simple. Use the following syntax from interface configuration mode:

```
Router(config-if)#ip access-group <access_list_number> <in/out>
```

The `<in/out>` keyword tends to be the most confusing portion of this syntax. The `in` keyword filters inbound traffic to the interface, whereas the `out` keyword filters outbound traffic from the interface. The easiest way to remember this is to picture yourself as a router. Seriously, stand up and say out loud, "I am a router." Now hold your arms out and picture them as router interfaces. Your left arm is a FastEthernet connection to a switch. Your right arm is a serial link to a remote office. If you apply an access list on your FastEthernet interface in the IN-bound direction, it filters traffic coming from the switch, up your arm, and into your body. If you apply it OUT-bound on your FastEthernet interface, you are filtering traffic leaving your body, and going out to the switch. By putting yourself in the place of the router, you will get the direction right every time.

EXAM ALERT

Cisco testing procedures do not currently restrict you from standing and waving your arms wildly in the testing center as long as you do not hit any other test takers.

For example, let's apply access list 25 that was created previously to a router's FastEthernet 0 interface in the inbound direction. Just as a refresher, I list the syntax used to create the access list first, and then apply it to the interface:

```
Trinity(config)#access-list 25 permit 10.1.1.5 0.0.0.0
Trinity(config)#access-list 25 permit 192.168.77.0 0.0.0.255
Trinity(config)#interface fastethernet 0
Trinity(config-if)#ip access-group 25 in
```

The access list is now applied and in effect. The router permits the host 10.1.1.5 and anyone from the network 192.168.77.0/24 to enter the router's FastEthernet 0 interface (inbound)

from an attached switch. The implicit `deny` keeps any other devices from entering FastEthernet 0.

Standard Access List Examples

Now let's start putting this newfound knowledge into practice. Use the topology shown in Figure 13.1 to see a visual diagram for this example.

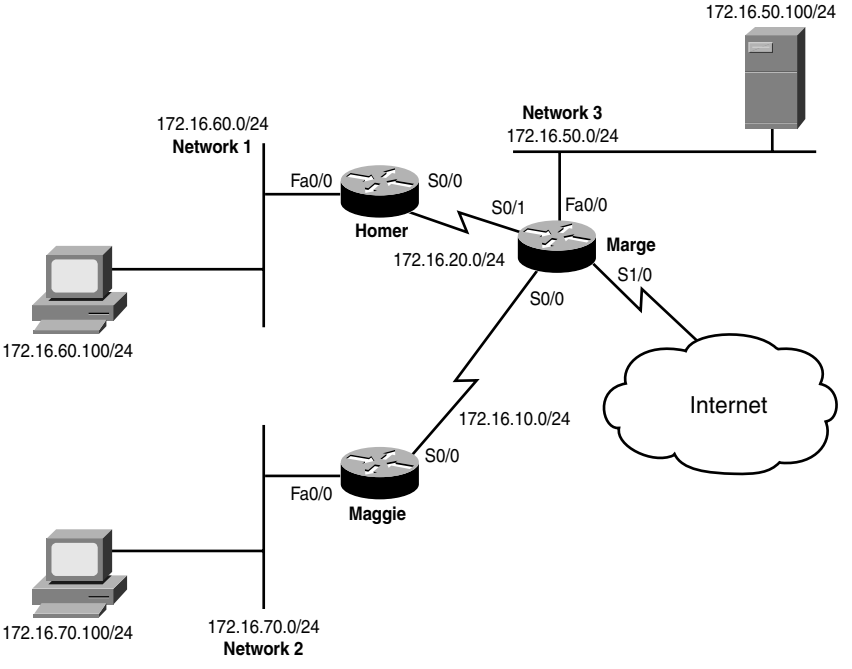


FIGURE 13.1
Standard access list deployment.

Isolating Networks

To keep devices on Network 3 from accessing devices on Network 1 the first thing you must determine is where in the network you want to create the access list. When configuring standard access lists, the best practice is to create and apply the access list on the router closest to the *destination*. Standard access lists cannot dictate what the source IP addresses are permitted or denied; they can say just that they are permitted or denied. By applying the access list close to the destination, you effectively limit the scope of effect that the access list has. If you apply it too close to the source, you may deny or permit too much. You will see more examples of this as you work through applying more access lists.

EXAM ALERT

Know that the best practice of standard access lists is to apply them on the interface closest to the destination.

When you look at the figure, you can see that the Homer router is closest to the destination (Network 1), so that is the place to begin configuration:

```
Homer>enable
Homer#configure terminal
Homer(config)#access-list 30 deny 172.16.50.0 0.0.0.255
```

A line has been added to the access list to block Network 1. If the access list is left like this, it will also deny all other traffic because of the implicit deny at the end, so you need to add a statement that permits all other networks to reach Network 1:

```
Homer(config)#access-list 30 permit any
```

TIP

The `any` keyword is a shortcut, just as the `host` keyword is. You could accomplish the same thing by using the statement:

```
access-list 30 permit 0.0.0.0 255.255.255.255
```

When you have a wildcard mask of all 255s, the router does not care what you enter for the IP address (which is all zeros in this case, but could have been anything). This is equivalent to a `permit any` statement. Use whichever one you feel more comfortable with.

You have created the access list; now it's time to apply it. Looking back at the figure, there are two possible places to apply this access list on the Homer router: inbound on the S0/0 interface, or outbound on the Fa0/0 interface. Using the best practice of applying closest to the destination, this is how to do the latter:

```
Homer(config)#interface fastethernet 0/0
Homer(config-if)#ip access-group 30 out
```

Voilà! This part of the example is accomplished. Now here's the complete code without the commentary:

```
Homer>enable
Homer#configure terminal
Homer(config)#access-list 30 deny 172.16.50.0 0.0.0.255
Homer(config)#access-list 30 permit any
Homer(config)#interface fastethernet 0/0
Homer(config-if)#ip access-group 30 out
```

Isolating a Network from Specific Hosts

You now need to prevent just two devices (the Network 1 and 2 hosts) from accessing Network 3. If you remember the rule of applying the standard access list closest to the destination, you know that the configuration should be performed on the Marge router:

```
Marge>enable
Marge#configure terminal
Marge(config)#access-list 45 deny host 172.16.70.100
Marge(config)#access-list 45 deny host 172.16.60.100
Marge(config)#access-list 45 permit any
```

Now that the access list has been created, you have to decide where to apply it. Initially, you might eye the S0/0 interface inbound. If you applied it there, the host 172.16.70.100 and 172.16.60.100 would be denied as soon as they tried to make their way into the S0/0 interface of Marge. Although this would prevent the hosts from reaching Network 3, it would also block them from accessing Network 1 and the Internet (because they cannot even enter the Marge router). Aha! Do you now see why it is so important to apply the standard access list close to the destination? In this case, you need to apply it to the FastEthernet 0/0 interface, outbound:

```
Marge(config)#interface fastethernet 0/0
Marge(config-if)#ip access-group 45 out
```

Perfect. This part of the example is complete.

Isolating the Internal Network from the Internet

The servers on Network 3 contain confidential information and should not be accessible from the Internet. Assuming your entire internal network uses 172.16.0.0/16 addresses, this configuration should maintain the isolation of Network 3 from Network 1 and 2 hosts. Wow! This requires a little thought. You have no idea what addresses may be trying to come in from the Internet, so you have to reverse your strategies. So far, you have been denying a host or network and permitting everything else. You must now permit what you know and deny everything else, still keeping in mind that you cannot allow the two hosts from the previous objective to access the server. Start on the Marge router in Global Configuration mode and remove the access list applied previously:

```
Marge(config)#no access-list 45
```

CAUTION

Removing the access list by using the `no access-list <number>` command does not remove the `access-group` command from the interface. The access list is still applied! Thankfully, an empty access list allows all traffic (this overrules the implicit `deny` statement). However, as soon as you add one line to the access list, the implicit `deny` statement is reapplied with all its fury. It is a very good idea to un-apply the access list from the interface while you make changes.

Whew! That caution popped up at just the right place. Let's follow that advice:

```
Marge(config)#interface fastethernet 0/0
Marge(config-if)#no ip access-group 45 out
```

Now you can start on a new access list. First, deny the specific hosts that should not be able to reach Network 3:

```
Marge(config)#access-list 45 deny host 172.16.70.100
Marge(config)#access-list 45 deny host 172.16.60.100
```

Super. Now that they're taken care of, you can permit the rest of the 172.16.0.0/16 subnet (all the internal networks):

```
Marge(config)#access-list 45 permit 172.16.0.0 0.0.255.255
```

Notice that the wildcard mask cares about only the first two octets of the IP address, thus permitting any IP address that begins with 172.16. This is why the `deny` statements for the hosts were listed first. Otherwise, this line would have permitted them. With the one `permit` statement added, you have finished creating the access list. The implicit `deny` should catch any other networks not specified (including those coming from the Internet). Finally, using best practices, you need to apply this list close to the destination:

```
Marge(config)#interface fastethernet 0/0
Marge(config-if)#ip access-group 45 out
```

Awesome! This just keeps getting better. Mission accomplished.

Restricting VTY Access

Now here's a new application for an access list. So far, access lists have been applied inbound and outbound on interfaces, but access lists can also be applied to VTY lines (which are used for Telnet). This example will allow only the host on Network 2 to Telnet to the Marge router. The command syntax to do this differs slightly from applying an access list to an interface. Instead of using the `ip access-group` command, use the `access-class` command.

After referring back to the figure, you can see that the host on Network 2 has the IP address 172.16.70.100. Here's the configuration:

```
Marge(config)#access-list 55 permit host 172.16.70.100
Marge(config)#line vty 0 4
Marge(config-line)#access-class 55 in
```

That's it! The implicit `deny` blocks all other hosts from accessing your VTY lines. This brings up a huge tip.

CAUTION

If you are configuring access lists on your router remotely, be sure to allow your remote Telnet session access into the router in the access list. It is a very common mistake to create an access list that kills the remote Telnet session and requires the administrator to drive to the site (or contact someone on-site) to reconfigure the router through the console port. It is, therefore, a good practice to issue the following command before applying an access list remotely:

```
Router# reload 5
```

This instructs the router to reboot itself in 5 minutes if there is no administrative intervention. This way, if you lock yourself out of the router, it reboots and sets its configuration back to what it was before you applied the access list. If the access list applies successfully without limiting remote access, be sure to issue the `no reload` command to stop the automatic reboot countdown.

Extended Access Lists

"Beware of the extended access list!" This grave warning comes from many CCNA testers who have gone before you. Out of all the topics on the CCNA exam, not one has come close to tripping up candidates more than the extended access list. With most things in Cisco, the difficulty comes in the concept and the syntax is quite simple. However, when it comes to the extended access lists, the concepts are fairly straightforward; it is the syntax that can be a monster. Fear not, my brave CCNA studier. After working through this section, you will feel quite comfortable with extended access lists.

Configuration of Extended Access Lists

After you have set up a few standard access lists, you'll have the configuration mastered. Standard access lists allow you to permit or deny network traffic based only on the source address. On the other hand, extended access lists allow you to permit or deny traffic based on the sub-protocol, source address, source port number, destination address, and destination port number—and that's just what is on the CCNA exam. An extended access list can even filter based on time of day or user authentication. Now if you imagine fitting all those parameters into a single line of syntax, you begin to understand why extended access list syntax can become quite long.

Before we get deep into each step of the syntax, let's take a step back and look at extended access list parameters from a distance. First off, extended access lists are identified by the numbers 100–199, as shown by context-sensitive help:

```
Neo(config)#access-list ?
  <1-99>            IP standard access list
  <100-199>         IP extended access list
  <1100-1199>       Extended 48-bit MAC address access list
```

```
  <1300-1999>       IP standard access list (expanded range)
  <200-299>         Protocol type-code access list
  <2000-2699>       IP extended access list (expanded range)
  <700-799>         48-bit MAC address access list
  dynamic-extended  Extend the dynamic ACL absolute timer
```

From a broad view, an extended access list requires three major parameters: a protocol, source information, and destination information. The general syntax looks like this:

```
Access-list <100-199> <protocol> <source_information>
<destination_information>
```

Now let's walk through the creation of an extended access list, one piece at a time. This example uses access list 150, putting it smack in the middle of the access list range. For this example, web access should be allowed for one host, 10.1.1.5.

```
Neo(config)#access-list 150 ?
  deny     Specify packets to reject
  dynamic  Specify a DYNAMIC list of PERMITs or DENYs
  permit   Specify packets to forward
  remark   Access list entry comment
```

The first thing you notice is that you have the standard `<permit/deny>` option, but now a `dynamic` option has been added to the list. Although dynamic access lists are beyond the scope of the CCNA certification, the concept is pretty amazing: You can have an access list that allows minimal outbound or inbound access. If you have a user that needs access to a network through your router, you can authenticate that user to the router with a pre-determined username and password. If the authentication is successful, a dynamic entry is added to the access list allowing the device access for a certain amount of time, after which the access list entry is removed. Amazing stuff!

Because extended access lists have the same implicit `deny` statement as standard access lists, you must permit at least one type of packet or all traffic is denied. You can now continue on through this configuration of permitting web access for the host 10.1.1.5, using context-sensitive help to guide you through each additional piece of syntax.

```
Neo(config)#access-list 150 permit ?
  <0-255>  An IP protocol number
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  igmp     Internet Gateway Message Protocol
  ip       Any Internet Protocol
  ipinip   IP in IP tunneling
  nos      KA9Q NOS compatible IP over IP tunneling
  ospf     OSPF routing protocol
```

```
  pcp      Payload Compression Protocol
  pim      Protocol Independent Multicast
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
```

Now the syntax is starting to look quite a bit different from the standard access list. You now have the choice of what protocol to permit or deny.

EXAM ALERT

Although the list is quite exhaustive, for the CCNA exam you need to be concerned with only the following four protocols: IP, TCP, UDP, and ICMP.

These protocols are roughly defined as the following (the applications are explained further during the discussion on port numbers):

- **IP**—Permits or denies source/destination addresses that use the entire TCP/IP protocol suite. Using this keyword permits or denies *all* access from a source to a destination.
- **TCP**—Permits or denies source/destination addresses that use TCP-based applications. The most common applications include FTP, Telnet, SMTP, and HTTP.
- **UDP**—Permits or denies source/destination addresses that use UDP-based applications. The most common applications include DNS and TFTP.
- **ICMP**—Permits or denies source/destination addresses that use ICMP-based applications. The most common applications include Echo, Echo-Reply, and Unreachables.

In this example, the access list needs to permit HTTP access, which uses the TCP protocol.

```
Neo(config)#access-list 150 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

You are now prompted for the source IP address information. Just as with a standard access list, you have the option of entering a source IP address followed by a wildcard mask, using the `host` keyword to designate an individual host, or using the `any` keyword to designate all hosts. This example uses the `host` keyword to designate an individual PC.

```
Neo(config)#access-list 150 permit tcp host 10.1.1.5 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
```

```
gt       Match only packets with a greater port number
host     A single destination host
lt       Match only packets with a lower port number
neq      Match only packets not on a given port number
range    Match only packets in the range of port numbers
```

From this next context-sensitive help prompt, it looks as if there is a prompt to enter either a destination IP address or port information. BEWARE! This is where most extended access list mistakes are made! As you can see from the context-sensitive help, you can enter many forms of port information: a port equal (eq) to a certain number, greater than (gt) a certain number, less than (lt) a certain port number, a range of port numbers, and the list goes on and on. Initially, you might think that this is the place to permit the port for HTTP access (port 80). Unfortunately, that thought process is incorrect. This area is where you discover the strange and fascinating phenomena known as a source port number.

By this point, you most likely know the commonly used port numbers such as TCP port 21 for FTP, TCP port 80 for HTTP, and so on. However, most administrators never learn that these are actually destination port numbers. For any TCP/IP-based communication, there is always a destination *and* source port number. Here's how it works: imagine you have a PC connected directly to the Internet. You would like to use a web browser to access the latest news headlines; however, like most technology-based individuals, you also have 10 other web browser instances minimized at the bottom of your task bar. You open a new web browser (instance #11) and access the news website. Sure enough, the web browser window fills with text and pictures of all the latest news and events. Now how in the world did your computer know to fill *that* web browser window (#11) with the information rather than one of the other 10 you had minimized at the bottom of the screen? The answer is in the source port information. As soon as you opened the web browser #11, Windows (or whatever operating system you are using) generated a unique source port number for that window. Whenever it attempts to communicate with the destination host, it uses its unique source port number. The source port number that the operating system chooses is always above the range of "well known" ports (which range from 0–1023).

For example, imagine that the news website you want to communicate with is Fox News (www.foxnews.com), and your PC's IP address is 204.1.9.52. When the web browser opens, it generates a random source port of 3382. As shown in Figure 13.2, when the web request is sent from your PC to the Fox News web server, it is sent to the destination www.foxnews.com:80 (this is known as a socket—the combination of a destination IP address with a destination port number). It has a source of 204.1.9.52:3382. When the Fox News website communicates back to your PC, it uses a destination of 204.1.9.52:3382 with a source address of www.foxnews.com:80.

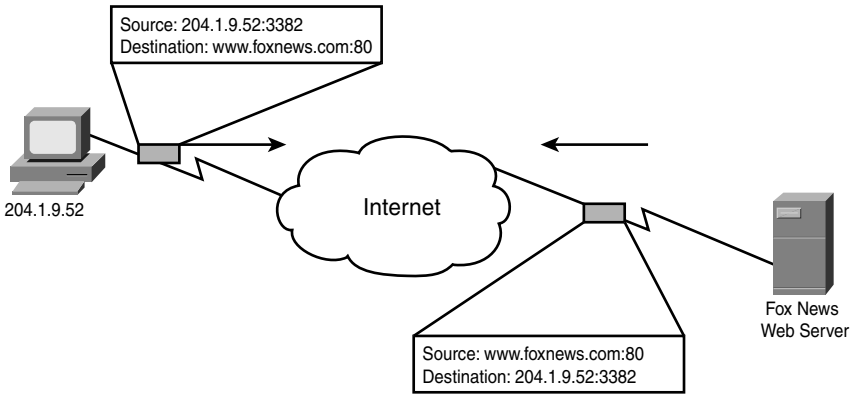


FIGURE 13.2 TCP communication using source and destination port numbers.

Back to the task at hand. If you enter port number information after the source IP address, you permit or deny *source* port information.

NOTE

You will rarely, if ever, know a network device's source port number information. This number is randomly generated by the host's operating system.

By omitting the any source port information and continuing on to the destination address specifications, the Cisco router assumes all source ports are permitted. This example allows web access. The destination address is the entire Internet address space. This can be easily summed up with the destination address keyword of `any`. The following code enters the `any` keyword and continues to use the context-sensitive help to guide you through each additional piece of syntax.

```
Neo(config)#access-list 150 permit tcp host 10.1.1.5 any ?
  ack          Match on the ACK bit
  dscp         Match packets with given dscp value
  eq           Match only packets on a given port number
  established  Match established connections
  fin          Match on the FIN bit
  fragments    Check non-initial fragments
  gt           Match only packets with a greater port number
  log          Log matches against this entry
  log-input    Log matches against this entry, including input interface
```

```
  lt            Match only packets with a lower port number
  neq           Match only packets not on a given port number
  precedence    Match packets with given precedence value
  psh           Match on the PSH bit
  range         Match only packets in the range of port numbers
  rst           Match on the RST bit
  syn           Match on the SYN bit
  time-range    Specify a time-range
  tos           Match packets with given TOS value
  urg           Match on the URG bit
  <cr>
```

Now you can see that you have a multitude of choices, some of which include the same port number options you were given before. Now that the destination IP address information has been specified (with the `any` keyword), you can now fill in the destination port number. Most of the time you will use the `eq` (equals to) port number syntax to designate a single port number. The following code enters the `eq` keyword and continues to use the context-sensitive help to guide you through each additional piece of syntax.

```
Neo(config)#access-list 150 permit tcp host 10.1.1.5 any eq ?
  <0-65535>    Port number
  bgp          Border Gateway Protocol (179)
  chargen      Character generator (19)
  cmd          Remote commands (rcmd, 514)
  daytime      Daytime (13)
  discard      Discard (9)
  domain       Domain Name Service (53)
  echo         Echo (7)
  exec         Exec (rsh, 512)
  finger       Finger (79)
  ftp          File Transfer Protocol (21)
  ftp-data     FTP data connections (20)
<…output omitted for brevety…>
  telnet       Telnet (23)
  time         Time (37)
  uucp         Unix-to-Unix Copy Program (540)
  whois        Nicname (43)
  www          World Wide Web (HTTP, 80)
```

Notice that the context-sensitive help now provides a list of commonly used port numbers. At the top of the list is the option `<0-65536>`, enabling you to enter any port number you choose. In this example, you can enter either the keyword `www` or port number `80` and the result will be the same.

EXAM ALERT

Although you can see the list of commonly used port numbers right now, the list may not be available to you in the CCNA exam. At a minimum, you should commit the following list of ports to memory:

TCP Ports:

- **Port 21: FTP**
- **Port 23: Telnet**
- **Port 25: SMTP**
- **Port 53: DNS**
- **Port 80: HTTP**
- **Port 443: HTTPS**

UDP Ports:

- **Port 53: DNS**
- **Port 69: TFTP**

To complete the access list, the necessary port information is added:

```
Neo(config)#access-list 150 permit tcp host 10.1.1.5 any eq 80
```

As before, for the access list to take effect, it must be applied. The same syntax is used to do this as is used for the standard access list: `ip access-group <in/out>`. Don't forget the best way to find the direction you should apply the access list: Imagine yourself as a router. Is the traffic going away from you (leaving one of your interfaces)? Apply the access list *out*bound. Is the traffic coming into you (received by one of your interfaces)? Apply the access list *in*bound.

Cisco recommends applying extended access lists closer to the source of the network traffic you are permitting or denying. This is completely opposite to what you do with standard access lists. The reason for the complete turnaround is that extended access lists enable you to specify source *and* destination requirements, whereas standard access lists allow you to specify only source requirements. With a standard access list, network traffic may have to cross an entire worldwide network just to find out that it has been denied. With extended access lists, you can designate that traffic is denied from a certain destination before that traffic ever leaves its local subnet.

EXAM ALERT

Standard access lists are always applied closest to the destination. Extended access lists are always applied closest to the source.

Practical Extended Access List Examples

Because of their flexibility, extended access lists are, by far, the most commonly used access lists in production networks. This section takes a look at a few real-world requirements and puts extended access lists into action. Figure 13.3 shows the network diagram used for the extended access list examples.

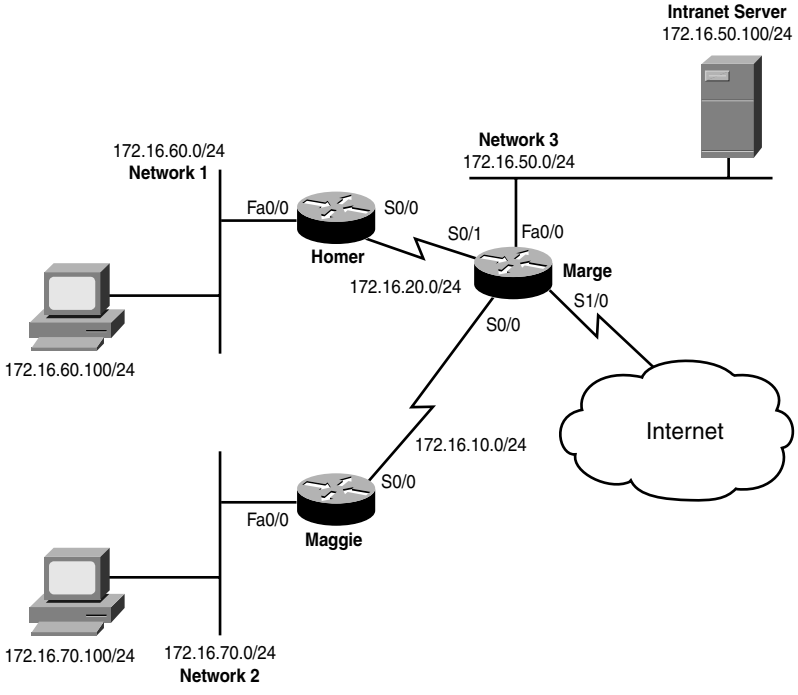


FIGURE 13.3 Extended access lists network diagram.

Blocking a Subnet

This example blocks the Network 2 subnet from reaching the intranet server using the FTP protocol. You must first decide what router to work with. Extended access list best practices recommend denying this traffic as close to the source as possible. This means that you need to access the Maggie router.

```
Maggie(config)#access-list ?
  <1-99>            IP standard access list
  <100-199>         IP extended access list
  <1100-1199>       Extended 48-bit MAC address access list
  <1300-1999>       IP standard access list (expanded range)
  <200-299>         Protocol type-code access list
  <2000-2699>       IP extended access list (expanded range)
  <700-799>         48-bit MAC address access list
  dynamic-extended  Extend the dynamic ACL absolute timer
```

Because these are extended access lists, you must use access list numbers 100–199. This example uses 125.

```
Maggie(config)#access-list 125 ?
  deny     Specify packets to reject
  dynamic  Specify a DYNAMIC list of PERMITs or DENYs
  permit   Specify packets to forward
  remark   Access list entry comment
```

The objective requires you to deny FTP traffic, so you should use the `deny` keyword:

```
Maggie(config)#access-list 125 deny ?
  <0-255>  An IP protocol number
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  igmp     Internet Gateway Message Protocol
  ip       Any Internet Protocol
  ipinip   IP in IP tunneling
  nos      KA9Q NOS compatible IP over IP tunneling
  ospf     OSPF routing protocol
  pcp      Payload Compression Protocol
  pim      Protocol Independent Multicast
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
```

The FTP application protocol runs on top of TCP, so this is the protocol to choose from the list:

```
Maggie(config)#access-list 125 deny tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

The access list now requires source IP address information. Because you are blocking Network 2, you should include the whole 172.16.70.0/24 range:

```
Maggie(config)#access-list 125 deny tcp 172.16.70.0 0.0.0.255 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers
```

Be careful, now. You can enter either the destination IP address information or port number information. Remember, this first prompt enables you to enter *source* port information. You will rarely, if ever, enter any source port restrictions. Of course, the CCNA exam constantly tries to trick you with this often confused fact. This example continues right on to the destination IP address information. The intranet server has the address 172.16.50.100.

```
Maggie(config)#access-list 125 deny tcp 172.16.70.0 0.0.0.255
➥host 172.16.50.100 ?
  ack          Match on the ACK bit
  dscp         Match packets with given dscp value
  eq           Match only packets on a given port number
  established  Match established connections
  fin          Match on the FIN bit
  fragments    Check non-initial fragments
  gt           Match only packets with a greater port number
  log          Log matches against this entry
  log-input    Log matches against this entry, including input interface
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  precedence   Match packets with given precedence value
  psh          Match on the PSH bit
  range        Match only packets in the range of port numbers
  rst          Match on the RST bit
  syn          Match on the SYN bit
  time-range   Specify a time-range
  tos          Match packets with given TOS value
  urg          Match on the URG bit
  <cr>
```

Now you are given the option again to enter the port configurations. At this point, the router is requesting destination port information, which is what you need to use to block FTP. Before you can specify an individual port, you must first designate the `eq` (equal to) syntax:

```
Maggie(config)# access-list 125 deny tcp 172.16.70.0 0.0.0.255
➥host 172.16.50.100 eq ?
  <0-65535>    Port number
  bgp          Border Gateway Protocol (179)
  chargen      Character generator (19)
  cmd          Remote commands (rcmd, 514)
  daytime      Daytime (13)
  discard      Discard (9)
  domain       Domain Name Service (53)
  echo         Echo (7)
  exec         Exec (rsh, 512)
  finger       Finger (79)
  ftp          File Transfer Protocol (21)
  ftp-data     FTP data connections (20)
<…output omitted for brevety…>
```

```
  telnet       Telnet (23)
  time         Time (37)
  uucp         Unix-to-Unix Copy Program (540)
  whois        Nicname (43)
  www          World Wide Web (HTTP, 80)
```

You are again given a laundry list of port numbers that you can enter. You can enter the exact port number or use the commonly used port names in the list.

```
Maggie(config)#access-list 125 deny tcp 172.16.70.0 0.0.0.255
➥host 172.16.50.100 eq 21
```

The first line of the access list is now created, but don't forget that there is still an implicit `deny` at the end of the list. If you were to apply this list now, it would block the subnet from reaching anything. You must add at least one `permit` line; in this case, it is a `permit any` statement.

```
Maggie(config)#access-list 125 permit ?
  <0-255>  An IP protocol number
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  igmp     Internet Gateway Message Protocol
  ip       Any Internet Protocol
  ipinip   IP in IP tunneling
  nos      KA9Q NOS compatible IP over IP tunneling
  ospf     OSPF routing protocol
  pcp      Payload Compression Protocol
  pim      Protocol Independent Multicast
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
```

CAUTION

Remember that with extended access lists, the only protocol that encompasses *all* TCP/IP traffic is the IP protocol. Often, the TCP protocol is mistakenly chosen for the `permit any` statement, which results in only TCP-based applications working.

As mentioned before, the access list must permit all other traffic through. Thus, you must use the `ip` protocol selection followed by a source of `any` and a destination of `any`. This is accomplished in the following line:

```
Maggie(config)#access-list 125 permit ip any any
```

This line allows all TCP/IP traffic from any source to any destination. This is how to create a `permit any` (which overrules the implicit `deny`) in an extended access list.

The access list is now created, but before it can take effect, it must be applied—in this case, as close to the source as possible. Looking back at Figure 13.3, you can see that the FastEthernet 0/0 interface is as close to the source as you can get (directly connected), so that is the best option.

```
Maggie(config)#interface fastethernet 0/0
Maggie(config-if)#ip access-group 125 in
```

Just like that, the first objective is accomplished. All hosts on Network 2 are denied from using FTP to access the intranet server, but permitted to do anything else. Here is the complete configuration, without commentary:

```
Maggie(config)#access-list 125 deny tcp 172.16.70.0 0.0.0.255
➥host 172.16.50.100 eq 21
Maggie(config)#access-list 125 permit ip any any
Maggie(config)#interface fastethernet 0/0
Maggie(config-if)#ip access-group 125 in
```

Restricting by Protocol

Allow the host on Network 1 to use only HTTP and HTTPS to access the intranet server. Do not restrict any other access to or from the Network 1 subnet.

This example allows the host on Network 1 to use HTTP and HTTPS only to access the intranet server. Do not restrict any other access to or from the Network 1 subnet. Now that you have seen a couple access list examples, you can do this with a little less commentary. The router closest to the source this time is the Homer router.

```
Homer(config)#access-list 130 permit tcp host 172.16.60.100
➥host 172.16.50.100 eq 80
Homer(config)#access-list 130 permit tcp host 172.16.60.100
➥host 172.16.50.100 eq 443
```

Now that you have added the lines to permit the HTTP and HTTPS protocols coming from the host on Network 1, you need to deny the host from using any other protocol or port to access the intranet server:

```
Homer(config)#access-list 130 deny ip host 172.16.60.100 host 172.16.50.100
```

Did you remember that you should use the `ip` keyword rather than `tcp`? That's an easy mistake to make. Now you must allow all other traffic to continue unhindered:

```
Homer(config)#access-list 130 permit ip any any
```

Finally, you must apply as close to the source as possible:

```
Homer(config)#interface fastethernet 0/0
Homer(config-if)#ip access-group 130 in
```

Objective, accomplished!

Restricting by Network

Now here's something new! In this example, your network should block all incoming Internet traffic unless an Internet host is fulfilling a request originating from the internal network. This is one of the most common requests for networks requiring Internet access. Executives want the network to be secure, so they want to block all incoming traffic from the Internet. However, if you plan on applying a `deny ip any any`–style access list to the Internet interface, you might as well unplug the cable. This is why Cisco came up with something known as the *TCP-established* access list command. Here's the concept:

When a web browser connects to a web server, it typically does so on TCP port 80. To be reliable, the TCP protocol initiates all its sessions using something known as a *TCP three-way handshake*. This process gets both the sending and receiving hosts on the same page and begins the data transfer. What the TCP-established command access list argument does is watch for this handshake to take place. It then opens return traffic ports to allow the contacted Internet host (and *only* that host) to communicate back to the internal machine requesting data.

To satisfy the objective, you can access the command prompt on the Marge router and enter the following line:

```
Marge(config)#access-list 110 permit tcp any any established
```

This access list is then applied to the interface connected to the Internet in the incoming direction:

```
Marge(config)#interface serial 1/0
Marge(config-if)#ip access-group 110 in
```

CAUTION

Although permitting only the TCP established sessions is very secure, it is not flawless. Cisco therefore created something known a Context Based Access Control (CBAC), implemented in firewall feature-set IOS versions. Although this is not on the exam, it is worth mentioning.

EXAM ALERT

Know how to implement a TCP-established access list and what effect this type of configuration has.

Named Access List

In recent years, Cisco has introduced a much better form of access list. As the name implies, a named access list transcends the typical access list number ranges, enabling you to assign a logical name to the access list. In addition to the logical name, these named access lists also

allow some simple editing. You can remove individual access list lines without deleting and re-creating the entire access list. In very recent IOS versions, the named access lists have been enhanced to allow complete flexibility of inserting and even rearranging access list entries.

Named access lists are also configured from Global Configuration mode, but are prefaced with the `ip` command:

```
Marge(config)#ip access-list ?
  extended    Extended Access List
  log-update  Control access list log updates
  logging     Control access list logging
  resequence  Resequence Access List
  standard    Standard Access List
```

Because you have specified that you would like to create an IP access list (as opposed to IPX or Appletalk), the router would like to know whether you would like to create a standard or extended access list (and don't worry, I talk about that intriguing `resequence` keyword later). It's time to set up a standard access list:

```
Marge(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
```

At first, it doesn't look too different from the numbered access lists created thus far. However, look at that last option: `Access-list name`. You can enter the name of an access list. I'll name this one Jeremy's_List. Watch what happens:

```
Marge(config)#ip access-list standard Jeremy's_List
Marge(config-std-nacl)#
```

Now, instead of adding access list lines directly from Global Configuration mode, you are taken into an access list sub-configuration mode. From here, you can add `permit` and `deny` entries.

```
Marge(config-std-nacl)#?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
```

Notice the addition of the `sequence number` option! By default, the Cisco router inserts lines with sequence number increments of 10. That means that the first line you enter is sequence 10, the next will be 20, and so on. This is fantastic because you can squeeze lines in between

just by choosing a sequence number in the greater than 10 and less than 20. Here is a brief example of this:

```
Marge(config-std-nacl)#10 permit host 10.1.1.1
Marge(config-std-nacl)#20 permit host 10.2.2.2
Marge(config-std-nacl)#15 permit host 10.3.3.3
Marge(config-std-nacl)#^Z
Marge#show access-lists
Standard IP access list Jeremy's_List
    20 permit 10.2.2.2
    15 permit 10.3.3.3
    10 permit 10.1.1.1
```

Lines can be removed by entering `no <sequence number>`. This makes the old form of access list look rudimentary.

```
AdTEC1750(config)#ip access-list standard Jeremy's_List
AdTEC1750(config-std-nacl)#no 15
AdTEC1750(config-std-nacl)#^Z
AdTEC1750#show access-lists
Standard IP access list Jeremy's_List
    20 permit 10.2.2.2
    10 permit 10.1.1.1
```

Now, check out the command you saw in the context-sensitive help earlier:

```
Marge(config)#ip access-list resequence Jeremys_List ?
  <1-2147483647>  Starting Sequence Number
```

This `resequence` command makes it possible to move access list lines around! For example, if I wanted to move sequence number 10 to sequence number 35, I could enter

```
Marge(config)#ip access-list resequence Jeremys_List 10 35
```

NOTE

The sequence number feature was added to all access lists (named or otherwise) in IOS version 12.2(15)T and 12.3(2)T.

Verifying Access Lists

You can use three commands to verify your access list configuration. These commands are `show running-config`, `show ip interface`, and `show access-lists`.

```
show running-config
```

Although this command can be used to verify nearly any configuration on your Cisco router, it is especially useful when you are working with access lists. There is no other command that

can quickly show you where access lists are applied without requiring you to weed through excessive amounts of output. The following output has been trimmed down for brevity.

```
Marge#sh running-config
Building configuration...
Current configuration : 1867 bytes
!
version 12.3
service telnet-zeroidle
service tcp-keepalives-in
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Marge
!
interface Serial 1/0
 ip address dhcp
 ip access-group 170 in
!
access-list 170 permit tcp any any established
show ip interface
```

This command shows you where your access lists are applied, as long as you are patient enough to weed through the excessive amounts of output. The following command views the access lists applied to interface serial 1/0. Pay particular attention to lines 10 and 11.

```
Marge#show ip interface serial 1/0
Serial0/1 is up, line protocol is up
  Internet address is 10.152.19.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  Peer address is 10.152.19.2
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 170
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
```

```
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is enabled, interface in domain outside
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
show ip access-lists
```

Initially, this command might look like a concise version of `show running-config`. However, it has one very handy feature that the other `show` commands lack: the capability to show how many packets have matched a given line in an `access-list`. This capability can be critical in times of troubleshooting and verification.

In the following example, you can see that there is a single access list (30) that has three lines. Next to each line, the number of packets that have matched those entries is displayed.

```
Neo#show ip access-lists
Standard IP access list 30
    permit 10.0.0.0, wildcard bits 0.255.255.255 (94 matches)
    permit 172.16.0.0, wildcard bits 0.0.255.255 (82 matches)
    deny   any (250 matches)
```

Chapter Summary

This chapter has given the theory and configuration of IP standard and extended access lists. A full understanding of these concepts is absolutely critical, not only for your network security, but also for a variety of additional configurations on your router such as NAT, QoS, and dial-on-demand routing (DDR) to name a few.

The two classifications of IP access lists give you all the flexibility you need in applying them to your network. Standard access lists filter based only on the source address. These are useful because they consume less processor and memory resources on your router when you require only simple `allow` and `deny` statements based on source addressing. Common uses of standard access lists include NAT, QoS, and restricting Telnet or Secure Shell (SSH) router access. On the other hand, extended access lists enable you to filter based on the source address, destination address, protocol, and port number. Although they may cost you significant processor resources, extended access lists give you the ultimate in flexibility when choosing the types of traffic to allow or deny in your network. Extended access lists have many uses, but are primarily used for security. The type of access list you create depends on the access list number you select when performing the configuration. For standard access lists, use numbers between 1–99; for extended access lists, use numbers between 100–199.

Access lists can be created without any effect to your router. For an access list to be put in action, it must be applied in some way. To apply an access list to an interface, use the `ip access-group <access_list_number> <in/out>` syntax. To determine the direction the access list should be applied, put yourself in the place of the router. Is the access list filtering traffic coming into you (*in*bound) or going away from you (*out*bound)? If you would like to use an access list to filter Telnet access to your router, the access list should be applied to your VTY ports. Under this line configuration mode, use the `access-class <access_list_number> in` command to apply the access list.

Modern IOS versions include the capability to support sequenced, named access lists. This feature offers the tremendous advantage of being able to assign a logical name to the access list, remove statements from the access list, and resequence entries in your access list.

Key Terms

- standard access list
- extended access list
- named access list
- IP `access-group`
- `access-class`
- inverse mask/wildcard mask
- TCP-established
- IP
- TCP
- UDP

- ICMP
- FTP
- HTTP
- HTTPS/SSL
- Telnet
- TFTP
- DNS

Apply Your Knowledge

Exercises

13.1 Configuring an Access List to Restrict Telnet Access

You are designing a corporate network and would like to implement tight security on all Cisco devices. The first concern is ensuring that only specific hosts can manage the Cisco routers. Figure 13.4 gives the corporate network layout.

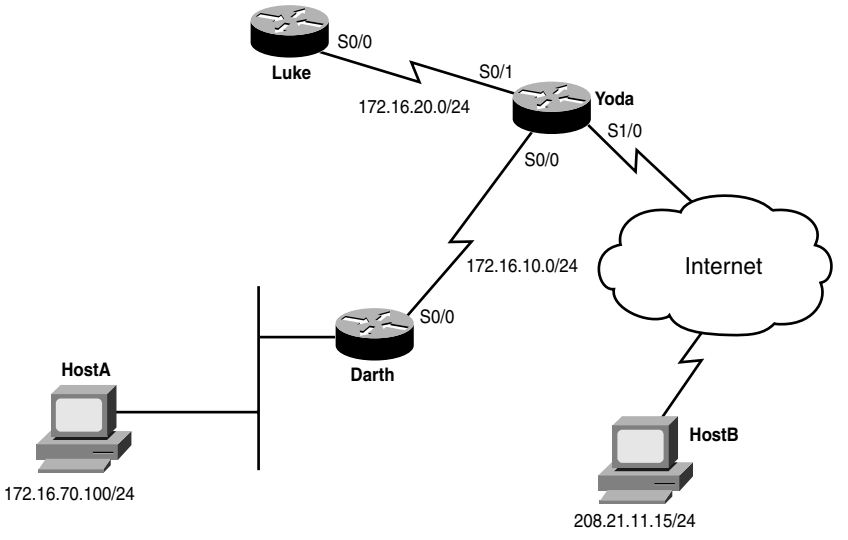


FIGURE 13.4
Corporate network diagram.

You are currently working on the Yoda router. Create and apply an access list that allows only HostA and HostB to manage the Yoda router remotely via Telnet, using the most efficient process.

Estimated Time: 5 minutes

TIP

Be careful when approaching these types of questions on the CCNA exam. You could use an extended access list and apply it to all interfaces of the Yoda router that blocks TCP port 23 (Telnet) from all hosts except HostA and HostB; however, this would not be the most efficient process. Telnet restrictions should be applied to the VTY lines of your device.

To complete this exercise, use the following steps:

1. Log on to the Yoda router and enter Global Configuration mode.

```
Yoda>
Yoda>enable
Yoda#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Yoda(config)#
```

2. Create a standard access list that permits only HostA and HostB. The implicit `deny` at the end of the list blocks all other users.

```
Yoda(config)#access-list ?
  <1-99>            IP standard access list
  <100-199>         IP extended access list
  <1100-1199>       Extended 48-bit MAC address access list
  <1300-1999>       IP standard access list (expanded range)
  <200-299>         Protocol type-code access list
  <2000-2699>       IP extended access list (expanded range)
  <700-799>         48-bit MAC address access list
  dynamic-extended  Extend the dynamic ACL absolute timer

Yoda(config)#access-list 1 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment

Yoda(config)#access-list 1 permit ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address

Yoda(config)#access-list 1 permit host ?
  Hostname or A.B.C.D  Host address

Yoda(config)#access-list 1 permit host 172.16.70.100
Yoda(config)#access-list 1 permit host 208.21.11.15
```

3. Apply the access list to the VTY ports to restrict Telnet access.

```
Yoda(config)#line vty 0 4
Yoda(config-line)#access-class ?
  <1-199>      IP access list
  <1300-2699>  IP expanded access list
  WORD         Access-list name

Yoda(config-line)#access-class 1 ?
  in   Filter incoming connections
  out  Filter outgoing connections

Yoda(config-line)#access-class 1 in
```

13.2 Configuring an Access List to Allow Basic Web Access

You have been contacted to set up a simple Cisco network to provide Internet access to a small, 20-person company. The owners of the company want to ensure that only basic Internet access (HTTP/HTTPS/FTP) is allowed for the internal employees. Refer to Figure 13.5 for a diagram of the network.

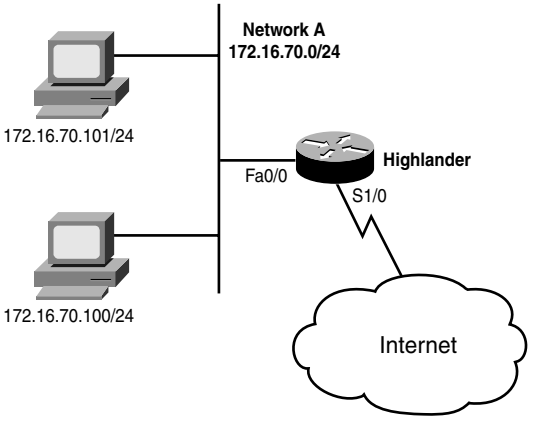


FIGURE 13.5 Small company network diagram.

Estimated Time: 10 minutes

TIP

Most people think that FTP uses only TCP port 21. However, port 21 negotiates only the FTP session. If that is the only port you open, users can log in to FTP servers, but as soon as they try to get a directory list or initiate a file transfer, the connection fails. The FTP Data channel is negotiated on TCP port 20, by default.

To provide the basic web access, perform the following steps:

1. Log in to the Highlander router and enter Global Configuration mode.

```
Highlander>enable
Highlander#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Highlander(config)#
```

2. Create the access list permitting the correct ports. HTTP uses TCP port 80, HTTPS uses TCP port 443, FTP uses port 21 and 20.

```
Highlander(config)#access-list ?
  <1-99>            IP standard access list
  <100-199>         IP extended access list
  <1100-1199>       Extended 48-bit MAC address access list
  <1300-1999>       IP standard access list (expanded range)
  <200-299>         Protocol type-code access list
  <2000-2699>       IP extended access list (expanded range)
  <700-799>         48-bit MAC address access list
  dynamic-extended  Extend the dynamic ACL absolute timer

Highlander(config)#access-list 135 ?
  deny     Specify packets to reject
  dynamic  Specify a DYNAMIC list of PERMITs or DENYs
  permit   Specify packets to forward
  remark   Access list entry comment

Highlander(config)#access-list 135 permit ?
  <0-255>  An IP protocol number
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  igmp     Internet Gateway Message Protocol
  ip       Any Internet Protocol
  ipinip   IP in IP tunneling
  nos      KA9Q NOS compatible IP over IP tunneling
  ospf     OSPF routing protocol
  pcp      Payload Compression Protocol
  pim      Protocol Independent Multicast
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol

Highlander(config)#access-list 135 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

```
Highlander(config)#access-list 135 permit tcp 172.16.70.0 ?
  A.B.C.D  Source wildcard bits

Highlander(config)#access-list 135 permit tcp 172.16.70.0 0.0.0.255 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers

Highlander(config)#access-list 135 permit tcp 172.16.70.0 0.0.0.255 any ?
  ack          Match on the ACK bit
  dscp         Match packets with given dscp value
  eq           Match only packets on a given port number
  established  Match established connections
  fin          Match on the FIN bit
  fragments    Check non-initial fragments
  gt           Match only packets with a greater port number
  log          Log matches against this entry
  log-input    Log matches against this entry, including input interface
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  precedence   Match packets with given precedence value
  psh          Match on the PSH bit
  range        Match only packets in the range of port numbers
  rst          Match on the RST bit
  syn          Match on the SYN bit
  time-range   Specify a time-range
  tos          Match packets with given TOS value
  urg          Match on the URG bit
  <cr>

Highlander(config)#access-list 135 permit tcp 172.16.70.0 0.0.0.255 any eq ?
  <0-65535>    Port number
  bgp          Border Gateway Protocol (179)
  chargen      Character generator (19)
  cmd          Remote commands (rcmd, 514)
  daytime      Daytime (13)
  discard      Discard (9)
  domain       Domain Name Service (53)
  echo         Echo (7)
  exec         Exec (rsh, 512)
  finger       Finger (79)
  ftp          File Transfer Protocol (21)
  ftp-data     FTP data connections (20)
  gopher       Gopher (70)
```

```
  hostname     NIC hostname server (101)
  ident        Ident Protocol (113)
  irc          Internet Relay Chat (194)
  klogin       Kerberos login (543)
  kshell       Kerberos shell (544)
  login        Login (rlogin, 513)
  lpd          Printer service (515)
  nntp         Network News Transport Protocol (119)
  pim-auto-rp  PIM Auto-RP (496)
  pop2         Post Office Protocol v2 (109)
  pop3         Post Office Protocol v3 (110)
  smtp         Simple Mail Transport Protocol (25)
  sunrpc       Sun Remote Procedure Call (111)
  syslog       Syslog (514)
  tacacs       TAC Access Control System (49)
  talk         Talk (517)
  telnet       Telnet (23)
  time         Time (37)
  uucp         Unix-to-Unix Copy Program (540)
  whois        Nicname (43)
  www          World Wide Web (HTTP, 80)

Highlander(config)#access-list 135 permit tcp 172.16.70.0 0.0.0.255 any eq 80
Highlander(config)#access-list 135 permit tcp 172.16.70.0 0.0.0.255 any eq 443
Highlander(config)#access-list 135 permit tcp 172.16.70.0 0.0.0.255 any eq 21
Highlander(config)#access-list 135 permit tcp 172.16.70.0 0.0.0.255 any eq 20
```

3. Apply the access list. In this case, apply the list closest to the destination. Although this is not typical for extended access lists, it is necessary when providing Internet access because the destination must be specified as `any`.

```
Highlander(config)#interface serial 1/0
Highlander(config-if)#ip access-group 135 out
```

Review Questions

1. Your manager at the office asks you to explain the concept behind a standard access list. Using simple terms, explain these concepts.
2. It is critical that an access list is applied correctly when it is used on a router for security purposes. What mantra dictates the rules behind access list application?
3. Explain how a router processes an access list filtering traffic inbound from the Internet.
4. What filtering options does an extended access list give you that are not supplied by a standard access list?
5. One of the criteria an extended access list allows you to use in your filtering options is the source and destination port number. What is the difference between these? Why are two ports necessary for all communication?

Exam Questions

1. Which of the following are valid reasons to implement access lists? (Choose all that apply.)

   - ❍ **A.** QoS
   - ❍ **B.** Route filtering
   - ❍ **C.** Dial-on-demand routing
   - ❍ **D.** Console port security

2. Which type of access list can filter traffic based on the source port? (Choose all that apply.)

   - ❍ **A.** Standard
   - ❍ **B.** Extended
   - ❍ **C.** User-Based
   - ❍ **D.** Static
   - ❍ **E.** Named
   - ❍ **F.** Unnamed

3. You are filtering traffic to an FTP site and you want only FTP traffic to reach the server. You do not want additional traffic to reach the server. Which traffic should be allowed?

   - ❍ **A.** TCP on ports 20 and 21
   - ❍ **B.** UDP on ports 20 and 21
   - ❍ **C.** TCP on port 21
   - ❍ **D.** TCP and UDP on ports 20 and 21

4. What happens to a packet that does not meet the conditions of any access list filters?

   - ❍ **A.** The packet is routed normally.
   - ❍ **B.** The packet is flagged and then routed.
   - ❍ **C.** The packet is dropped.
   - ❍ **D.** The administrator is notified.

5. You have an IP address and wildcard mask of 10.0.20.5 255.255.0.0. Which of the following IP addresses will be affected by this access list? (Choose all that apply.)

- ❍ **A.** 10.0.0.10
- ❍ **B.** 192.168.20.5
- ❍ **C.** 172.30.20.5
- ❍ **D.** 10.2.1.1

6. You want to create an access list to filter all traffic from the 172.16.16.0 255.255.240.0 network. What wildcard mask is appropriate?

- ❍ **A.** 0.0.7.255
- ❍ **B.** 0.0.15.255
- ❍ **C.** 0.0.31.255
- ❍ **D.** 0.0.63.255

7. Regarding access lists, which of the following statements is correct?

- ❍ **A.** Only one access list per protocol, per direction, per interface
- ❍ **B.** Only one access list per port number, per protocol, per interface
- ❍ **C.** Only one access list per port number, per direction, per interface
- ❍ **D.** Only one access list per port number, per protocol, per direction

8. You need to temporarily remove access list 101 from one of your interfaces—which command is appropriate?

- ❍ **A.** `no access-list 101`
- ❍ **B.** `no ip access-group 101`
- ❍ **C.** `access-list 101 disable`
- ❍ **D.** `access-group 101 disable`

9. Which of the following creates a standard access list that allows traffic from the 172.16 subnet?

- ❍ **A.** `access-list 1 permit 172.16.0.0 0.0.255.255`
- ❍ **B.** `access-list 100 permit 172.16.0.0 255.255.0.0`
- ❍ **C.** `access-list 1 permit 172.16.0.0 255.255.0.0`
- ❍ **D.** `access-list 100 permit 172.16.0.0 0.0.255.255`

10. You want to create an access list that denies all outbound traffic to port 80 from the 10.10.0.0 network. Which access list entry meets your requirements?

    - **A.** `access-list 101 deny tcp 10.10.0.0 0.0.255.255 eq 80`
    - **B.** `access-list 91 deny tcp 10.10.0.0 0.0.255.255 any eq 80`
    - **C.** `access-list 101 deny tcp 10.10.0.0 0.0.255.255 all eq 80`
    - **D.** `access-list 101 deny tcp 10.10.0.0 0.0.255.255 any eq 80`

Answers to Review Questions

1. A standard access list is nothing more than a generic list of `permit` and `deny` statements. It chooses what devices are allowed through a router based on who they are (their source IP addresses).
2. One access list, per protocol, per interface, per direction.
3. Regardless of how an access list is applied, the router processes it the same: Statements are read from the top of the list down. If a packet matches one of the statements, the router executes the direction of the statement (permit or deny) and exits the access list processing. If the packet does not match any of the statements in the access list, it is implicitly denied.
4. An extended access list gives you the option of filtering based on the TCP/IP sub-protocol (such as TCP, UDP, or ICMP), the destination address, and the source/destination port number. Beyond the CCNA level, an extended access list also enables you to filter based on criteria such as time of day or QoS marking.
5. When communicating on a TCP/IP-based network, the destination port helps identify what server application your client is attempting to access. For example, sending data to TCP port 80 indicates the HTTP server service. The source port number is used to identify the client application to which the server should respond. These two ports are always necessary in any communication to identify the applications on both ends of the connection.

Answers to Exam Questions

1. **A, B, C**. Access lists can be used with QoS in implementing many forms of queuing and congestion avoidance techniques. Access lists can filter routing protocol updates. Access lists can also specify interesting traffic to trigger dial-on-demand routing. Answer D is incorrect because access lists aren't used for console port security.
2. **B, E**. Extended access lists can use source and destination information, including the source port, and named access lists can be either extended or standard, so they have the capability to filter based on the source port. Answer A is incorrect because standard access lists can filter on source address information, but not source port. Answer C is incorrect because there are no user-based access lists. Answer D is incorrect because there are no static access lists. Answer F is incorrect because there are no unnamed access lists.

3. **A**. FTP uses TCP and ports 20 and 21. Answer B is incorrect because FTP uses TCP. Answer C is incorrect because port 20 is required as well. Answer D is incorrect because UDP is not necessary.

4. **C**. A packet that does not meet any filters is dropped. Answer A is incorrect because the packet is discarded rather than routed. Answer B is incorrect because there is no mechanism to flag the packet. Answer D is incorrect because although it is conceivable that an administrator could be notified by default, the packet is simply dropped.

5. **B, C.** The significant bits are the last 16, indicated by the wildcard mask of 255.255.0.0. 192.168.20.5 and 172.30.20.5 match the last two octets, or 16 bits, of the 10.0.20.5 IP address. Answers A and D are incorrect because although the first portions of the IP address match, it is the last two octets that are significant.

6. **B**. 0.0.15.255 affects the 172.16.16.0 255.255.240.0 network. In the third octet, the first four bits are checked in binary, resulting in 00000000.00000000.00001111.11111111. Answer A is incorrect because this does not match the given problem, checking too many bits (five) in the last octet. Answer C is incorrect because this mask checks only three bits in the third octet. Answer D is incorrect because this mask checks only two bits in the third octet.

7. **A**. You may create only one access list per protocol, per direction, per interface. Answer B is incorrect because you can have multiple access lists for a single port number, and only one per direction. Answer C is incorrect because you may have only one access list per protocol, not per port number. Answer D is incorrect because you may not have more than one access list per interface.

8. **B.** The correct syntax is `no ip access-group 101`. This removes the access list from the interface. Answer A is incorrect because this line deletes the access list entirely. Answers C and D use invalid syntax.

9. **A**. This answer has the correct syntax of the `access-list` command followed by the list number, `permit`/`deny`, IP address, and a wildcard mask. Answers B and D are incorrect because they indicate an extended access list. Answer C is incorrect because the wildcard mask has been reversed.

10. **D**. Use the `any` keyword to specify all destinations. Answer A is incorrect because no destination is specified. Answer B is incorrect; this specifies a standard access list. Answer C is incorrect because `all` is not the proper keyword.

Suggested Reading and Resources

1. Cisco Online Documentation: Filtering IP Packets Using Access Lists, http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm#wp1109098.

2. Ward, Chris and Cioara, Jeremy. *Exam Cram 2 CCNA Practice Questions*. Que Publishing, 2004.

3. Odom, Wendell. *CCNA Certification Library*. Cisco Press, 2003.

CHAPTER 14

Network Address Translation

Objectives

Describe Network Address Translation

Understand the operational terminology of Network Address Translation

Configure Network Address Translation to address a variety of network requirements

Verify Network Address Translation operation

- If you add Network Address Translation configurations to your network, you can place an additional security barrier between your internal clients and the Internet. In addition, this technology also enables you to share a single Internet IP address between many internal clients, which minimizes connection costs.
- Network Address Translation uses confusing terms to describe the location of an IP address on the network. Understanding these terms is key to configuring and troubleshooting Network Address Translation.
- There are many options for configuring Network Address Translation. Although the most popular configuration focuses around sharing a single Internet IP address for internal clients, many others can address common network needs.
- After you have configured Network Address Translation, you need to view a snapshot of your IP address mappings to ensure unauthorized access is prevented and verify the configuration has been applied successfully.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- Focus on the Network Address Translation terminology. Understanding these terms is paramount to understanding the NAT configuration as a whole.
- When studying, focus on the Static NAT configurations first because these are the simplest. After you master this configuration, move on to NAT Overload, followed by Dynamic NAT.

Introduction

I can still remember the very first time I saw Network Address Translation (NAT) in action. "This is the most amazing thing I have ever seen," I said, with the same awestruck feeling as the first time you walk up and look over the Grand Canyon in Arizona. Okay, perhaps it wasn't that fantastic, but at the same time, NAT is definitely at the top of my list of configurations I love to set up.

Despite it being one of the most widely implemented concepts in the world of network technology, NAT is the newest topic added to the CCNA exam. This is most likely because of its configuration complexity: It requires a thorough understanding of standard access lists to successfully deploy. However, Cisco is very wise in adding it to the entry-level exam because nearly every network in the world uses NAT in some shape or form. Even home networks using Linksys, D-Link, and Netgear routers use NAT.

NAT was originally developed through a combination of Cisco engineers and the Internet Engineering Task Force (IETF) group in 1994 to overcome the quickly approaching IP address shortage. With the Internet popularity growing at a rate far faster than expected, the remaining public IP addresses would soon be depleted. At that time, TCP/IP version 6 (IPv6, which would have solved the IP address shortage) had been created in a draft status, but would require a worldwide upgrade of network devices and operating system software to successfully deploy. Rather than upgrading all network-capable devices, the focus was placed on creating a gateway device that could enable multiple network devices to share a single IP address.

As this concept materialized, NAT was born. Theoretically, a router running NAT is capable of allowing more than 60,000 devices to share a single Internet-valid IP address. Practically speaking, the router resources (processor and memory) and WAN bandwidth are depleted long before that limit is reached. With thousands of devices capable of using a single, public IP address, the life of TCP/IP version 4 (IPv4) has been extended years beyond what was thought possible.

NAT also acts as a natural security boundary by eliminating end-to-end traceability. If your router only has a single IP address that is connected to the Internet, the public IP address, which is assigned to the outside interface, does not belong to any one internal host. For example, imagine that your router's public IP address is 209.1.5.9, and all your internal hosts come from the subnet 192.168.1.0/24. Whenever one of the internal hosts accesses the Internet, it is seen as 209.1.5.9. However, if anyone from the Internet attempts to access 209.1.5.9, the address maps to no individual host, which makes the internal network invisible to the Internet.

NAT Concepts

Although the introductory discussion of NAT hits the most popular uses of the technology, NAT can be used for much more. Before you go deeper into the specific uses, though, you must first understand the foundation concepts.

In its core function, Network Address Translation does just that: translate addresses. It can take any IP address and make it look like another. This is why the creative geniuses behind TCP/IP defined three ranges of "private IP addresses" in RFC 1918. The following is a list of the three private address ranges:

- **Class A**—10.0.0.0–10.255.255.255
- **Class B**—172.16.0.0–172.31.255.255
- **Class C**—192.168.0.0–192.168.255.255

TIP

You need to know the private IP address ranges.

You might notice that a private address range is defined for each class of address. This gives a company more flexibility to use different ranges based on the company size. As a general statement, most small companies use the 192.168.X.X range, most medium companies use the 172.16.X.X–172.31.X.X ranges, and most large companies use the 10.X.X.X ranges. Remember, this is just a general statement, not a solid rule.

It is commonly stated that these private addresses are non-routable, which is not true at all. Thousands of companies around the world use these addresses and route them throughout their private networks just fine. This misunderstanding came about because all Internet Service Providers (ISPs) use access lists to block these addresses from entering or leaving their networks. It is accurate to say that these private addresses are not *Internet* routable because, if they were, there would be thousands of duplicate IP address conflicts every single day.

As shown in Figure 14.1, networks connected to the Internet typically use these private IP addresses internally and then translate them when attempting to access the Internet. This enables you to have many duplicate addresses around the world without any conflicts because they never communicate directly. This can cause problems with overlapping IP addresses when companies merge, but NAT can even be engineered to solve these problems.

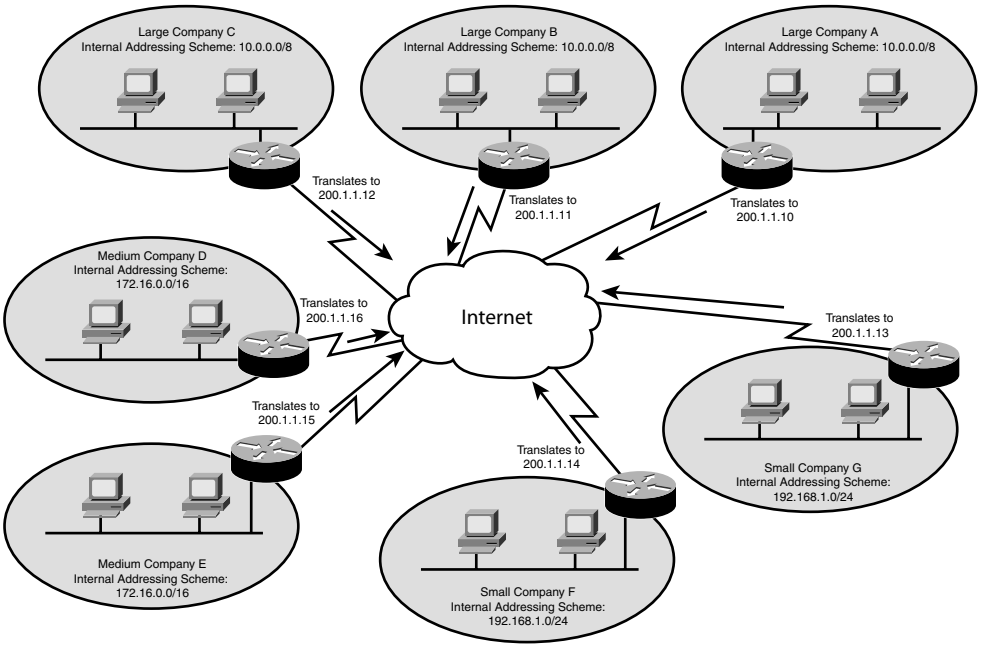


FIGURE 14.1 Network that uses a NAT configuration with private addressing.

With this foundation in place, you're ready to examine the styles of NAT.

Static NAT

Static NAT is the simplest form of NAT. It enables you to map one IP address to another in a one-to-one relationship. This is typically used to allow access to internal servers from the Internet that are using a private address space. In Figure 14.2, there are three servers located on the internal network: a web server, an FTP server, and an email server. These three servers are assigned to a private IP address space (192.168.1.0/24) and would typically be inaccessible from the Internet. By using Static NAT, you can map the private IP addresses to a public IP on a one-to-one basis, enabling these servers to be accessed from the Internet using the three public IP addresses shown in Figure 14.2.

This Static NAT mapping goes both ways. When someone from the Internet accesses 200.1.1.1, it is translated to the internal address 192.168.1.1. Likewise, when the server 192.168.1.1 accesses the Internet, it is seen as 200.1.1.1. Although this form of NAT does not allow multiple internal hosts to share a single address, it does implement the security features of NAT by eliminating end-to-end traceability and enables servers that are sharing your private network to be accessed from the Internet.

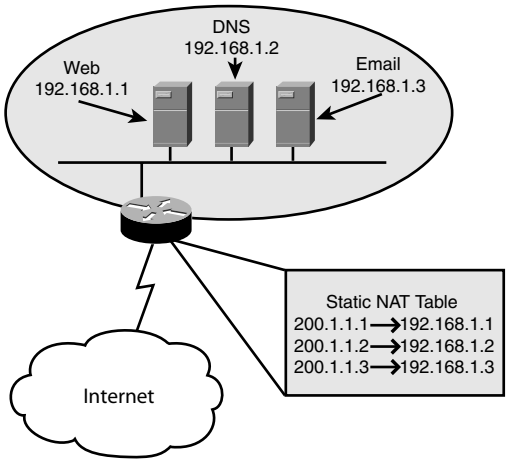


FIGURE 14.2 Static NAT address mappings.

Static NAT can also be configured to statically translate individual TCP or UDP ports. This awesome feature enables you to take a single IP address and translate one or many ports to either the same host or many different hosts. For example, you might have a router that has the external IP address 195.1.1.1. You can statically configure NAT so that when your router receives a request on 195.1.1.1, using TCP port 80 (HTTP), it redirects it to the internal address 192.168.1.50 on TCP port 80. However, when it receives a request on 195.1.1.1, using TCP port 21 (FTP), it redirects it to the internal address 192.168.1.100 on TCP port 21. In this way, NAT can act as a type of firewall (allowing only some ports through to specific hosts) and give you the flexibility of offering many services through the same IP address. Using Static NAT with ports even makes it possible to redirect port numbers. For example, you might be using one of those scandalous DSL or cable Internet providers that block certain port numbers to keep you from running a web server from home. You can configure Static NAT in such a way that when your router receives a request on TCP port 800 it redirects it to an internal IP address on TCP port 80.

Dynamic NAT

Static NAT is superb if you have a few hosts that need to be translated; however, if many hosts need to be translated, creating static entries for each one can be quite tedious. This is where dynamic NAT can help. Dynamic NAT enables you to define a pool of addresses to be translated along with a pool of addresses to which they are to be translated. The router then dynamically maps these IP addresses as the need arises. This is *not* the same thing as allowing multiple hosts to share the same IP address (known as *NAT overloading*). Dynamic NAT makes many one-to-one mappings without requiring you to configure them statically.

NAT Overload and Port Address Translation

Now we come to the form of NAT that made it famous. NAT Overload, also known as Port Address Translation (PAT), enables a single IP address to support many internal clients. Whenever a host establishes communication with a server outside the NAT firewall, it tries to access a specific port number (known as the *destination port*). However, it also uses a source port number to allow for return traffic (this is discussed more thoroughly in Chapter 13, "Access Lists"). Figure 14.3 shows how NAT Overload also incorporates this source port number into the translation.

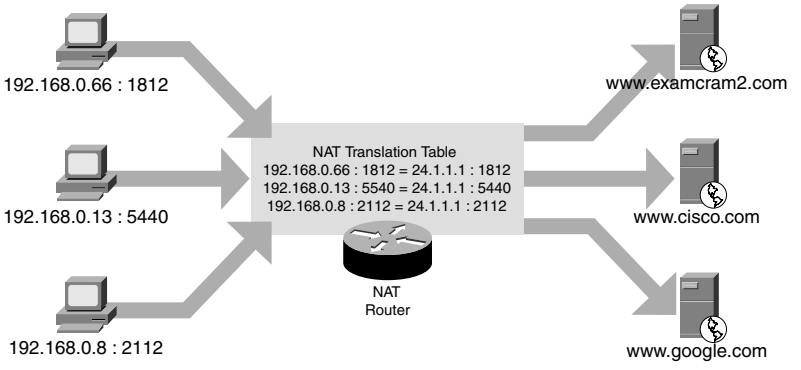


FIGURE 14.3 NAT Overload uses port numbers to make translations unique.

The hosts communicating randomly generate the source ports. The NAT router then appends these to the public IP address to make the source *socket* (or IP address and port number combination) unique. When the Internet server replies to whatever request was made, it does so to the source IP and socket. When the NAT router receives the reply it is then able to redirect it to the correct internal host by referring to its NAT translation table. Because hosts use random source ports, there is very little possibility that two hosts will choose the same source port number (one chance out of some 60,000); however, if two hosts do happen to choose the same port number, the NAT device causes one of the device sessions to reset and choose a different port number. By using unique port numbers, the router can originate thousands of requests from its single Internet IP address. This provides Internet access to the internal network clients while using just one Internet address.

NAT Terminology

Believe it or not, setting up NAT is not very difficult; it's learning the terminology used with NAT that can cause your brain to fry. The first time you see these terms, it may make no sense to you at all, and that's just fine. It takes some time to soak in. Now, keep in mind that these are not "Cisco terms," rather, they are an industry standard way of referring to the four different points in a NAT-based network. Before trying to understand four NAT address descriptions, you must understand the building blocks used to construct these terms:

- **Inside/Outside**—These NAT descriptors refer to where a device is physically located. If a device is "inside," it is under your control; it is in your network. If a device is "outside," it is not under your control; it is outside your network.
- **Local/Global**—These NAT descriptors refer to where an IP address is located *from the perspective of a NAT device*. The NAT device is a network device that has its address translated through a NAT router. It could be a PC, a server, an XBox, or any other type of host that has a private address that is translated to a real address on the Internet. If the IP address is considered "local," it is seen as a device on the local subnet from the perspective of a NAT device (this may or may not be true). If the IP address is considered "global," it is seen as not on the local subnet from the perspective of a NAT device.

If that doesn't sound confusing, just wait until we start combining those terms together for the four NAT address descriptions. Figure 14.4 shows a visual location of these address on the network.

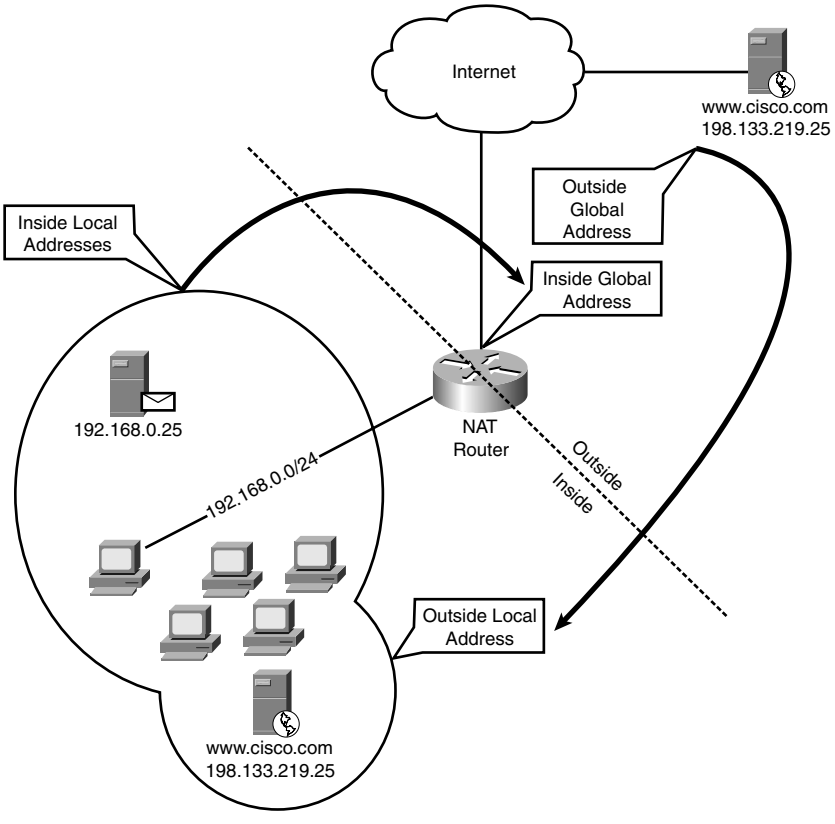


FIGURE 14.4 NAT terminology.

- **Inside Local Addresses**—These addresses are the easiest to understand because they refer to everything inside your network. Remember the word *constructs* discussed just a moment ago: An address "inside" is physically located inside your network. From the perspective of the NAT device, it is "local," meaning it is seen on the internal network. If an inside local address were to communicate with another inside local address, that communication would be described as standard LAN connectivity. No routers would be needed.
- **Inside Global Addresses**—Now the terms begin to mix a little bit. Let's break this down into the individual pieces: First off, the address is "inside," which means that it is physically located on your network; it is under your control. "Global" means that it is seen as an IP address not on the local subnet from the perspective of one of your NAT devices. Put all this together and you are left with the Internet valid IP address assigned to your router that is directly connected to the Internet. This is where a fundamental understanding of inside and outside can really help; if the address were an "outside global," it would not be under your control, meaning that it could be any of the millions of devices attached to the Internet.
- **Outside Global Addresses**—Outside global addresses refer to devices that are physically "outside" your network—outside your control. These addresses are "global," meaning that the NAT devices on the inside of your network see these as non-local addresses. Put these two pieces together and you have a description of a standard, Internet IP address.
- **Outside Local Addresses**—I saved the best for last. Outside local addresses confused me for quite some time until I fully understood the capabilities of NAT. First let's look at the pieces: This address is physically "outside" your network, out of your control, out on the Internet. However, it appears to NAT devices as an IP address on the "local" subnet. What this describes is an Internet host translated as it comes through the NAT router *into* your local network. You can think of this as "reverse NAT," or just NAT in the other direction. As shown in Figure 14.4, when the cisco.com web server speaks to the internal hosts on the 192.168.0.0/24 network, they believe it to be co-located on the local subnet with them. They come to this conclusion because the NAT router translates the outside global address to something local (perhaps 192.168.0.1, the NAT gateway's address).

TIP

Understanding the four NAT address descriptors listed is not only useful for the CCNA exam, but also for understanding any real-world NAT documentation.

NAT Configurations

Configuring NAT is not all that bad as long as you focus in on your objective. I mention this because the syntax can be quite daunting when you see all the options available to you. Advanced NAT configurations can get quite complex.

TIP

For the CCNA exam, you should be able to perform these three NAT-related tasks:

- Configure Static NAT, translating an inside global address (or port number) to an internal host, such as a web, DNS, or email server.
- Configure Dynamic NAT, translating a pool of inside local addresses to a pool of outside global addresses.
- Configure NAT Overload, translating many inside local addresses to a single inside global address.

Of these three, I would especially focus on the first and third configurations because they are more common in the real world.

With that said, it's time to walk through these configurations one at a time.

Static NAT

As discussed earlier, Static NAT performs a one-to-one mapping from an inside local address to an inside global address (in English: from a private to a public address). This could mean that all traffic is translated between these addresses, or it could mean that you just choose certain ports through which to translate. As I go through the syntax, I expand a little more on this. Figure 14.5 adds a network diagram to this syntax.

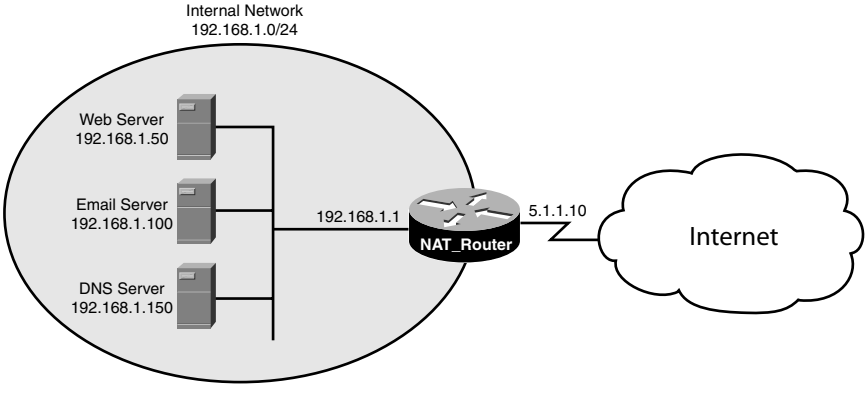


FIGURE 14.5 Static NAT configuration.

Before you get into the syntax, I want to make sure you've got the terms down. The internal network consists of the 192.168.1.0/24 addresses. In NAT terms, these are all inside local addresses. The router has a single Internet IP address of 5.1.1.10. This is considered the inside global address. The rest of the hosts on the Internet that will be accessing your internal servers all have outside global addresses.

- **Scenario 1**: Configure a Static NAT translation so that if any request on any port is received on the inside global address of the NAT_Router, it forwards that request to the Internal Web server.

Here we go! First, get familiar with the current interfaces:

```
NAT_Router#show ip interface brief
Interface                  IP-Address      OK? Method Status      Protocol
FastEthernet0              192.168.1.1     YES manual up          up
Serial0                    5.1.1.10        YES manual up          up
```

Everything is as shown in the Figure 14.5. The first step in configuring NAT is to identify your inside and outside interfaces to the router. This is done on a per-interface basis:

```
NAT_Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
NAT_Router(config)#interface fastethernet0
NAT_Router(config-if)#ip nat inside  !identifies internal interface
NAT_Router(config-if)#exit
NAT_Router(config)#interface serial0
NAT_Router(config-if)#ip nat outside !identifies external interface
NAT_Router(config-if)#exit
NAT_Router(config)#
```

With these interfaces identified to the router, it now knows which interface(s) are considered outside and inside. Setting up the Static NAT translation is a little more difficult.

Static NAT configurations are set up in global configuration mode with the `ip nat` syntax:

```
NAT_Router(config)#ip nat ?
  inside       Inside address translation
  log          NAT Logging
  outside      Outside address translation
  pool         Define pool of addresses
  service      Special translation for application using non-standard port
  translation  NAT translation entry configuration
```

The primary keywords to consider are the `inside` and `outside` keywords. These two commands perform exactly the same function from different perspectives. If you choose the `inside` keyword, the syntax that follows will translate an inside address to an outside address. If you choose the `outside` keyword, the syntax that follows translates an outside address to an

inside address. Because NAT translations are always two-way, the keyword you choose influences the order you use for the addresses in the upcoming syntax. To save confusion, I would recommend picking one method (`inside` or `outside`) and using it indefinitely. Many moons ago, I chose to use `inside`, so that's what I'll do here:

```
NAT_Router(config)#ip nat inside ?
  destination  Destination address translation
  source       Source address translation
```

The choice now is whether to translate the inside `source` IP address or inside `destination` IP address. Well, if you are looking from the perspective of the *inside* device (what was chosen when the `inside` keyword was used rather than `outside`), you need to translate the internal device's source IP address rather than its various destination IP addresses (you see now how this can get confusing if you alternate between `inside` and `outside` keywords?).

```
NAT_Router(config)#ip nat inside source ?
  list       Specify access list describing local addresses
  route-map  Specify route-map
  static     Specify static local->global mapping
```

At this point, the router wants to know what type of translation you would like to perform. The `list` keyword is used to perform dynamic NAT translations. Using `route-maps` for NAT is far beyond the scope of the CCNA (and perhaps even the CCNP). In this case, you need to define a static translation.

```
NAT_Router(config)#ip nat inside source static ?
  A.B.C.D  Inside local IP address
  esp      IPSec-ESP (Tunnel mode) support
  network  Subnet translation
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
```

The router would now like to have either the inside local address or the protocol information. This scenario requests a full translation from the router's inside global address to the web server's inside local address. If you were choosing to use NAT to translate individual ports, you would use either TCP or UDP protocols. For this scenario, you can enter the web server's inside local address.

```
NAT_Router(config)#ip nat inside source static 192.168.1.50 ?
  A.B.C.D  Inside global IP address
```

The router now needs to know what inside global address to use. In this example, the router's inside global address is 5.1.1.10, which is the same IP address assigned to its `Serial0` interface. In the real world, you have the option of purchasing blocks of IP addresses from your ISP. You can then translate each one of these public addresses to an inside local address *without the address even being assigned to an interface*! All you need to do is create Static NAT mappings for

each one of the addresses that you have been assigned by the ISP, and your router automatically responds to them on the interface(s) you have designated as `ip nat outside` interfaces. In this example, there is only a single IP address, so that's plugged in here:

```
NAT_Router(config)#ip nat inside source static 192.168.1.50 5.1.1.10 ?
  extendable  Extend this translation when used
  no-alias    Do not create an alias for the global address
  <cr>
```

The `extendable` keyword enables you to have multiple inside global addresses mapped to the same inside local address (all the mappings must be marked with the `extendable` keyword). The `no-alias` command enables you to set up a one-way NAT mapping from the inside to outside. (The outside interface does not pass requests through to the inside host, but the inside host is translated to the outside.) In this case, you're not adding either of these special functions, so you can just press the Enter key. Awesome!

You can verify this configuration by using either the `show running-config` command or the much more concise `show ip nat translations`:

```
NAT_Router#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 5.1.1.10           192.168.1.50       ---                ---
```

Because this is a manually defined static entry, only the inside global and inside local fields are populated. If a host tried to connect to this entry (to access the internal web server), you would see the outside local and outside global columns populate as well. Let me generate some traffic from the outside to show you what this will look like:

```
NAT_Router#show ip nat translations
Pro Inside global  Inside local       Outside local         Outside global
--- 5.1.1.10       192.168.1.50       ---                   ---
tcp 5.1.1.10:80    192.168.1.50:80    52.1.9.3:3367         52.1.9.3:3367
```

In this case, I had an outside host access the 5.1.1.10 address with a web browser (TCP port 80). You can see that it kept the original static entry and added a line below it, showing the outside local and outside global addresses of the external client. In this case, they are the same because the outside host appears as an outside host to the web server (the outside local address). The port 3367 is the dynamically generated source port number of the outside host, port 80 is the destination port number sent to the web server. Scenario #1, accomplished!

- **Scenario 2**: Configure two additional Static NAT translations. If the NAT_Router receives a request to its inside global address that uses SMTP it should be sent to the internal email server. If it receives a DNS request on the inside global address, it should forward it to the internal DNS server. All other traffic should still remain forwarding to the internal web server.

Wow! What a scenario! To tackle this, you must remember the universal rule of routing: The more specific matches *always win*. So, if you were to add specific Static NAT entries that forward just a single port number, it would always overrule the `forward all` entry configured for the web server in Scenario #1. Let's walk through these using context-sensitive help one more time, with a little less commentary.

```
NAT_Router(config)#ip nat ?
  inside       Inside address translation
  log          NAT Logging
  outside      Outside address translation
  pool         Define pool of addresses
  service      Special translation for application using non-standard port
  translation  NAT translation entry configuration

NAT_Router(config)#ip nat inside ?
  destination  Destination address translation
  source       Source address translation

NAT_Router(config)#ip nat inside source ?
  list       Specify access list describing local addresses
  route-map  Specify route-map
  static     Specify static local->global mapping

NAT_Router(config)#ip nat inside source static ?
  A.B.C.D  Inside local IP address
  esp      IPSec-ESP (Tunnel mode) support
  network  Subnet translation
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
```

So far, the Static NAT mapping has been configured in exactly the same fashion as the previous one. Now we'll add a little twist: Because we are just forwarding specific ports to the internal server, we'll need to choose the protocol those ports are using. The scenario called for us to forward SMTP traffic to the internal E-Mail server and DNS traffic to the internal DNS server. SMTP uses TCP port 25 and DNS traffic uses UDP port 53 (remember this from the access-list chapter?), so here's how the syntax will continue. First, we'll focus on creating the map for the E-Mail server:

```
NAT_Router(config)#ip nat inside source static tcp ?
  A.B.C.D  Inside local IP address

NAT_Router(config)#ip nat inside source static tcp 192.168.1.100 ?
  <1-65535>  Local UDP/TCP port

NAT_Router(config)#ip nat inside source static tcp 192.168.1.100 25 ?
  A.B.C.D    Inside global IP address
  interface  Specify interface for global address
```

All righty then. A specific Static NAT mapping has been configured that uses the TCP protocol and pointed to the inside local address of 192.168.1.100 with the *inside local port* 25. Isn't that interesting? Now it's time to specify an inside local port as well! This opens up a bunch of possibilities. But before I expand on those, let's finish the command:

```
NAT_Router(config)#ip nat inside source static tcp 192.168.1.100 25
➥5.1.1.10 ?
  <1-65535>  Global UDP/TCP port

NAT_Router(config)#ip nat inside source static tcp 192.168.1.100 25
➥5.1.1.10 25 ?
  extendable  Extend this translation when used
  no-alias    Do not create an alias for the global address
  <cr>
NAT_Router(config)#ip nat inside source static tcp 192.168.1.100 25
➥5.1.1.10 25
NAT_Router(config)#^Z
NAT_Router#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 5.1.1.10           192.168.1.50       ---                ---
tcp 5.1.1.10:25        192.168.1.100:25   ---                ---
```

Did you see that? Not only was the command finished and the Static NAT mapping added to the table, but now you can see the possibility for the *global TCP/UDP port*! This enables you to perform the fantastic configuration of *port redirection*. Here's the idea: Perhaps for security reasons, you didn't want to have the internal email server answering SMTP requests on port 25, so the internal port on the server is changed to 5525. Now, none of the internal clients can access that email server via port 25; however, the NAT router can redirect incoming Internet requests on port 25 to the inside local port 5525! All this is seamless to the Internet clients. Are you as excited about this as I am?

Finally, let's add the last NAT translation for the DNS server:

```
NAT_Router(config)#ip nat inside source static udp ?
  A.B.C.D  Inside local IP address

NAT_Router(config)#ip nat inside source static udp 192.168.1.150 ?
  <1-65535>  Local UDP/TCP port

NAT_Router(config)#ip nat inside source static udp 192.168.1.150 53 ?
  A.B.C.D    Inside global IP address
  interface  Specify interface for global address

NAT_Router(config)#ip nat inside source static udp 192.168.1.150 53
➥5.1.1.10 ?
  <1-65535>  Global UDP/TCP port
```

```
NAT_Router(config)#ip nat inside source static udp 192.168.1.150 53
➥5.1.1.10 53
NAT_Router(config)#^Z
NAT_Router#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 5.1.1.10           192.168.1.50       ---                ---
tcp 5.1.1.10:25        192.168.1.100:25   ---                ---
udp 5.1.1.10:53        192.168.1.150:53   ---                ---
```

Perfect! Three Static NAT entries have now been added. Before moving on, let me call your attention to the context-sensitive help after the local port information has been entered. Take a look:

```
NAT_Router(config)#ip nat inside source static udp 192.168.1.150 53 ?
  A.B.C.D    Inside global IP address
  interface  Specify interface for global address
```

So far, you have been entering the inside global address that you would like to translate. However, there may be an occasion that you do not know what your global address may be (primarily when using DHCP for your Internet address). In this case, you can use the `interface` keyword rather than an inside global address to translate requests received on the outside interface to internal hosts. This can be especially useful when using a Cisco router to perform NAT on a cable or DSL connection at a home.

```
NAT_Router(config)#ip nat inside source static udp 192.168.1.150 53interface serial 0
➥53
```

Dynamic Pool Translations

The next step is to move from the manual, Static NAT entries to allowing the router to do the work for you. Dynamic NAT enables you to define a pool of addresses to translate *from* and a pool of addresses to translate *to*. The primary application of Dynamic translations is to temporarily overcome overlapping IP addresses. For example, a company might use subnets of the 10.0.0.0/8 address range for their internal addressing. This company might merge with another company that uses the same internal address space (this happens all the time). The IT staff could implement an intermediary design that used NAT to translate between the two networks. When performing this type of translation, hosts must refer to each other by hostname rather than IP address, thus requiring a DNS server be in place. When the NAT router sees a reply from a remote DNS server, it changes the remote IP address to something other than an overlapping IP address.

Although the CCNA-level NAT does not get deep into design for overlapping IP addresses, you need to know the basic configurations of Dynamic NAT. These configurations also act as springboards into the NAT Overload configuration. First, examine Figure 14.6 for a look at a Dynamic NAT network diagram.

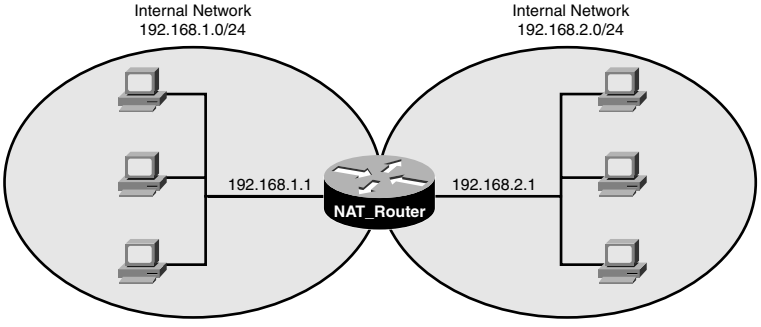


FIGURE 14.6 Dynamic NAT translations.

- **Scenario 3**: Configure the NAT_Router so that hosts from the 192.168.1.0/24 network are seen as IP addresses 192.168.2.200–225 when accessing the hosts in the 192.168.2.0/24 network. Likewise, the hosts from the 192.168.1.0/24 network should be seen as IP addresses 192.168.1.200–225 when accessing the hosts in the 192.168.1.0/24 network.

This configuration is known as a two-way Dynamic NAT configuration. The truth is, the NAT_Router in the middle of the diagram is not even doing any routing. It's just translating between the subnets. If you ever aspire to move on and tackle the CCIE lab, these sorts of tricks are key to have in your tool belt. Here's the configuration walkthrough:

1. As before, configure the interfaces as NAT outside and inside interfaces. In this case, it does not really matter which one is set up as inside or outside because just a private network is being translated.

```
NAT_Router#show ip interface brief
Interface                  IP-Address      OK? Method Status      Protocol
FastEthernet0              192.168.1.1     YES manual up          up
Serial0                    192.168.2.1     YES manual up          up
NAT_Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
NAT_Router(config)#interface fastethernet0
NAT_Router(config-if)#ip nat inside
NAT_Router(config-if)#exit
NAT_Router(config)#interface serial0
NAT_Router(config-if)#ip nat outside
NAT_Router(config-if)#exit
NAT_Router(config)#
```

2. Now you are introduced to a new concept: the NAT pool. This pool defines to what addresses you will translate. Based on the scenarios, you need to create two NAT pools: one for the 192.168.2.200–225 range and one for the 192.168.1.200–225 range.

```
NAT_Router(config)#ip nat ?
  inside       Inside address translation
  log          NAT Logging
  outside      Outside address translation
  pool         Define pool of addresses
  service      Special translation for application using non-standard port
  translation  NAT translation entry configuration

NAT_Router(config)#ip nat pool ?
  WORD  Pool name

NAT_Router(config)#ip nat pool NETWORK1 ?
  A.B.C.D        Start IP address
  netmask        Specify the network mask
  prefix-length  Specify the prefix length

NAT_Router(config)#ip nat pool NETWORK1 192.168.1.200 ?
  A.B.C.D  End IP address

NAT_Router(config)#ip nat pool NETWORK1 192.168.1.200 192.168.1.225 ?
  netmask        Specify the network mask
  prefix-length  Specify the prefix length

NAT_Router(config)#ip nat pool NETWORK1 192.168.1.200 192.168.1.225
➥prefix-length ?
  <1-32>  Prefix length

NAT_Router(config)#ip nat pool NETWORK1 192.168.1.200 192.168.1.225
➥prefix-length 24
NAT_ROUTER(config)#
```

This command has created a NAT pool called "Network1" that defines the correct address range necessary. Notice that this is one of the first commands you have seen that enables you to use CIDR notation (also known as "bit notation") for your subnet mask. You now need to create a second NAT pool for the other network range.

```
NAT_Router(config)#ip nat pool NETWORK2 192.168.2.200 192.168.2.225
➥prefix-length 24
```

3. You must now create a couple of standard access lists that will define the addresses that *will be translated.* This is one of the non-security uses of an access list.

```
NAT_Router(config)#access-list 50 permit 192.168.1.0 0.0.0.255
NAT_Router(config)#access-list 51 permit 192.168.2.0 0.0.0.255
```

4. Now you can put all the pieces together and turn on the NAT translation between the networks. The first thing is to define a translation going from the 192.168.1.0/24 subnet to the 192.168.2.0/24 network.

```
NAT_Router(config)#ip nat ?
  inside       Inside address translation
  log          NAT Logging
  outside      Outside address translation
  pool         Define pool of addresses
  service      Special translation for application using non-standard port
  translation  NAT translation entry configuration

NAT_Router(config)#ip nat inside ?
  destination  Destination address translation
  source       Source address translation

NAT_Router(config)#ip nat inside source ?
  list       Specify access list describing local addresses
  route-map  Specify route-map
  static     Specify static local->global mapping

NAT_Router(config)#ip nat inside source list ?
  <1-2699>  Access list number for local addresses
  WORD      Access list name for local addresses

NAT_Router(config)#ip nat inside source list 50 ?
  interface  Specify interface for global address
  pool       Name pool of global addresses

NAT_Router(config)#ip nat inside source list 50 pool ?
  WORD  Pool name for global addresses

NAT_Router(config)#ip nat inside source list 50 pool NETWORK2 ?
  overload  Overload an address translation
  <cr>

NAT_Router(config)#ip nat inside source list 50 pool NETWORK2
NAT_Router(config)#
```

If you were to read the preceding line of syntax in English, it would sound something like this: "Translate the internal addresses defined in access-list 50 into the pool of addresses defined in the NAT pool NETWORK2." Keep a mental note of that `overload` keyword you see in the final-context sensitive help; you'll make use of that soon enough. For now, let's define the translation going back the other way:

```
NAT_Router(config)#ip nat outside source list 51 pool NETWORK1
NAT_Router(config)#
```

Notice that this time an outside-to-inside translation was configured because the interface was marked as connected to the 192.168.2.0/24 subnet as the outside interface.

At this point, the networks are translating quite well. Remember that the pool of 25 addresses defined earlier allows only 25 consecutive sessions between the subnets. Any consecutive sessions above that number will fail.

NAT Overload

Finally it's time to explore the feature that made NAT famous around the network world: NAT Overload. NAT Overload is the official name of the feature that allows multiple hosts to share a single IP address. When Microsoft began allowing their servers to perform routing with the Routing and Remote Access administrative tools, they decided to call the feature Port Address Translation (PAT), which caught on in many circles. I prefer to use the former of the two terms because NAT can statically translate TCP or UDP ports to different inside local address; the true "port address translation."

The configuration of NAT Overload is a piece of cake, especially now that you've seen the prior Dynamic NAT configuration. Let's walk through a new scenario step by step. In Figure 14.7, a typical network is connected to the Internet through the NAT_Router. The router needs to be configured to perform NAT Overload to enable all the internal clients to access the Internet through a single IP address. Notice as well that the Internet IP address is assigned via DHCP, so there's no way to be sure what the inside global address is at any given point and time. Here goes!

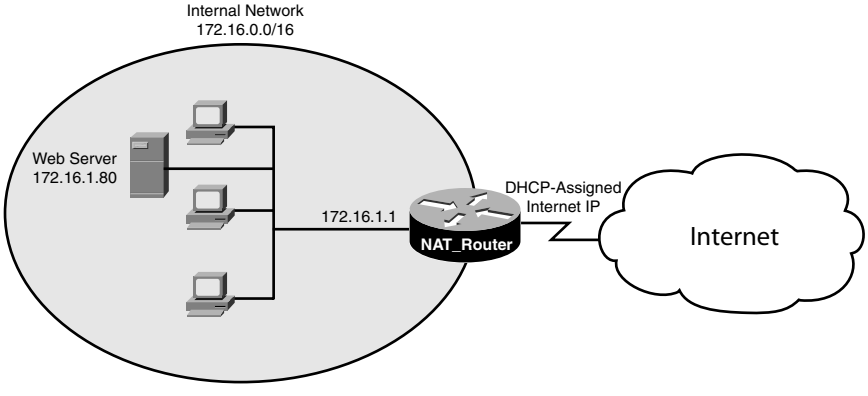


FIGURE 14.7
NAT Overload configuration.

- **Scenario 4**: Configure the network pictured in Figure 14.7 for NAT Overload, allowing all internal clients to access the Internet. In addition, configure a static entry that sends any incoming request on TCP port 80 or 443 to the internal web server.

This first thing is to become familiar with NAT_Router:

```
NAT_Router#show ip interface brief
Interface                  IP-Address      OK? Method Status      Protocol
FastEthernet0              172.16.1.1      YES manual up          up
Serial0                    68.3.160.5      YES DHCP   up          up
```

Now it's time to identify the interfaces to the NAT process:

```
NAT_Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
NAT_Router(config)#interface fastEthernet 0
NAT_Router(config-if)#ip nat inside
NAT_Router(config-if)#exit
NAT_Router(config)#interface serial 0
NAT_Router(config-if)#ip nat outside
```

Now, just as with the Dynamic NAT, you need to create an access list that identifies the addresses to be translated by NAT. Use a named access list this time:

```
NAT_Router(config)#ip access-list ?
  extended    Extended Access List
  log-update  Control access list log updates
  logging     Control access list logging
  standard    Standard Access List

NAT_Router(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name

NAT_Router(config)#ip access-list standard INTERNAL_ADDRESSES
NAT_Router(config-std-nacl)#permit ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address

NAT_Router(config-std-nacl)#permit 172.16.0.0 ?
  A.B.C.D  Wildcard bits
  log      Log matches against this entry
  <cr>

NAT_Router(config-std-nacl)#permit 172.16.0.0 0.0.255.255
```

Perfect! Now on to the final command that will enable NAT Overload for the addresses that have been defined. Once again, the "`ip nat`" syntax from Global Configuration mode is used to set this up:

```
NAT_Router(config)#ip nat ?
  inside       Inside address translation
  log          NAT Logging
  outside      Outside address translation
```

```
  pool         Define pool of addresses
  service      Special translation for application using non-standard port
  translation  NAT translation entry configuration

NAT_Router(config)#ip nat inside ?
  destination  Destination address translation
  source       Source address translation

NAT_Router(config)#ip nat inside source ?
  list       Specify access list describing local addresses
  route-map  Specify route-map
  static     Specify static local->global mapping
```

This is where the router is asking you to specify the internal addresses to be translated. Previously, the `static` keyword was used to perform 1:1 IP address or port translations; now the `list` keyword designates a list of internal addresses to be translated. The access list just created specifies which internal addresses will translate.

```
NAT_Router(config)#ip nat inside source list ?
  <1-2699>  Access list number for local addresses
  WORD      Access list name for local addresses

NAT_Router(config)#ip nat inside source list INTERNAL_ADDRESSES ?
  interface  Specify interface for global address
  pool       Name pool of global addresses
```

Now the router needs to know what inside global address the inside local addresses should use. You can designate this either by using a NAT pool (as shown with the Dynamic NAT configuration), or by specifying an outgoing interface to use. Because you do not know what inside global address you will have (because of the DHCP configuration), you need to specify the outgoing interface.

```
NAT_Router(config)#ip nat inside source list INTERNAL_ADDRESSES interface ?
  Async              Async interface
  BVI                Bridge-Group Virtual Interface
  CTunnel            CTunnel interface
  Dialer             Dialer interface
  FastEthernet       FastEthernet IEEE 802.3
  Lex                Lex interface
  Loopback           Loopback interface
  Multilink          Multilink-group interface
  Null               Null interface
  Serial             Serial
  Tunnel             Tunnel interface
  Vif                PGM Multicast Host interface
  Virtual-Template   Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing

NAT_Router(config)#ip nat inside source list INTERNAL_ADDRESSES interface
➥serial 0 ?
```

```
  overload  Overload an address translation
  <cr>

NAT_Router(config)#ip nat inside source list INTERNAL_ADDRESSES interface

➥serial 0 overload
```

There it was! The magic `overload` keyword. That's all it takes to turn on NAT Overload for the interface connected to the Internet. The router will now translate thousands of internal hosts through a single IP address. One more thing needs to be done to complete the scenario: Add the Static NAT translation for the web server. By adding this configuration, you combine NAT Overload with Static NAT, which is a very common configuration. Here goes:

```
NAT_Router(config)#ip nat ?
  inside       Inside address translation
  log          NAT Logging
  outside      Outside address translation
  pool         Define pool of addresses
  service      Special translation for application using non-standard port
  translation  NAT translation entry configuration

NAT_Router(config)#ip nat inside ?
  destination  Destination address translation
  source       Source address translation

NAT_Router(config)#ip nat inside source ?
  list       Specify access list describing local addresses
  route-map  Specify route-map
  static     Specify static local->global mapping

NAT_Router(config)#ip nat inside source static ?
  A.B.C.D  Inside local IP address
  esp      IPSec-ESP (Tunnel mode) support
  network  Subnet translation
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol

NAT_Router(config)#ip nat inside source static tcp ?
  A.B.C.D  Inside local IP address

NAT_Router(config)#ip nat inside source static tcp 172.16.1.80 ?
  <1-65535>  Local UDP/TCP port

NAT_Router(config)#ip nat inside source static tcp 172.16.1.80 80 ?
  A.B.C.D    Inside global IP address
  interface  Specify interface for global address

NAT_Router(config)#ip nat inside source static tcp 172.16.1.80 80
➥interface ?
  Async              Async interface
```

```
  BVI                Bridge-Group Virtual Interface
  CTunnel            CTunnel interface
  Dialer             Dialer interface
  FastEthernet       FastEthernet IEEE 802.3
  Lex                Lex interface
  Loopback           Loopback interface
  Multilink          Multilink-group interface
  Null               Null interface
  Serial             Serial
  Tunnel             Tunnel interface
  Vif                PGM Multicast Host interface
  Virtual-Template   Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing

NAT_Router(config)#ip nat inside source static tcp 172.16.1.80 80
➥interface serial 0 ?
  <1-65535>  Global UDP/TCP port

NAT_Router(config)#ip nat inside static tcp 172.16.1.80 80

➥interface serial 0 80
```

Beautiful. This has added the line that will translate incoming requests to the web server *in addition to performing NAT Overload for all other internal clients*. If some internal clients are accessing the Internet, you can verify that the translations are working properly:

```
NAT_Router#show ip nat translation
Pro Inside global    Inside local       Outside local      Outside global
tcp 68.3.160.5:39449 172.16.1.15:39449  66.102.7.104:80    66.102.7.104:80
tcp 68.3.160.5:39450 172.16.1.150:39450 66.102.7.147:80    66.102.7.147:80
udp 68.3.160.5:43617 172.16.1.25:43617  207.228.226.5:53   207.228.226.5:53
udp 68.3.160.5:43617 172.16.1.13:43617  64.233.161.9:53    64.233.161.9:53
udp 68.3.160.5:43617 172.16.1.14:43617  192.52.178.30:53   192.52.178.30:53
udp 68.3.160.5:347   172.16.1.13:347    202.71.97.92:123   202.71.97.92:123
tcp 68.3.160.5:39453 172.16.1.76:39453  207.228.243.100:80 207.228.243.100:80
tcp 68.3.160.5:39454 172.16.1.182:39454 207.228.243.100:80 207.228.243.100:80
tcp 68.3.160.5:39446 172.16.1.87:39446  67.138.240.17:110  67.138.240.17:110
tcp 68.3.160.5:39448 172.16.1.140:39448 67.138.240.17:110  67.138.240.17:110
udp 68.3.160.5:43617 172.16.1.140:43617 216.239.36.10:53   216.239.36.10:53
tcp 68.3.160.5:80    172.16.1.80:80     ---                --- !Web Server
udp 68.3.160.5:43617 172.16.1.67:43617  216.239.53.9:53     216.239.53.9:53
udp 68.3.160.5:43617 172.16.1.220:43617 192.5.6.30:53      192.5.6.30:53
tcp 68.3.160.5:37389 172.16.1.82:37389  68.6.19.2:110      68.6.19.2:110
tcp 68.3.160.5:39447 172.16.1.77:39447  68.6.19.2:110      68.6.19.2:110
tcp 68.3.160.5:39451 172.16.1.77:39451  64.233.167.147:80  64.233.167.147:80
tcp 68.3.160.5:39452 172.16.1.15:39452  64.233.167.147:80  64.233.167.147:80
udp 68.3.160.5:40477 172.16.1.25:40477  216.115.25.17:5061 216.115.25.17:5061
udp 68.3.160.5:40478 172.16.1.142:40478 216.115.25.17:5061 216.115.25.17:5061
udp 68.3.160.5:43617 172.16.1.150:43617 216.239.32.10:53   216.239.32.10:53
```

Holy cow! They sure are working, and it looks like the internal clients have taken advantage of that fact. If you look down the list of inside local addresses, you can see what inside hosts are accessing the Internet (along with what source port they are using to establish the request). Also, take a look at the inside global address; notice anything odd? It's the same address the whole way down, just using different port numbers. This is the perfect picture of NAT Overload. Finally, take a look at the highlighted translation. This is the Static NAT entry that was added for the internal web server. There are no outside local/global addresses for this because it is not in use at this time.

Verifying NAT Operation

Although a `show running-config` command will always be useful to show what commands you have entered into your router to get NAT running, you can use a few commands to ensure NAT is operational. The primary command you have seen may times up to this point: `show ip nat translations`. This command gives you a snapshot view of what current NAT translations are active on your router. Its sidekick command, `show ip nat statistics`, gives you a view of how many translations are currently active, how many total translations have occurred, and how much of your NAT pool is being used (if performing Dynamic NAT). A sample output of this command follows:

```
NAT_Router#show ip nat statistics
Total active translations: 12 (0 static, 12 dynamic; 11 extended)
Outside interfaces:
  Serial0
Inside interfaces:
  FastEthernet0
Hits: 38415022  Misses: 567286
Expired translations: 568274
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT_TRANSLATION interface Ethernet0 refcount 4
```

Finally, you may encounter a situation where a bad NAT translation is kept in the table. This happens frequently when you are changing your internal IP address scheme in some way, especially when you are changing individual host addresses that were just accessing the Internet. Although waiting for some time for the translations to time out solves the problem, impatient administrators may want to use the `clear ip nat translation *` command to wipe out any dynamically created NAT entries. This is not likely to disrupt service to your internal network because active NAT translations immediately re-create themselves as the internal host sends or receives data to or from the Internet.

Chapter Summary

Network Address Translation (NAT) has become so successful for prolonging the life of IPv4 that it has now become a prohibitor of a progressive move to TCP/IP version 6. Because of its widespread use, NAT features have grown over the years to provide a solution to almost any network situation.

A company planning to use NAT will deploy one of the three private address ranges on their internal network, which are prevented from routing to the Internet. They will then use one of the three forms of NAT—Static NAT, Dynamic NAT, or NAT Overload—to translate these private ranges onto the Internet. Most networks use a combination of NAT Overload and Static NAT to accomplish most major network objectives.

Most of the challenge with NAT is learning the terminology that describes the different addresses on a network. Inside local addresses are internal to a network. The inside global address represents the public Internet address assigned to your router. Ouside global addresses represent all the hosts outside of your network attached to the Internet with Internet IP addresses. Finally, outside local addresses represent hosts outside your network as they are seen by the internal NAT hosts.

Key Terms

- Network Address Translation (NAT)
- Port Address Translation (PAT)
- Static NAT
- Dynamic NAT
- NAT Overload
- private IP addresses
- public IP addresses
- inside local address
- inside global address
- outside local address
- outside global address
- port redirection
- NAT pool

Apply Your Knowledge

Exercises

14.1 Configuring NAT for a Home Network Enviroment

You would like to deploy NAT on a home network. This network has five internal hosts and receives a public Internet IP address through DHCP on a DSL connection. The Cisco 1700 router should use NAT Overload to enable all internal clients to access the Internet. In addition, you would like to use Windows Remote Desktop Client (TCP Port 3389) to access your home PC (192.168.1.100) from anywhere in the world. Figure 14.8 shows a picture of this home network with relavent addressing details.

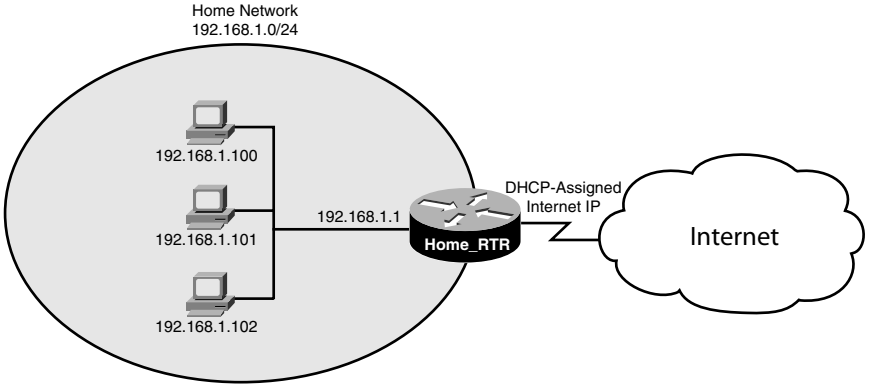


FIGURE 14.8
Home network diagram.

Estimated Time: 5–10 minutes

1. This is something that any CCNA student can do at home, provided you have some type of high-speed Internet connection. The first thing you need to do is verify your router configuration and identify your inside and outside interfaces:

```
Home_Router#show ip int brief
Interface                  IP-Address      OK? Method Status      Protocol
FastEthernet0              192.168.1.1     YES manual up          up
Ethernet0                  68.209.55.8     YES DHCP   up          up
Home_Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Home_Router(config)#int fastethernet0
Home_Router(config-if)#ip nat inside
Home_Router(config-if)#exit
Home_Router(config)#int ethernet0
Home_Router(config-if)#ip nat outside
```

2. Now you need to configure an access list that matches the internal IP addresses to be translated.

```
 Home_Router(config)#ip access-list ?
  extended    Extended Access List
  log-update  Control access list log updates
  logging     Control access list logging
  standard    Standard Access List

Home_Router(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name

Home_Router(config)#ip access-list standard INSIDE_IP
Home_Router(config-std-nacl)#permit ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address

Home_Router(config-std-nacl)#permit 192.168.1.0 ?
  A.B.C.D  Wildcard bits
  log      Log matches against this entry
  <cr>

Home_Router(config-std-nacl)#permit 192.168.1.0 0.0.0.255
Home_Router(config-std-nacl)#exit
Home_Router(config)#
```

3. Now that the access list is defined, you can put the NAT Overload in action:

```
Home_Router(config)#ip nat ?
  inside       Inside address translation
  log          NAT Logging
  outside      Outside address translation
  pool         Define pool of addresses
  service      Special translation for application using non-standard port
  translation  NAT translation entry configuration

Home_Router(config)#ip nat inside ?
  destination  Destination address translation
  source       Source address translation

Home_Router(config)#ip nat inside source ?
  list       Specify access list describing local addresses
  route-map  Specify route-map
  static     Specify static local->global mapping

Home_Router(config)#ip nat inside source list ?
  <1-2699>  Access list number for local addresses
  WORD      Access list name for local addresses
```

```
Home_Router(config)#ip nat inside source list INSIDE_IP ?
  interface  Specify interface for global address
  pool       Name pool of global addresses

Home_Router(config)#ip nat inside source list INSIDE_IP interface
ethernet 0 ?
  overload  Overload an address translation
  <cr>

Home_Router(config)#ip nat inside source list INSIDE_IP interface
ethernet 0 overload
Home_Router(config)#
```

4. The NAT Overload configuration is in place; clients are now able to access the Internet with the single, DHCP-assigned address from the DSL provider. Now you need to configure your Static NAT entry to allow remote desktop access to your internal PC.

```
Home_Router(config)#ip nat ?
  inside       Inside address translation
  log          NAT Logging
  outside      Outside address translation
  pool         Define pool of addresses
  service      Special translation for application using non-standard port
  translation  NAT translation entry configuration

Home_Router(config)#ip nat inside source ?
  list       Specify access list describing local addresses
  route-map  Specify route-map
  static     Specify static local->global mapping

Home_Router(config)#ip nat inside source static ?
  A.B.C.D  Inside local IP address
  esp      IPSec-ESP (Tunnel mode) support
  network  Subnet translation
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol

Home_Router(config)#ip nat inside source static tcp ?
  A.B.C.D  Inside local IP address

Home_Router(config)#ip nat inside source static tcp 192.168.1.100 ?
  <1-65535>  Local UDP/TCP port

Home_Router(config)#ip nat inside source static tcp 192.168.1.100 3389 ?
  A.B.C.D    Inside global IP address
  interface  Specify interface for global address
```

```
Home_Router(config)#$ inside source static tcp 192.168.1.100 3389
interface ethernet 0 ?
  <1-65535>  Global UDP/TCP port

Home_Router(config)#$nside source static tcp 192.168.1.100 3389
interface ethernet 0 3389
```

5. The configuration is now complete.

Exam Questions

1. You have an internal web server that has the IP address 172.16.5.9. You need to enable this server to be accessed on TCP port 80 from the Internet; what would be the best solution for this situation?

   - ❍ **A.** Static NAT
   - ❍ **B.** Dynamic NAT
   - ❍ **C.** NAT Overload
   - ❍ **D.** Standard routing

2. Which of the following forms of NAT incorporate the source IP address (inside local) along with the source port number to make every translation unique?

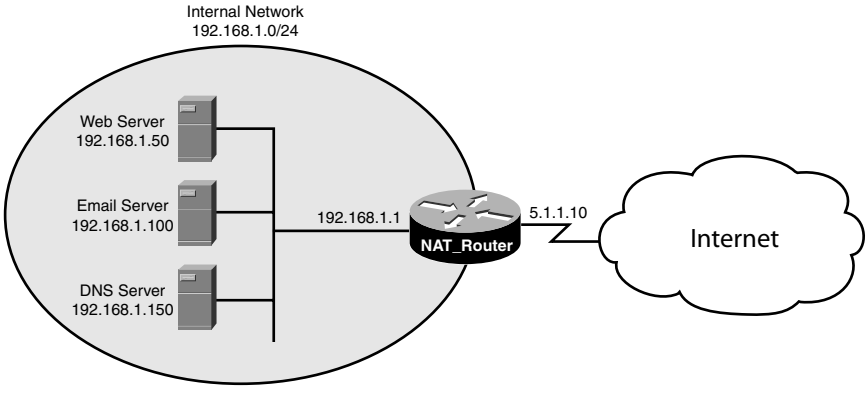
   - ❍ **A.** Static NAT
   - ❍ **B.** Dynamic NAT
   - ❍ **C.** NAT Overload
   - ❍ **D.** NAT Port Mapping

3. Which of the following commands enables an FTP server with the inside local address 10.5.9.100 to be accessed from a `Serial0` interface (that is directly connected to the Internet)?

   - ❍ **A.** `ip nat inside source static tcp interface serial 0 21 10.5.9.100 21`
   - ❍ **B.** `ip nat inside source static tcp 10.5.9.100 21 interface serial 0 21`
   - ❍ **C.** `ip nat inside destination static tcp interface serial 0 21 10.5.9.100 21`
   - ❍ **D.** `ip nat inside destination static tcp 10.5.9.100 21 interface serial 0 21`

4. Refer to Figure 14.9; according to NAT terminology, the IP address 192.168.1.100 for the email server is considered an _____.

- ❍ **A.** Inside local address
- ❍ **B.** Inside global address
- ❍ **C.** Outside local address
- ❍ **D.** Outside global address



5. Refer to Figure 14.9. According to NAT terminology, the IP address 5.1.1.10 is considered an _____.

- ❍ **A.** Inside local address
- ❍ **B.** Inside global address
- ❍ **C.** Outside local address
- ❍ **D.** Outside global address

6. Which of the following represent a private IP address? (Choose 2.)

- ❍ **A.** 192.168.5.205
- ❍ **B.** 172.32.65.31
- ❍ **C.** 10.168.5.205
- ❍ **D.** 224.16.23.1

7. The configuration of Dynamic NAT requires the use of an _____, which is a list of the inside global addresses that the Cisco router will use when translating the inside local addresses.

   - ❍ **A.** Inside interface
   - ❍ **B.** Access list
   - ❍ **C.** Outside interface
   - ❍ **D.** IP NAT Pool

8. What command is necessary to designate the inside interface in a NAT configuration?

   - ❍ **A.** `nat interface inside`
   - ❍ **B.** `nat inside interface`
   - ❍ **C.** `ip nat inside`
   - ❍ **D.** `ip inside interface`

9. You would like to see the active NAT translations that are happening on your router. Your primary interest is in the inside local IPs that are being translated. What command shows you this information?

   - ❍ **A.** `show ip nat statistics`
   - ❍ **B.** `show ip nat translations`
   - ❍ **C.** `show ip interface`
   - ❍ **D.** `show running-config`

10. You have just changed one of your internal computer's IP addresses and it appears that it can no longer access the Internet. You have verified the correct subnet and gateway information. What commands should you perform on the router to ensure cached information does not play a role in this failure? (Choose 2.)

    - ❍ **A.** `clear arp`
    - ❍ **B.** `clear ip route`
    - ❍ **C.** `clear ip nat translations*`
    - ❍ **D.** `clear startup-config`

Answers to Exam Questions

1. **A.** Static NAT provides the best solution when you need a 1:1 translation from a private address or port number to a public address or port number. Answer B is incorrect because Dynamic NAT allows many hosts to be translated at the same time. Answer C is incorrect because NAT Overload allows many internal hosts to share a single Internet IP address. Answer D is also incorrect. Standard routing does not work because private addresses are blocked from traversing the Internet.

2. **C.** NAT Overload uses the source port number to send many unique requests out a single, public IP address. Answer A is incorrect because Static NAT performs 1:1 translations from public to private IP addresses. Answer B is incorrect because Dynamic NAT performs many 1:1 translations without requiring manual entries. Answer D is incorrect because NAT Port Mapping is not a valid form of NAT.

3. **B.** This syntax correctly lists the source address (inside local) and port number first and the inside global address and port second. The IP NAT `inside destination` syntax enables you to specify only a list of inside global addresses and does not work for this situation. Answers A, C, and D use invalid syntax.

4. **A.** Inside local addresses encompass any address on your internal network that is translated to the outside network via NAT. Answer B is incorrect because the inside global addresses are the IPs assigned to the outside interface of your router. Answer C is incorrect because the outside local addresses are outside (Internet) addresses as they appear to a NAT device. Answer D is incorrect because the outside global addresses are standard Internet-attached devices.

5. **B.** The inside global addresses are the IPs assigned to the outside interface of your router. Answer A is incorrect because inside local addresses encompass any address on your internal network that is translated to the outside network via NAT. Answer C is incorrect because the outside local addresses are outside (Internet) addresses as they appear to a NAT device. Answer D is incorrect because the outside global addresses are standard Internet-attached devices.

6. **A, C.** The private address ranges are 10.x.x.x, 172.16.x.x–172.31.x.x, and 192.168.x.x. Answers B and D fall outside these ranges.

7. **D.** Dynamic NAT requires the use of an `ip nat pool` that lists the inside global addresses (typically Internet-valid) that will be used for the translation. Answer B is incorrect because access lists are used to define the inside local addresses that will be translated. Answers A and C are incorrect because the inside and outside interfaces must be defined, but do not define what addresses are to be translated.

8. **C.** The `ip nat inside` designates the inside interface to the NAT router. The other commands are considered invalid syntax.

9. **B.** The `show ip nat translations` shows you all active translations currently in place on your router. It includes the inside local and global and the outside local and global addresses for each translation. Answer A is incorrect because the `show ip nat statistics` command tells you only how many translations are currently happening. Answer C is incorrect because the `show ip interface` command does not give you any NAT statistics, and answer D is incorrect because the `show running-config` command tells you only the NAT configurations you have set up.

10. **A, C.** The `clear arp` command ensures that the router does not have the incorrect MAC address mapped to the computer's IP address. The `clear ip nat translations *` command ensures that the cached NAT translations are not pointed to the wrong IP address. Answer B is incorrect. The `clear ip route` is not necessary because the routing table did not change, and could cause downtime for your router. Answer D is incorrect because the `clear startup-config` does not remove any cached configuration.

Suggested Reading and Resources

1. Cisco TAC NAT Configuration Syntax, http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfipadr.htm#wp1042290
2. Ward, Chris and Cioara, Jeremy. *Exam Cram 2 CCNA Practice Questions*. Que Publishing, 2004.
3. How Network Address Translation Works, http://computer.howstuffworks.com/nat1.htm

CHAPTER FIFTEEN

15 Wide Area Networks

Objectives

Describe the function of Wide Area Networks as it relates to Cisco routers

Understand the variety of Wide Area Network connections and the advantages and disadvantages of each

Configure point-to-point Wide Area Network connections using the High-level Data Link Control (HDLC) and the Point-to-Point Protocol (PPP)

Verify Wide Area Network connectivity and operation

- Up until now, you have studied a variety of technologies used to combine multiple networks into a single autonomous system. Now it's time to discuss the technology that is used to connect those networks over a larger geographical area.
- To meet the industry network requirements, many types of Wide Area Network connections and protocols are available. Each offers a different set of advantages and disadvantages. This chapter discusses each one to ensure you can make an informed decision when choosing between network connectivity options.
- This chapter focuses on the configuration of dedicated (private) connections between offices. When using these types of connections, you have the option of using HDLC or PPP for the Data Link connectivity. The configuration of these two protocols and their related options are covered in depth.
- After the Wide Area Network connection has been configured, this chapter discusses the commands used to troubleshoot and ensure correct operation.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- Although Wide Area Network configuration is important, many of the advanced configuration options discussed are reserved for the CCNP BCRAN exam. At the CCNA level, be sure to focus on understanding the concepts thoroughly.
- Because it is in widespread use, focus your energy on learning the ideas behind the PPP protocol. Be sure to pay special attention to the authentication concepts.

Introduction

In nearly all traditional Cisco texts, Wide Area Networks (WANs) are typically moved to the end of the book. This is amusing to me because WAN connectivity is usually listed in the top three functions of a router. WAN connections do just that: connect networks that have a wide area separating them. This type of connection requires you to work with one or more service providers that supply the logical connections between your locations.

The good news about WAN connections is this: These technologies only encompass only the Physical and Data Link layers of the OSI Model. Just like the concepts of ethernet and token ring, WAN links are just another method of transporting data between devices. So with only two layers worth of technology, WAN links should be fairly simple to learn, right? Well, that's the bad news: Because of the ever-increasing demands of the IT machine, WAN links have become increasingly complex to the point where they can be a specialization in themselves. Thankfully, the CCNA exam focuses primarily on three specific types of WAN connections:

- Leased Lines
- Integrated Services Digital Network (ISDN)
- Frame Relay

EXAM ALERT

To prepare for the CCNA exam, you need to be very familiar with these WAN connections.

Although there are many more WAN connection types, these are currently the most popular. By studying these WAN connections you will learn the foundation concepts behind WAN connections in general, making it easier to learn any new WAN technologies as they emerge.

WAN Connection Types

The following three categories of WAN connections comprise most of the connections used by businesses around the world. As the name implies, each of the WAN connection categories contains multiple connection types. If you ever called a service provider and asked for a packet-switched connection, the next question would inevitably be, "What type?"

Leased Lines

This connection category is what most people are familiar with when they hear the term, "WAN connection." A leased line connection provides a dedicated, point-to-point link

between two locations. The beauty of this connection type is that you have a virtual private road between your sites. You have complete control over the traffic on that road; nobody else can share the road with you. If you have a T1-speed connection (1.544Mbps) between your locations, that bandwidth is always dedicated to you, regardless of whether you use it or not. Therefore, leased lines are typically the most expensive connection types.

In the Field

The two factors that directly affect the cost of a leased line are

- How far apart, geographically, the sites are located
- The amount of bandwidth required

Leased lines are the most appropriate when you need a fixed amount of bandwidth and complete control over all your traffic. Companies that are implementing Voice over IP (VoIP), which runs their telephone system over the data network, will usually vie for leased line connections. Because the telecommunications carrier (service provider) is dedicating the leased line bandwidth to you, they can provide a guaranteed level of service. This not only includes the uptime (reliability) of the line, but also delay requirements. The delay of the line is how long it takes a packet to get from the entry point to the end of the connection. Long delays can cause the quality of a VoIP call to degrade to the point of sounding like a bad cellular phone call. Because the service provider typically has end-to-end control over a leased line connection, they can guarantee a specific level of delay.

Circuit-Switched Networks

Anytime you hear the hum of a dial tone followed by the rhythmic beeping of digits, you are more than likely connected to a circuit-switched network. This type of connection establishes a dedicated channel (or circuit) for the duration of the transmission, and then tears down the channel when the transmission is complete. This is known as a *dial-on-demand connection*. The largest circuit-switched network in the world is the telephone system, which links together many different network segments to create an end-to-end circuit for each telephone call.

Circuit-switched networks can be called a "connection-oriented" network type. They are most useful when you have small amounts of data to reliably send at a time. Some circuit-switched networks charge on a per-use or per-minute basis (primarily ISDN), so the amount you pay for the connection is directly related to how much you use it. This type of connection would be ideal for a small office that uses local area network (LAN) connectivity during the day and then replicates all the updated data back to the main site in the evening. For example, you might have a sales office that creates a log of transactions that it sends back to the corporate headquarters at night.

Packet-Switched Networks

Packet-switched networks enable the service provider to create a large pool of bandwidth for their clients, rather than dedicate specific amounts of bandwidth to each client (as in leased lines). The client can then dictate what circuits they would like established through the service provider network between their sites (these are called *permanent virtual circuits*), providing an end-to-end connection. By using packet-switched networks to provide WAN connectivity, you can gain lower-cost WAN connections that can potentially provide more bandwidth to your locations.

When you sign up for a packet-switched network, the service provider gives you a guaranteed level of bandwidth. The higher your service guarantee, the more you pay for the connection on a monthly basis. The great aspect of a packet switched network is that you usually get more than you are guaranteed; depending on the type of contract you negotiate with the service provider, you could get much more bandwidth than you are guaranteed. However, you must realize that this bandwidth is just that: non-guaranteed. If you send extra traffic during a busy time of day, the service provider can drop the traffic and be well within the service contract. This also applies for delay guarantees. Because traffic sent through a packet-switched network may take different paths (depending on the service provider's infrastructure) to reach the destination, most service providers offer a very loose delay guarantee (if they decide to offer one at all).

Broadband

Broadband technology, in its base definition, is a system that enables you to send multiple signals over a wire at one time. The alternative technology, baseband, enables you to send only a single signal over the wire at a time. Broadband connections primarily encompass small office/home office (SOHO) WAN links that use cable modem or DSL technology to connect to the Internet. A cable service provider sends multiple signals over a cable coaxial line, enabling a home user to run many services, such as cable television, high-speed Internet, and telephone service, over a single line. Telephone providers are offering the same services through the copper phone line connections.

Medium and large businesses are just now beginning to consider cable and DSL connections as backup Internet connections for their main offices. Broadband technology is one of the newest WAN connection offerings to market, and has yet to prove its reliability on a long-term basis.

Virtual Private Networks (VPNs)

VPNs are not a specific type of WAN connection, but are often used to accomplish the same purpose as a WAN connection. Connections to the Internet have become widely available at

an extremely low cost (when compared against the other types of WAN connectivity). Rather than purchasing dedicated circuits between locations, you can just purchase a standard Internet connection at each site. The quality of your Internet connection determines the quality of your WAN connectivity. After all sites have a connection to the Internet, you can then create tunnels through the Internet to each location, enabling the sites to connect through a full-mesh relationship (every site is directly connected, through the Internet, to every other site). These tunnels isolate the interoffice connectivity from the rest of the Internet traffic and secure the traffic through heavy encryption algorithms.

The VPN tunnels are created with the application of a heavy amount of encryption to the traffic sent between the locations. Because sending your company's private data across a public network, such as the Internet, could be perilous, you should scramble (encrypt) your data before sending it. Because the process of encrypting and de-encrypting data is extremely hard on a router processor, you may choose to offload this work to a router VPN card (a hardware add-on), a PIX firewall (Cisco's firewall platform), or a VPN concentrator (a specific device manages and maintains many VPN connections). Within this concept lie the advantages and disadvantages of using VPNs for your WAN connections. The major advantage is the cost: You can establish full connectivity between all your locations for a small fraction of what it would cost to purchase dedicated WAN links. You can also allow home users to connect into the office through a VPN connection to allow for telecommuting employees. The disadvantage is the delay incurred in applying the VPN encryption algorithms and the unreliable nature of the Internet. Although the Internet is the most redundant network in the world, because of the massive amount of traffic that crosses the Internet daily, the delay can be inconsistent.

Metropolitan Ethernet (Metro Ethernet)

Metro ethernet technology began to emerge early in the new millennium as a viable alternative to traditional WAN connections when connecting offices within a metropolitan area (primarily major cities). At the end of the century, .com-based businesses were booming. Many of these companies began laying complex fiber optic–based networks throughout many of the major metropolitan areas of the nation. When the world economy plummeted at the turn of the century, many of these .com companies went out of business, leaving huge amounts of unmanaged fiber cable under the city streets. This fiber was quickly acquired by local service providers and is slowly being leased to their customers.

Using this fiber to connect offices in the same general region allows for WAN links at speeds of 1000Mbps or greater, at a fraction of the cost of a standard T1 line. The WAN link can even terminate onto a standard Category 5E/6 UTP copper cable and plug directly into a switch using a fiber to copper converter at the customer premise. This enables the WAN connections to be managed completely through VLANs with no dedicated router hardware in place. The connections, which are already fast enough, become even faster.

Metro ethernet is beginning to stretch even between cities, as service providers are planting fiber-optic cable runs between major metropolitan areas. It shouldn't be too long before intra-nation WAN links are rated in terms of Gbps as a standard. Metro ethernet is becoming quite popular in government organizations that have many locations in the same general geographic region.

EXAM ALERT

For the CCNA exam, you should be familiar with the following network types:

- **Leased Lines**
- **Circuit Switched**
- **Packet Switched**

The WAN Physical Layer

The physical connections for WANs are very diverse, primarily because of the diverse form factors that were created by CSU/DSU manufacturers. The Channel Service Unit/Data Service Unit (CSU/DSU) device is the box that connects and converts your WAN cabling to the service provider's WAN cabling. Although CSU/DSUs often have many lights, buttons, and LCD displays, they are typically nothing more than a glorified terminal adapter, converting between the service provider's cable and your local router connection. Figure 15.1 shows a typical physical layout for a WAN connection.

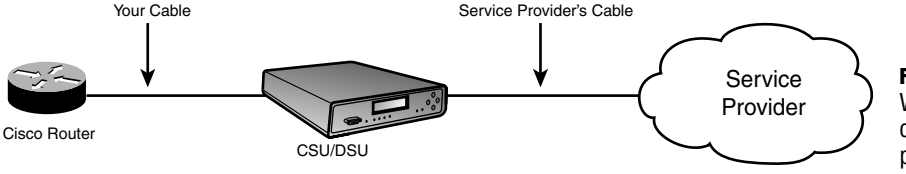


FIGURE 15.1 WAN physical connection points.

If a CSU/DSU is involved, you will be responsible for purchasing the cable that connects your router to the CSU/DSU unit.

Cisco routers primarily use serial interfaces when connecting to a WAN. The Cisco interfaces come in two types: DB-60 serial interfaces and Smart Serial interfaces. Typically, older routers use the DB-60 style interfaces, whereas newer routers use the Smart Serial interfaces. The DB-60 interface received its name because of the 60 pins in the interface. Smart Serial interfaces are much more space efficient, and can squeeze two interfaces into the same WAN Interface Card (WIC) that the DB-60 interface used.

These WIC interfaces can be installed into any of Cisco's mainline routers (1700 series, 2600/2800 series, 3600/3800 series).

After you have installed the interface, you must then purchase the cable that connects your router to the CSU/DSU. This cable converts from one of Cisco's two proprietary interface types (DB-60 or Smart Serial) to a standards-based CSU/DSU connector. Five primary standard connectors have been created for the CSU/DSU units: V.35, X.21, EIA/TIA-232, EIA/TIA-449, and EIA/TIA-530. The most common connector in North America is V.35.

Notice how these cables convert from the Cisco proprietary Smart Serial or V.35 connector to the industry standard V.35 connector, which would connect to the CSU/DSU device.

T1 and other ISDN PRI interfaces use an RJ-48 connector. These interface types usually come with a built-in CSU/DSU, which eliminates the need to purchase an outside box and thereby eliminates another point of potential failure in your network. Upon initial inspection, the RJ-48 connector looks exactly like the RJ-45 connector used for ethernet technology, but don't be fooled! The RJ-48 connector is very different. First off, it is fastened to Shielded Twisted Pair cabling (STP) instead of the standard Unshielded Twisted Pair (UTP) of ethernet. This reduces line noise on these connections. This is important because WAN connectivity is much more susceptible to interference than LAN cabling. In addition, the voltage sent across these wires, the pin-out arrangement, and the line capacitance is different on the RJ-48 connection than RJ-45.

WAN Data Link Encapsulations

After you have the Physical layer plugged in, you must move up to the Data Link WAN encapsulation. Just as with the Physical layer, a variety of standards are available for the data link connections. However, the choice of the Data Link protocol is usually much simpler. As long as your WAN connection supports the Data Link encapsulation you use and you are using the same type of encapsulation on both ends of the connection, the WAN link will work. Sometimes, the type of WAN connection you are using forces you to choose one, specific Data Link encapsulation. For example, if you sign up with a service provider for a Frame Relay connection, you must use Frame Relay Data Link encapsulation. Likewise, if you sign up for an ATM connection, you must use ATM encapsulation. Other times, there may be some flexibility on the choice of protocol you can use. For example, if you sign up for a point-to-point T1 or an ISDN BRI connection, you can use Cisco HDLC, SLIP, or PPP for your data link encapsulation. Here is a brief description of each of the encapsulation types.

Serial Line Internet Protocol (SLIP)

SLIP is a standards-based protocol for point-to-point serial connections that use only TCP/IP. This was primarily used for dial-up connections to the Internet back in the earlier days of the Internet. It has been widely replaced by PPP.

Point-to-Point Protocol (PPP)

This protocol has largely replaced SLIP connections for point-to-point WAN connections and dial-up networking. PPP was released as an improvement to SLIP and added support for non-TCP/IP protocols and encrypted authentication (among many other features). PPP is the most popular protocol for connecting ISDN or point-to-point WAN connections.

Cisco High-Level Data Link Control (HDLC)

HDLC was originally designed as an open standard protocol, meaning all routers could support it. However, the open standard version of HDLC was pretty horrible. It did not support multiple network-layer protocols, which meant that you could support only one protocol (such as TCP/IP, IPX/SPX, or AppleTalk) over your WAN connection. In view of this shortcoming, Cisco modified the standard HDLC to support this missing feature. However, anytime a standard is modified, the protocol becomes proprietary. In this case, you can use HDLC only on Cisco routers to connect to other Cisco routers. HDLC is the default encapsulation on all serial interfaces on Cisco routers. Although HDLC does not have as many features as PPP, it does offer very low overhead, which makes your WAN connections very efficient.

X.25 Link Access Procedure, Balanced (LAPB)

This encapsulation is used on X.25-based networks, which is the predecessor to Frame Relay. Although X.25 is used rarely in well-developed countries, it has widespread use in countries not as technologically advanced.

Frame Relay

This encapsulation relates directly to the Frame Relay WAN connection, which is the faster successor to X.25. Frame Relay increased its speed capabilities by removing much of the error correction that is no longer needed on the more reliable circuits of today. Frame Relay has widespread use in nearly all well-developed areas.

Asynchronous Transfer Mode (ATM)

This technology is very similar to frame relay, but chops packets into very small pieces (53 bytes each) called *cells*. Because all the frames are exactly the same size, routers are able to process them much quicker. ATM also has the capability to run at very fast speeds because it adapts to run over fiber optic cabling.

PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA)

These technologies have been implemented to allow service providers to harness the features of PPP on an ethernet or ATM connection. This technology is primarily used in DSL high-speed Internet deployments.

EXAM ALERT

The CCNA exam requires you to be familiar with the configuration of HDLC, PPP, and Frame Relay encapsulation types.

Cisco HDLC

As mentioned previously, HDLC in its truest form is an industry standard created by the International Organization for Standardization (ISO). These are the same folks who created the OSI Model (bless their hearts). Because the ISO version of HDLC lacked the support for multiple protocol use, Cisco modified it and caused HDLC on Cisco routers to become a proprietary protocol.

The beauty of HDLC is that it is very simple and works out of the box. Typically, if you are deploying a WAN connection with a Cisco router on each side of the link, it eliminates plenty of troubleshooting involved in trying to enable the connection with HDLC, even if you plan on using PPP in the long run. Because HDLC is so simple, there are no options to negotiate and you can rule it out of any troubleshooting you may encounter. If the link is not coming up, it is usually something on the service provider side of the business.

Because HDLC is enabled by default, you don't need to perform any additional configuration for the data link configuration of your serial interfaces. However, if the data link encapsulation was changed to something other than HDLC, you can re-enable HDLC by moving into interface configuration mode for the serial interface you want to use and type the command `encapsulation hdlc`.

PPP

The PPP protocol has become the industry standard for connecting multi-vendor environments over WANs. Whenever people think about using an "industry standard" for anything, they usually think of the bland, saltine-cracker type of protocol. Surprisingly, PPP defies the norm and is one of the most feature-packed WAN protocols in existence. Although it functions at the Data Link layer of network connectivity, it comprises multiple sub-protocols that serve multiple functions. This provides you with a feature-rich connection, even when bringing up a WAN link between non-Cisco devices.

PPP can function over nearly any type of WAN connection that does not implement its own, specific mechanism for transporting data (such as frame relay and ATM). This means you can use PPP to connect if you are using an asynchronous (modem-like) connection or a synchronous (high-speed) point-to-point serial connection. ISDN connections barely function without using the PPP data link encapsulation because ISDN relies on the multilink functionality of PPP to properly bundle all the individual channels of the circuit into a single, logical connection.

Although PPP fills a single layer on the OSI Model (the Data Link layer), it has multiple "sub-layers" that give it all its functionality. Each sub-layer adds specific functionality to the PPP protocol suite. Figure 15.2 depicts the three PPP sub-layers as they relate to the OSI model. Notice that all three of these sub-layers fit into the single Data Link layer.

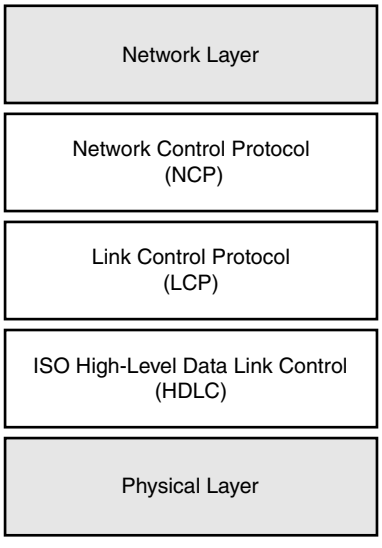


FIGURE 15.2 PPP sub-layers.

It is easy to get confused when expanding the already confusing OSI model into sub-layers for a specific protocol. This is just a logical view of the PPP protocol describing how it is able to include all the functions it advertises. The following sections look at each of these sub-layers, one at a time.

EXAM ALERT

You need to know the sub-layers of PPP and their functions for the CCNA exam because these directly relate to the features PPP provides.

Sub-Layer 1: ISO HDLC

Initially, seeing this layer in PPP seems quite odd. Wasn't HDLC a competing protocol to PPP? This sub-layer of PPP comprises the industry standard ISO HDLC. This sub-layer is responsible for allowing PPP to be supported by multiple devices. It gives the devices that run PPP common ground to stand on when they communicate with each other. As you will see in just a moment, the LCP layer above is responsible for negotiating all the features of HDLC. Because all devices that run HDLC may not support every single feature, the HDLC sub-layer enables the base PPP communication to continue, even if the platforms support different features.

Sub-Layer 2: Link Control Protocol (LCP)

You can think of the LCP sub-layer as the feature negotiation layer. All the features that PPP supports are negotiated by LCP. These features are

- Authentication
- Callback
- Compression
- Multilink

EXAM ALERT

Be able to pick the features negotiated by LCP out of a line-up.

Authentication

The authentication features of PPP enable you to require a username and password for the connecting device to bring up the WAN connection. This is not a very important feature on leased line, point-to-point connections because the only way a hacker would be able to get a device connected to the WAN would be to render one of the on-site administrators unconscious and replace the on-site router with one of the hacker's own. The PPP authentication features are most useful for dial-up connections that could be reached by users connected to the Public Switched Telephone Network (PSTN).

For example, you may choose to connect a modem to your router through the AUX port to allow dial-up access, should all the LAN and WAN connectivity to the router fail. This modem would be assigned a phone number, accessible from any computer modem in the world. PPP authentication would require a username and password to be entered before the modem connection would bridge a successful connection.

There are two types of authentication supported by PPP: the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP).

PAP

This authentication protocol is one of the earliest authentication types to be released for WAN connectivity. If PAP is enabled for the connection, the call flow progresses as follows:

1. Client dials up to a router running PPP.
2. After the link (connection) is established, *the client* sends its username and password at the LCP (feature) layer.
3. The PPP router checks the username and password against its user database and allows or denies the client.

Although this list of three steps is a logical authentication process, it has a few flaws. First off, the client dictates the timing of sending the username and password; the server (router running PPP) receives the username and password whenever the client decides to send it. This causes the PAP mechanism to be susceptible to playback attacks. This is a type of attack where a hacker captures (sniff) packets from a conversation and then plays the packets back in an attempt to mirror the connection. Because the client is in complete control of the authentication attempt, the server accepts the played-back packets whenever the client decides to send them.

The authentication of PAP is also done in clear text, which makes it even more vulnerable to packet-sniffing intruders. Anyone who does have a way of monitoring the connection can capture the packets, break them open, and find the username and password used for authentication in clear text. Can you say, "network devastation"?

With all this being said, the only reason you would choose to use the PAP method for authentication is if you were using very old equipment that did not support the newer method of authentication, CHAP.

CHAP

CHAP is a much more secure procedure for connecting to a PPP-based system. The authentication process for CHAP goes like this:

1. Client dials up to a router running PPP.
2. The *router* sends a challenge message to the client.
3. The client responds with the *hash* of the password it is configured to use.
4. The router looks up the password hash against its database. If the hash matches, the client is allowed into the network.

5. After the client is authenticated, the router sends re-authentication messages at random intervals, requiring the client to send the password hash whenever prompted.

Doesn't that list already make you feel better than PAP? The first thing to notice is that the router (server) is in control of the authentication process. Rather than accepting the username and password whenever the client decides to send it, the router demands the username and password on its timeframe. If the client isn't ready to ante up with the credentials, the server immediately terminates the connection. This makes performing a playback attack much more difficult to accomplish.

Even if a hacker were to successfully execute a playback attack with CHAP, the random authentication interval ensures the hacker will not be connected for long. Executing the initial playback attack would require intricate timing for the hacker to be successful. The random authentication requests would be nearly impossible to keep up.

The clear text issues have also been solved by using a system known as *password hashing*. Without getting too deep into cryptography and security mechanisms, you must understand that this is not the same thing as encrypting a password and sending it across the network. Given the time, nearly any encryption algorithm can be broken if the data is captured. Using a hashed version of the password means that the client never actually sends the real password across the line. To accomplish this, the router (PPP server) and the PPP client must be configured to have the identical password. Before the client sends the password, it runs an irreversible mathematical algorithm on the password. The result of that algorithm is called the hash, which is sent to the server. The server runs the same algorithm on its password and compares the two hashes. If the answer is the same, the client successfully authenticates.

Now, you may be thinking the same thing I did when I first heard about this process, "Well, can't you just get the mathematical formula and reverse it to figure out what the password is from the hash? For example, if the formula is (*the password)*× 2 = *the hash*, could you just take *the* (*hash*÷2) = *the password*?" Fair question, but just wait until you see the formula. The hashing method (formula) used is known as the MD5 hash. This formula has been *engineered* with the sole purpose of being irreversible. With that in mind, someone might capture the password hash and find out that it is 5,381,120,123,590. Now the trick is to reverse-engineer an irreversible formula to figure out how the algorithm came up with that answer. It would be much easier for hackers to render the IT staff unconscious at whatever site they were looking to compromise and steal the servers containing the data they needed.

Callback

Just as the name implies, the PPP callback functionality enables a dial-up server (or router) running PPP to use a predefined number to call the person back who initially dialed into the location. One of the major advantages of this function is the increased security: It requires the dial-up user to authenticate and then be present at the predefined phone number to be able to receive the return call. The other advantage is the toll consolidation. If you have long distance

users dialing into the network, you leave your company at the mercy of the long distance carriers of your users. By using PPP callback, you can ensure that the company long distance charges are applied, which are typically much lower than normal carrier charges.

A PPP callback process goes through the following steps:

1. A user dials into a router using PPP and authenticates.
2. Upon a successful authentication, the router terminates the connection (typically without any notification) and dials the user back at the predefined number configured by the administrator.
3. Upon reconnect, the user authenticates a second time.
4. Upon a successful authentication, the user is granted network access.

Compression

When I first heard about compression on a WAN link, my mind flashed back to the days of the Stacker compression program of Microsoft DOS. This program slowed your computer down to a crawl to gain a few megabytes of storage space on a hard disk. Surprisingly, one of the two compression algorithms used on PPP WAN connections is named "Stacker"; however, the effects are much less devastating than they were with the old DOS program.

Using compression to make your WAN connection more efficient is not a new concept. These technologies have been around since the days of DOS. However, these technologies have become much more viable on today's networks because of the increase in CPU and memory resources on network equipment. The tradeoff when choosing to use compression is that you gain more WAN bandwidth by sacrificing your router's processor and memory resources. How much you sacrifice depends on the type of compression algorithm you use.

Stacker

The compression type analyzes the data that is being sent and replaces continuous streams of characters with codes. These codes are stored in a dictionary and looked up on the other end of the connection to rebuild the original data. The Stacker algorithm (which is actually called Lempel-Ziv) uses a "flat dictionary-style compression." This means that for every packet of data, it goes through the same process: Look up the character streams in the dictionary, replace the characters with codes, begin again. Therefore, it is very good for network connections that have constantly varying data types (such as SQL, HTTP, FTP, and so on) crossing them. It doesn't matter what the previous traffic was; the same compression algorithm is applied. The Stacker algorithm is notoriously heavy on CPU resources and has less effect on the router's memory resources.

Predictor

This compression algorithm received its name because it literally attempts to predict the next character stream that will be sent or received. It uses a similar dictionary lookup process as Stacker; however, it takes the most common characters looked up and builds a cached index file. Anytime some traffic needs to be sent or received, the index file is checked first. If the character stream (or codes) is not found in the index file, it then consults the full dictionary to find the necessary compression or decompression algorithm. Therefore, the Predictor algorithm works best on network connections that have fairly similar traffic patterns (that can be cached in the index file). For example, perhaps you have a WAN link back to a central office that houses an intranet server that users access to update the corporate e-commerce website. In this case, the traffic patterns would be very similar (HTTP/HTTPS) for most times of the day. The Predictor algorithm usually uses more memory resources and has less effect on the router's CPU than the Stacker algorithm (as long as the traffic patterns do not vary largely).

Microsoft Point-to-Point Compression

Microsoft has its own compression algorithm for PPP, aptly named the Microsoft Point-to-Point Compression (MPPC). This protocol offers slightly improved processor and bandwidth utilization for Microsoft Windows–based clients. Because other devices, such as Cisco routers, would need to support this compression algorithm for Microsoft Windows to use it, Microsoft released the algorithm as an RFC standard (RFC 2118). Under the licensing in this RFC, Microsoft permits other vendors to implement MPPC solely for the purpose of connecting to other MPCC clients. MPPC therefore is used only to allow Windows dial-up users to use compression.

Multilink

PPP multilink enables you to bundle multiple WAN connections (or WAN channels in the case of ISDN) into a single, logical connection. This could be as small as bundling two 33.6Kbps modems together to make a 67.2Kbps connection, or bundling four T1 lines together to give yourself a 6.176Mbps connection. The separate interfaces that are bundled together are no longer seen as individual interfaces, but rather join a larger "logical" multilink interface. You can assign this single interface its own IP address, configure authentication, or optimize the logical line with compression. It acts and feels like a real interface, even though it could potentially comprise many physical links.

There are two major benefits to using Multilink PPP (MLPPP). First off, the logical link becomes a single point of management. Rather than figuring out what the traffic utilization is on all the individual physical lines, you can focus your monitoring software (if you have some) on just a single interface. The second benefit to MLPPP is the fact that all physical links bundled in the logical group get *exact* load balancing. When I say "exact," I mean the down-to-the-exact-bit-level kind of exact. MLPPP chops all your packets (referred to as *fragmentation*) into exactly equal sizes before it sends them across the line. This leads to the one drawback of using MLPPP: slightly increased processor and memory utilization on your router.

Sub-Layer 3: Network Control Protocol

The final sub-layer of PPP is what gives it the functionality to allow multiple Network layer protocols to run across a single WAN link at any given time. I think of this layer as the PPP DUPLO® LEGO® block connector. Have you ever seen the DUPLO® blocks for small children? They all have that standard connector with which any other DUPLO® can connect so the child can put any two pieces together (which provides positive affirmation, I'm sure). In that same sense, the Network Control Protocol (NCP) sub-layer of PPP has open-source, network-layer connectors that anyone can plug into. For example, the TCP/IP protocol has a connector called IPCP (the CP stands for "control protocol") that enables TCP/IP to run across a PPP WAN link. IPX/SPX has a connector called IPXCP. With the open-source nature of this protocol, I could create a "Jeremy protocol" and then write a JeremyCP to allow it to run across a PPP WAN link. Cisco has written its own extension called CDPCP that enables the Cisco Discovery Protocol to run across a PPP WAN link, which enables the routers on each end of the connection to use CDP to see each other.

Configuring PPP

The configuration of PPP without any options does not even deserve its own section. All you need to do is access the interface you would like to enable to run PPP and type the command `encapsulation ppp`. After you do that on both sides of the connection, you're finished. For example, if I wanted to configure PPP on the Serial 0 interface of a router, here is the process:

```
AccessServer#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AccessServer(config)#interface serial 0
AccessServer(config-if)#encapsulation ppp
```

After you begin turning on the options, the configuration can get a little more complex. This chapter discusses turning on PPP authentication and compression. PPP multilink is covered in the ISDN chapter because it is more conducive to the ISDN technology.

Authentication

The CCNA exam focuses on configuring PPP authentication between two Cisco routers rather than using authentication for dial-up users (this is covered in the Building Cisco Remote Access Networks CCNP course). Typically, when Cisco routers are performing authentication on a WAN link, the routers will be configured as two-way authentication. Two-way authentication means that both routers authenticate each other. Typically, when a dial-up user connects to a router, one-way authentication is performed (the user must authenticate to the Cisco router, not vice-versa).

To set up CHAP PPP authentication, you must do the following:

1. Turn on PPP encapsulation.
2. Configure the necessary hostname for the authenticating routers.
3. Create user accounts on each side of the connection.
4. Turn on CHAP PPP authentication.

At first, these steps may seem somewhat cryptic, but let me walk you through a configuration example and explain how all these pieces fit together. Refer to Figure 15.3 for a visual of this example configuration.

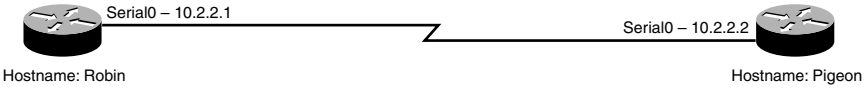


FIGURE 15.3 PPP authentication example.

This sample configuration enables two-way, CHAP PPP authentication between the Robin and Pigeon routers. For the sake of brevity, assume the router hostnames are already configured and PPP encapsulation has been enabled under the serial interfaces.

Before you begin, you need to understand the significance of the router hostname. By default, when a Cisco router attempts to authenticate with another router, it uses the router hostname as its PPP username to authenticate with the other side. In this example, the router with the hostname "Robin" crosses the PPP link and attempts to authenticate with the Pigeon router, using the username "Robin." The Pigeon router attempts to authenticate with the Robin router, using the username "Pigeon." You therefore need to create user accounts on each router that match the usernames the routers will use when authenticating. The following syntax accomplishes this:

```
Pigeon#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Pigeon(config)#username Robin password cisco

Robin#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Robin(config)#username Pigeon password cisco
```

Now, when the Robin router comes over to the Pigeon router and says "My username is Robin," the Pigeon router has a user database that identifies that username. Likewise, the Pigeon router can now authenticate the Robin router. If you have any experience with Windows administration, this is an identical concept to creating user accounts for people to log on to their PCs.

CAUTION

The CHAP username and passwords are both case sensitive. If the hostname of your router begins with a capital letter, ensure you create the user account the same way.

When using CHAP authentication, you must use the same password for both user accounts. In this case, both the Pigeon and Robin router share the password "cisco." It must remain the same on both sides because CHAP never actually sends the password across the wire; it sends only the MD5 hash version of it. When the receiving side gets the hash, it runs the MD5 algorithm on its own password and compares the two hashes. If they match, authentication succeeds. The following is the complete configuration of both the Pigeon and Robin routers to enable CHAP PPP authentication:

```
Pigeon#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Pigeon(config)#username Robin password cisco
Pigeon(config)#interface serial 0
Pigeon(config-if)#encapsulation ppp
Pigeon(config-if)#ppp authentication chap

Robin#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Robin(config)#username Pigeon password cisco
Robin(config)#interface serial 0
Robin(config-if)#encapsulation ppp
Robin(config-if)#ppp authentication chap
```

Compression

Enabling PPP compression is a piece of cake. You just have to make sure that both sides of the connection enable it; if only one side of the connection enables it, the link fails. Using the Pigeon and Robin scenario again, the following shows the steps you can take to enable compression:

```
Pigeon#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Pigeon(config)#interface serial 0
Pigeon(config-if)#compress  ?
  mppc       MPPC compression type
  predictor  predictor compression type
  stac       stac compression algorithm
  <cr>
```

That's it! Just use the `compress` command and type the mode of compression you would like to use, and let the bandwidth savings begin.

Verifying PPP

To ensure your PPP connection came up successfully, you can always use the ol' faithful `show ip interface brief` command.

```
Pigeon#show ip interface brief
Interface            IP-Address      OK? Method Status       Protocol
FastEthernet0        10.1.1.2        YES NVRAM  up           up
Serial0              10.2.2.2        YES manual up           up
```

In this case, all is well with the Serial 0 PPP connection between the routers because the `Protocol` is stated as `up`. Remember, the Status column generally dictates the Physical layer connectivity, whereas the Protocol column focuses on the Data Link connectivity.

If you want to get a little more in depth with the PPP negotiation on the interface, issue the `show interface <interface>` command as follows:

```
Pigeon#show interface serial 0
Serial0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.2.2.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP Open
  Open: IPCP, CCP, CDPCP
  Last input 00:00:51, output 00:00:01, output hang never
  Last clearing of "show interface" counters 05:07:30
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4127 packets input, 168000 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     84 input errors, 0 CRC, 84 frame, 0 overrun, 0 ignored, 0 abort
     8196 packets output, 404090 bytes, 0 underruns
     0 output errors, 0 collisions, 163 interface resets
     0 output buffer failures, 0 output buffers swapped out
     326 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

As you can see from the output above, the router has negotiated Link Control Protocol (LCP) options, which is indicated by the `LCP Open` state. If the LCP negotiations had failed (most

likely because of an authentication problem), the LCP state would rotate between `Listen`, `ACKSent`, or `TERMSent`. This is the Cisco router trying to go through the negotiation of the LCP options. In the line below `LCP Open`, you can verify all the Network layer communication occurring across the PPP link. In this case, you can see IPCP (indicates the TCP/IP protocol), CCP (Indicates compression is in effect—compressed control protocol [CCP]), and CDPCP (indicates the Cisco Discovery Protocol [CDP]). Technically, CDP is a Data Link protocol; however, Cisco adopted it to connect into the PPP options as a Layer 3 protocol.

EXAM ALERT

Be able to interpret the `show interface` command output as it relates to the PPP options.

Finally, if you would like to see how your PPP compression is working out, you can type the command `show compress`. This gives you the compression statistics for the line:

```
Pigeon#show compress
 Serial0
        Software compression enabled
        uncompressed bytes xmt/rcv 4215/4956
        compressed   bytes xmt/rcv 0/0
        1  min avg ratio xmt/rcv 0.223/4.621
        5  min avg ratio xmt/rcv 0.284/4.621
        10 min avg ratio xmt/rcv 0.270/1.372
        no bufs xmt 0 no bufs rcv 0
        resyncs 0
```

In this case, you have no compressed bytes because all the traffic sent over the PPP link was generated by the routers themselves (this traffic is exempt from compression).

Troubleshooting PPP

Whenever you reach the troubleshooting section for any topic, you can be guaranteed some `debug` output. In this case, the `debug` commands for PPP are pretty darn useful: Most of the output is easy to understand. The most useful command that I have found to troubleshoot a PPP link is the `debug ppp negotiation` command. Check out this output:

```
Pigeon#debug ppp negotiation
1d02h: Se0 PPP: Using default call direction
1d02h: Se0 PPP: Treating connection as a dedicated line
1d02h: Se0 PPP: Phase is ESTABLISHING, Active Open [0 sess, 1 load]
1d02h: Se0 LCP: O CONFREQ [Closed] id 157 len 15
1d02h: Se0 LCP:    AuthProto CHAP (0x0305C22305)
1d02h: Se0 LCP:    MagicNumber 0x0709760C (0x05060709760C)
1d02h: Se0 LCP: I CONFREQ [REQsent] id 208 len 15
```

```
1d02h: Se0 LCP:    AuthProto CHAP (0x0305C22305)
1d02h: Se0 LCP:    MagicNumber 0x22D5B7B3 (0x050622D5B7B3)
1d02h: Se0 LCP: O CONFACK [REQsent] id 208 len 15
1d02h: Se0 LCP:    AuthProto CHAP (0x0305C22305)
1d02h: Se0 LCP:    MagicNumber 0x22D5B7B3 (0x050622D5B7B3)
1d02h: Se0 LCP: TIMEout: State ACKsent
1d02h: Se0 LCP: O CONFREQ [ACKsent] id 158 len 15
1d02h: Se0 LCP:    AuthProto CHAP (0x0305C22305)
1d02h: Se0 LCP:    MagicNumber 0x0709760C (0x05060709760C)
1d02h: Se0 LCP: I CONFACK [ACKsent] id 158 len 15
1d02h: Se0 LCP:    AuthProto CHAP (0x0305C22305)
1d02h: Se0 LCP:    MagicNumber 0x0709760C (0x05060709760C)
1d02h: Se0 LCP: State is Open
1d02h: Se0 PPP: Phase is AUTHENTICATING, by both [0 sess, 1 load]
1d02h: Se0 CHAP: O CHALLENGE id 156 len 27 from "Pigeon"
1d02h: Se0 CHAP: I CHALLENGE id 2 len 26 from "Robin"
1d02h: Se0 CHAP: O RESPONSE id 2 len 27 from "Pigeon"
1d02h: Se0 CHAP: I RESPONSE id 156 len 26 from "Robin"
1d02h: Se0 CHAP: O SUCCESS id 156 len 4
1d02h: Se0 CHAP: I SUCCESS id 2 len 4
1d02h: Se0 PPP: Phase is UP [0 sess, 1 load]
1d02h: Se0 IPCP: O CONFREQ [Closed] id 4 len 10
1d02h: Se0 IPCP:    Address 10.2.2.2 (0x03060A020202)
1d02h: Se0 CCP: O CONFREQ [Closed] id 4 len 6
1d02h: Se0 CCP:    Predictor1 (0x0102)
1d02h: Se0 CDPCP: O CONFREQ [Closed] id 4 len 4
1d02h: Se0 IPCP: I CONFREQ [REQsent] id 5 len 10
1d02h: Se0 IPCP:    Address 10.2.2.1 (0x03060A020201)
1d02h: Se0 IPCP: O CONFACK [REQsent] id 5 len 10
1d02h: Se0 IPCP:    Address 10.2.2.1 (0x03060A020201)
1d02h: Se0 CCP: I CONFREQ [REQsent] id 2 len 6
1d02h: Se0 CCP:    Predictor1 (0x0102)
1d02h: Se0 CCP: O CONFACK [REQsent] id 2 len 6
1d02h: Se0 CCP:    Predictor1 (0x0102)
1d02h: Se0 CDPCP: I CONFREQ [REQsent] id 5 len 4
1d02h: Se0 CDPCP: O CONFACK [REQsent] id 5 len 4
1d02h: Se0 IPCP: I CONFACK [ACKsent] id 4 len 10
1d02h: Se0 IPCP:    Address 10.2.2.2 (0x03060A020202)
1d02h: Se0 IPCP: State is Open
1d02h: Se0 CCP: I CONFACK [ACKsent] id 4 len 6
1d02h: Se0 CCP:    Predictor1 (0x0102)
1d02h: Se0 CCP: State is Open
1d02h: Se0 CDPCP: I CONFACK [ACKsent] id 4 len 4
1d02h: Se0 CDPCP: State is Open
1d02h: Se0 IPCP: Install route to 10.2.2.1
1d02h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
➥changed state to up
```

Isn't that some great stuff?!? Okay, it does take a little bit of screening through all the output, but if you look about halfway through, you can see the exchange of the Robin and Pigeon hostnames. This shows the challenge/response action of the CHAP protocol. Thankfully, you can see a `SUCCESS` message to finish it off, showing the Pigeon and Robin routers have successfully authenticated each other. Near the bottom of the output, you see the CCP (compression negotiation) negotiate the Predictor algorithm between the two routers. Finally, at the end of the output, you see the link come up.

If your PPP connection is failing, this `debug` command will definitely show you the cause (as long as the failure is related to PPP). Another popular command is `debug ppp authentication`, which gives the same output, but slims it down to just the authentication information (because this is where many failures occur).

Chapter Summary

Managing WAN connections is one of the primary functions of a router. WAN connections tie distant locations together into a common network infrastructure. Choosing a WAN connection has become more difficult in recent years because there are now many more WAN connection technologies at our disposal. However, the most popular WAN connection technologies boil down to three main categories: Leased Lines, Circuit Switched, and Packet Switched.

After you have chosen the Physical connection type you would like to use, you can then move up to the Data Link connectivity. For leased line and ISDN connections, the two major protocols in use today are HDLC and PPP. On a Cisco router, HDLC has been modified to support multiple upper-layer protocols and has thus become proprietary. HDLC's major feature is the low amount of network overhead it causes on the WAN connection. Other than that, it is featureless. PPP is the more popular data link protocol because it supports multi-vendor interoperability and a plethora of features.

Key Terms

- leased lines
- packet-switched networks
- circuit-switched networks
- broadband
- Virtual Private Networks (VPNs)
- Integrated Services Digital Network (ISDN)
- metro ethernet
- X.25
- Frame Relay
- Asychronous Transfer Mode (ATM)
- High-level Data Link Control (HDLC)
- Point-to-Point Protocol (PPP)
- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- V.35
- X.21
- EIA/TIA-232, -449, and -530
- Link Control Protocol (LCP)
- Network Control Protocol (NCP)
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- stacker compression
- predictor compression
- Microsoft Point-to-Point Compression (MPPC)

Apply Your Knowledge

Exercises

15.1 Troubleshooting PPP Connections

One of the most common problems encountered when troubleshooting a PPP connection is authentication failures, which are due to the many parameters that must match for the link to successfully authenticate. In this exercise, you will incorrectly configure PPP authentication and walk through the steps necessary to troubleshoot the connection. Refer to Figure 15.4 for a visual of the connection.

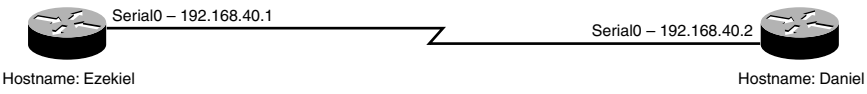


FIGURE 15.4 PPP troubleshooting network diagram.

Estimated Time: 5-10 minutes

What you will do is configure the two routers for CHAP authentication across the PPP connection. However, you will configure the username/password combination on one side of the connection as all lowercase and watch the story unfold. First, get the PPP connection running:

```
Daniel#show ip interface brief
Interface            IP-Address      OK? Method Status       Protocol
FastEthernet0        10.1.1.2        YES NVRAM  up           up
Serial0              192.168.40.2    YES manual up           down
Daniel#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Daniel(config)#interface serial 0
Daniel(config-if)#encapsulation ppp
```

You now have the Daniel rotuer configured for PPP; now configure the Ezekiel router on the other side.

```
Ezekiel#show ip interface brief
Interface   IP-Address      OK? Method Status                Protocol
Ethernet0   192.168.1.40    YES NVRAM  up                    up
Serial0     192.168.40.1    YES manual up                    down
Serial1     unassigned      YES NVRAM  administratively down down
Ezekiel#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ezekiel(config)#interface serial 0
Ezekiel(config-if)#encapsulation ppp
00:07:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
➥ changed state to up
1d14h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
➥ changed state to up
```

```
Ezekiel(config-if)#^Z
1d14h: %SYS-5-CONFIG_I: Configured from console by console
Ezekiel#ping 192.168.40.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/59/72 ms
```

It looks like the PPP link has been brought up successfully and you are now able to ping between the two routers. Now add the authentication piece to the picture:

```
Ezekiel#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ezekiel(config)#username Daniel password examprep
Ezekiel(config)#interface serial 0
Ezekiel(config-if)#ppp authentication chap
00:11:11: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
➥ changed state to down
```

Notice that as soon as you turned on CHAP authentication for one side of the connection, the link went down. This is because one side of the connection is configured to require authentication while the other is not configured to support it. You can solve that problem and, at the same time, introduce the authentication configuration error.

```
Daniel#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Daniel(config-if)#exit
Daniel(config)#username Ezekiel password examcram
Daniel(config)#interface serial 0
Daniel(config-if)#ppp authentication chap
Daniel(config-if)#exit
Daniel(config)#exit
1d14h: %SYS-5-CONFIG_I: Configured from console by console
Daniel#show ip interface brief
Interface            IP-Address      OK? Method Status       Protocol
FastEthernet0        10.1.1.2        YES NVRAM  up           up
Serial0              192.168.40.2    YES manual up           down
```

Notice that the password `examcram` was used for the Ezekiel account rather than `examprep`. Because CHAP requires both passwords to be the same on both sides of the connection, the Serial0 link remains down. Now, if we did not know about this configuration error, the troubleshooting process would go something like this:

```
Daniel#show interface serial 0
Serial0 is up, line protocol is down
  Hardware is PowerQUICC Serial
  Internet address is 192.168.40.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP Listen
  Closed: IPCP, CCP, CDPCP
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters 16:52:28
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
<…output removed for brevity...>
```

Notice first that the line protocol is down, which indicates a Data Link failure. When you look down at the PPP negotiation (LCP), you can see that it is in the `Listen` state and the NCP protocol communication is `Closed`. This means the LCP layer of PPP has not successfully negotiated, and points you in the correct direction for troubleshooting. Now is a good time to perform a `debug` and see whether you can weed out what is going on.

```
Daniel#debug ppp negotiation
PPP protocol negotiation debugging is on
Daniel#
1d14h: Se0 LCP: TIMEout: State Listen
1d14h: Se0 LCP: O CONFREQ [Listen] id 51 len 15
1d14h: Se0 LCP:    AuthProto CHAP (0x0305C22305)
1d14h: Se0 LCP:    MagicNumber 0x098EF573 (0x0506098EF573)
1d14h: Se0 LCP: I CONFACK [REQsent] id 51 len 15
1d14h: Se0 LCP:    AuthProto CHAP (0x0305C22305)
1d14h: Se0 LCP:    MagicNumber 0x098EF573 (0x0506098EF573)
1d14h: Se0 LCP: I CONFREQ [ACKrcvd] id 131 len 15
1d14h: Se0 LCP:    AuthProto CHAP (0x0305C22305)
1d14h: Se0 LCP:    MagicNumber 0x002934B3 (0x0506002934B3)
1d14h: Se0 LCP: O CONFACK [ACKrcvd] id 131 len 15
1d14h: Se0 LCP:    AuthProto CHAP (0x0305C22305)
1d14h: Se0 LCP:    MagicNumber 0x002934B3 (0x0506002934B3)
Daniel#
1d14h: Se0 LCP: State is Open
1d14h: Se0 PPP: Phase is AUTHENTICATING, by both [0 sess, 1 load]
1d14h: Se0 CHAP: O CHALLENGE id 144 len 27 from "Daniel"
1d14h: Se0 CHAP: I CHALLENGE id 45 len 28 from "Ezekiel"
1d14h: Se0 CHAP: O RESPONSE id 45 len 27 from "Daniel"
1d14h: Se0 CHAP: I RESPONSE id 144 len 28 from "Ezekiel"
1d14h: Se0 CHAP: O FAILURE id 144 len 25 msg is "MD/DES compare failed"
1d14h: Se0 PPP: Phase is TERMINATING [0 sess, 1 load]
1d14h: Se0 LCP: O TERMREQ [Open] id 52 len 4
1d14h: Se0 CHAP: LCP not open, discarding packet
1d14h: Se0 LCP: I TERMREQ [TERMsent] id 132 len 4
1d14h: Se0 LCP: O TERMACK [TERMsent] id 132 len 4
Daniel#
```

```
1d14h: Se0 LCP: TIMEout: State TERMsent
1d14h: Se0 LCP: O TERMREQ [TERMsent] id 53 len 4
1d14h: Se0 LCP: I TERMACK [TERMsent] id 53 len 4
1d14h: Se0 LCP: State is Closed
1d14h: Se0 PPP: Phase is DOWN [0 sess, 1 load]
1d14h: Se0 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 1 load]
```

You can watch in amazement as PPP goes from the `Listen` state into the `REQ/ACK` state (where it begins to negotiate the connection and authentication protocol). After the LCP state is `Open`, the full authentication phase begins. About halfway through the `CHALLENGE/RESPONSE` messages, you see the glaring `FAILURE` message that shows that the `MD/DES` compare failed. This means the password hashes are not the same for these routers. If you kept this debug turned on, it would continue to loop through the process again and again until you fixed the mismatched password. Turn off the `debug` and fix the password, and see what happens.

```
Daniel#u all
All possible debugging has been turned off
Daniel#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Daniel(config)#no username Ezekiel password examcram
Daniel(config)#username Ezekiel password examprep
Daniel(config)#
00:40:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
➥ changed state to up
1d14h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
➥ changed state to up
```

Wow! Just like that, the link has come online. The configuration is now successful.

Review Questions

1. List the three categories of WAN connections.
2. You are installing a new serial WAN connection into your offices in Tucson, Arizona. The service has already terminated their end of the connection at the premises and provided you with a CSU/DSU device. What physical connections should you use on your Cisco router?
3. What four features are negotiated by PPP's LCP?
4. What is the function of PPP's Network Control Protocol?
5. PPP has the capability to use two different compression algorithms. What are they? What is the effect of these algorithms on your router? Why would you choose to use one algorithm over the other?

Exam Questions

1. Which of the following network types would encompass Frame Relay and X.25?

   - ❍ **A.** Leased lines
   - ❍ **B.** Circuit-switched networks
   - ❍ **C.** Packet-switched networks
   - ❍ **D.** Broadband

2. What type of serial transition cable should you use to connect your Cisco router to a CSU/DSU device that has a V.35 female connector?

   - ❍ **A.** V.35 male on the Cisco side to V.35 male on the CSU/DSU
   - ❍ **B.** DB-60 male on the Cisco side to V.35 male on the CSU/DSU
   - ❍ **C.** DB-60 male on the Cisco side to V.35 female on the CSU/DSU
   - ❍ **D.** V.35 male on the Cisco side to V.35 female on the CSU/DSU

3. What type of packet is used during the initial PPP link establishment process?

   - ❍ **A.** Authentication
   - ❍ **B.** LCP
   - ❍ **C.** NCP
   - ❍ **D.** HDLC

4. Which of the following describes the Password Authentication Protocol (PAP) used by PPP during the LCP process? (Choose 2.)

   - ❍ **A.** PAP exchanges passwords in clear text.
   - ❍ **B.** PAP uses a MD5 hashing function to send password information.
   - ❍ **C.** PAP enables the server to be in control of the authentication attempt.
   - ❍ **D.** PAP enables the client to be in control of the authentication attempt.

5. When is CHAP authentication performed?

   - ❍ **A.** On a certain time interval
   - ❍ **B.** When the user decides to send the username/password
   - ❍ **C.** When the link connection is established
   - ❍ **D.** When the link connection is established and on a periodic interval

6. What Cisco IOS configuration mode should you be in to enable PPP authentication?

   - ❍ **A.** Global configuration mode
   - ❍ **B.** Router configuration mode
   - ❍ **C.** Interface configuration mode
   - ❍ **D.** PPP LCP configuration mode

7. What type of WAN connection enables the company to purchase a simple Internet connection and tunnel their information through the network between their sites?

   - ❍ **A.** Leased-lines
   - ❍ **B.** Circuit-switched
   - ❍ **C.** Packet-switched
   - ❍ **D.** Virtual private network

8. What verification command can show you the current state of the PPP Link Control Protocol?

   - ❍ **A.** `show interface`
   - ❍ **B.** `show ip interface`
   - ❍ **C.** `show ppp interface`
   - ❍ **D.** `show wan interface`

9. Which of the following PPP sub-layers is responsible for Network layer protocol negotiation?

   - ❍ **A.** HDLC
   - ❍ **B.** CDP
   - ❍ **C.** LCP
   - ❍ **D.** NCP

10. Which of the following WAN connection categories would include dial-up modems and ISDN BRI connections?

    - ❍ **A.** Leased lines
    - ❍ **B.** Circuit-switched
    - ❍ **C.** Packet-switched
    - ❍ **D.** Metro ethernet

Answers to Review Questions

1. The three WAN connection categories are leased line, circuit switched, and packet switched.
2. When configuring the physical connectivity for a serial WAN connection, you need to purchase either a DB-60 or Smart Serial WIC card for your router. From there, you need to purchase a cable that converts from the DB-60 or Smart Serial card of your Cisco router to the industry standard adapter found on the CSU/DSU device that connects to the service provider.
3. The four features negotiated by the PPP Link Control Protocol (LCP) are compression, callback, multilink, and authentication.
4. The Network Control Protocol (NCP) enables the router to encapsulate multiple upper-layer protocols (such as IP, IPX, and Appletalk) over a PPP WAN connection.
5. The two PPP compression algorithms are Stacker and Predictor. The Stacker algorithm requires more processor resources and fewer memory resources. The Predictor algorithm uses more memory resources and fewer processor resources. Stacker is the best algorithm to use when there are varying traffic types crossing the PPP WAN connection. Predictor works best when you have similar traffic types using the PPP WAN connection.

Answers to Exam Questions

1. **C.** Frame Relay and X.25 fall under the packet-switched networks category. These networks establish connections through a service provider cloud using virtual circuits. Answer B is incorrect because circuit-switched networks include technologies such as modems and ISDN. Answer A is incorrect because leased lines use dedicated bandwidth between locations. Answer D is incorrect because broadband encompasses DSL and cable modem technology.
2. **B.** The Cisco side of the connection always uses either a DB-60 or Smart Serial connector (these are always male because the router has female ports). Because the CSU/DSU has a V.35 female connector, you should be using a V.35 male transition cable. All other answers are incorrect because they use either the wrong connector type or gender on the Cisco side.
3. **B.** The Link Control Protocol (LCP) is used to negotiate all options related to PPP during the link establishment phase. The Network Control Protocol (NCP) negotiates the upper-layer protocols only after the initial PPP link has been established. The HDLC layer of PPP is what allows for multi-vendor interoperability with the protocol. Answer A is incorrect because an authentication packet falls under the LCP negotiations. Answer C is incorrect because NCP negotiates the upper-layer protocols. Answer D is incorrect because HDLC is used to give PPP an industry standard foundation when connecting to non-Cisco equipment.
4. **A, D.** PAP is the older of the two PPP authentication protocols. It has major security flaws, including the sending of passwords in clear text and allowing the client to choose when it sends the password. Answers B and C are incorrect because the MD5 hashing and server control is a function of the CHAP.

5. **D.** CHAP requires authentication both when the link is initially established and on a periodic basis thereafter. This is awesome because it combats playback attacks and packet sniffing (passwords are not sent). PAP requires authentication only when the link is initially established and when the client chooses to send the credentials, which is why answers B and C are incorrect. Answer A is incorrect because CHAP also sends authentication credentials when the link is initially established.

6. **C.** You enable PPP authentication from the interface configuration mode by typing the command `ppp authentication <chap/pap>`. All other answers are either irrelevant or non-existent (there is no PPP LCP configuration mode in the Cisco IOS).

7. **D.** VPNs enable companies to purchase simple Internet connections and tunnel their information through the networks between their sites. This information is heavily encrypted to ensure it is not compromised crossing the public network. This is far cheaper than any other type of WAN connection, but can suffer from the heavy encryption slowdown. Answers A, B, and C are incorrect because leased lines and circuit-switched and packet-switched networks require no tunneling or encryption capabilities.

8. **A.** The `show interface` command is used to verify the current state of the PPP LCP negotiations. This shows `Open`, `Listen`, `ACKSent`, or `TERMSent`, depending on the state of LCP at the time (you want LCP to show `Open`). The other `show` commands are either irrelevant or would produce invalid syntax.

9. **D.** NCP is used to negotiate the Network layer protocols. These negotiations are typically shown as in the syntax *<negotiated protocol>*`CP` in **`show interface`** output, such as IPCP (for the IP protocol), CDPCP (for the CDP protocol), or IPXCP (for the IPX protocol). Answer A is incorrect because HDLC is used at a lower layer of PPP to provide multi-vendor interoperability, and answer C is incorrect because LCP is used to negotiate PPP features. Answer B is incorrect because CDP has nothing to do with WAN links.

10. **B.** Circuit-switched connections encompass anything that has to dial a number to make a connection. These connections typically use the telephone company as a backbone. Answer C is incorrect as packet-switched networks include technologies such as X.25 and Frame Relay. Answer A is incorrect because leased lines do not dial because they are permanently established connections. Answer D is incorrect because metro ethernet is extremely high-speed connections running through a metropolitan area.

Suggested Reading and Resources

1. Cisco Introduction to WAN Technologies, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introwan.htm.

2. Ward, Chris and Cioara, Jeremy. *Exam Cram 2 CCNA Practice Questions*. Que Publishing, 2004.

3. Quinn, Eric and Glauser, Fred. *BCRAN Exam Cram 2 (Exam 642-821)*. Que Publishing, 2003.

16

CHAPTER SIXTEEN

ISDN

Objectives

Describe the building blocks of ISDN connections

Understand the physical layout and reference points of an ISDN network

Configure ISDN connections on Cisco routers

Implement dial-on-demand routing (DDR) and Dialer Profiles for ISDN connections

Verify ISDN operation

- Unlike technologies such as DSL or Frame Relay, ISDN loosely describes a type of connection that comprises a group of channels. These channels (called B-channels and D-channels) are used to transmit data and signaling between locations. This chapter discusses the difference between the channels and how they are bundled together to form a single ISDN connection.
- When describing an ISDN connection, you can use a number of devices and reference points to pinpoint areas of the network for implementation and troubleshooting. Cisco also expects you to know these areas for the certification purposes.
- Configuring the basic ISDN connection is fairly simple. This is the first area of discussion in the chapter.
- After you understand the basics of configuring ISDN, more flexibility is added through DDR and Dialer Profiles. These features enable you to save costs by disconnecting the ISDN line when not in use and connect to different locations which may require drastic changes to the interface configuration through Dialer Profiles.
- An ISDN configuration can malfunction in many different ways. This chapter will introduce a logical troubleshooting approach for each area of the ISDN connection.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- Pay special attention to the ISDN physical layout and reference points. Be sure to understand the conceptual view of the network.
- Most of the ISDN configuration will be reserved for the CCNP BCRAN exam; however, be sure to focus on the base configuration and verification commands for ISDN.

Introduction

If we were talking about the Integrated Services Digital Network (ISDN) a decade ago, this chapter would have started out something like this, "Are you ready for the technology that will blow your socks off? Do you have a need for speed? Would you like to be the envy of all other network administrators? Well let me tell you about ISDN…" Unfortunately, it is not a decade ago, so you'll just have to settle for, "This is the ISDN chapter."

As its name implies, ISDN was originally designed to *integrate* multiple services (voice and data) through a single medium. Rather than purchase voice and data service as separate bundles, a network could purchase a single connection through the same local carrier that provided both services through a single line. Because ISDN connections use the same cable as the local telephone company, it is still considered today as one of the most reliable connections available. Even though ISDN uses the telephone company as a backbone, it offers improved communication by using end-to-end digital signaling. When you normally are speaking on the telephone, you are using analog signals, which travel to the phone company and are converted into a digital format. Although this works fine for voice, it can impede the quality of data communications because analog signals are more susceptible to interference and loss. ISDN brings the digital signal all the way down to the end-user, which results in a cleaner, higher-quality signal.

So why do I start by saying, "This is the ISDN chapter" rather than my typical overly excited self? Because ISDN is ever so slowly making an exit from mainstream networking. ISDN services have been largely displaced by broadband Internet services, such as DSL, cable modem, and satellite services. The most popular flavor of ISDN (BRI) is now becoming very difficult to find in the United States. So why are we learning about it? For two primary reasons: First, ISDN is still quite popular overseas. Second, ISDN makes a fantastic backup connection. Third, because Cisco still asks ISDN questions on the CCNA exam.

EXAM ALERT

ISDN is slowly making an exit from mainstream Cisco exams. Cisco has already pulled ISDN from their flagship CCIE Routing and Switching certification exam. You can expect to be tested rather lightly on ISDN, if at all.

I hope you are still reading and have not flipped to some other chapter after that last test tip. The concepts used in ISDN are useful for many other network technologies.

The Flavors of ISDN

ISDN connections come in two primary flavors: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). To understand the difference between these two, you first need to understand the building blocks of ISDN connections.

ISDN connections are built with a combination of B-channels (bearer) and a D-channel (delta). Each B-channel gives the equivalent of 64Kbps of bandwidth that can be used to send or receive data. The D-channel is used for signaling. It can be 16Kbps or 64Kbps, depending on the flavor of ISDN you choose to implement. The signaling channel keeps multiple B-channels in line by transmitting all the control information related to those channels. The D-channel is not used to send your network traffic between your locations, but rather, controls the channels that send the network traffic. By combining multiple B-channels together along with a single D-channel, you build your ISDN connection.

In addition, the D-channel is always connected to the service provider. Because ISDN is a circuit-switched connection, it is considered a dial-on-demand technology. When you need the connection, you dial a phone number to have it connect. When you're finished with the connection, the line is hung up. If you have ever heard a modem dial, you'll realize that it is not a fast process. For a modem connection to dial, connect, and begin sending data, it could take anywhere from 30–60 seconds. In our high-speed network world, this type of delay is unacceptable. When using ISDN connections, the dialing process can take less than a second because the D-channel is the one doing the dialing and this channel is always connected to the service provider.

EXAM ALERT

Know the difference between B-channels and the D-channel.

BRI Connections

ISDN BRI connections comprise two 64Kbps B-channels and one 16Kbps D-channel. This gives the connection 128Kbps total bandwidth that can be used for data traffic. BRI connections used to be quite popular for backup connections in the United States, but have slowly been replaced by cheaper DSL and cable modem connections combined with VPN technology. Outside the United States, ISDN BRI connections are still quite prevalent.

Because they fall in the circuit-switched category, ISDN BRI connections typically use dial-on-demand technology. Because these connections are billed on a per-minute basis, keeping them continually connected usually is not an option. When the connection is needed, the router automatically dials through to the destination. When the connection has not been used for a certain amount of time, the link is broken. Because routers are constantly chatty devices

(sending routing updates, keepalives, and other miscellaneous messages), they can tend to keep the line continuously active without using your configuration expertise to prevent these traffic types from crossing the ISDN connection. Later in this chapter, you will learn how to properly and efficiently implement ISDN.

PRI Connections

ISDN PRI connections are composed of 23 64Kbps B-channels and a single 64Kbps D-channel. This is the ISDN equivalent of a T1 line. This brings me to a pretty big point: Don't get lost in the "T1 line" concept. Many people think that a T1 line is a type of WAN connection. "I'll have a T1 line with the red sauce on the side," is the feeling I get when hearing how most people describe a T1 connection. Saying something like that would be like walking into a seafood restaurant and saying, "I'll take a fish." To which the waiter would promptly respond, "What sort of fish?" T1 is just a measure of bandwidth, 1.544Mbps to be exact. The technology that gets it to you is another story. You could purchase a T1 Frame Relay connection or a T1 CAS connection. In this chapter, I am talking about a T1 ISDN connection. Depending on your location, an ISDN T1 connection may be the only type of T1 you'll be able to get. ISDN is one of the most widespread technologies available.

ISDN PRI connections give you slightly less bandwidth than other T1 technologies because of the signaling channel. Most other T1 connections use Channel Associated Signaling (CAS), which enables you to combine your signaling along with the data you are sending. This is slightly more efficient than the Common Channel Signaling (CCS) method ISDN uses. If you need additional bandwidth (beyond what a single ISDN PRI connection gives you), you can add more PRI lines to your bundle (remember, ISDN PRI are just a bunch of B-channels) and still use only a single 64Kbps D-channel for signaling.

EXAM ALERT

Know the number of B-channels and D-channels in BRI and PRI connections. To review:

Basic Rate Interface (BRI): 1 D-channel, 2 B-channels

Primary Rate Interface (PRI): 1 D-channel, 23 B-channels

It is also worth mentioning that in Europe, PRI lines are given 30 B-channels (this is known as an E1 speed).

ISDN Signaling Protocols

The initial WAN chapter (Chapter 15, "Wide Area Networks") discussed two major technologies: HDLC and PPP. These are both Data Link layer (Layer 2) communications that must match on both sides of the connection. ISDN does not use either HDLC or PPP. It uses two protocols known as Q.921 and Q.931. The creator of these ISDN standards was very kind

because he tells you at what layer the protocol works right in the name: Q.921 works at Layer 2 (Data Link) and Q.931 works at Layer 3 (Network). It is very odd to have a WAN protocol that works above Layer 2, which is where Q.931 operates. The following sections discuss the function of both of these protocols.

ISDN Reference Points and Equipment

Before you get into the configuration of ISDN interfaces, you need to understand the architecture of how ISDN connections connect into the office. Anytime you talk about ISDN, you'll see the diagram in Figure 16.1 pop up somewhere.

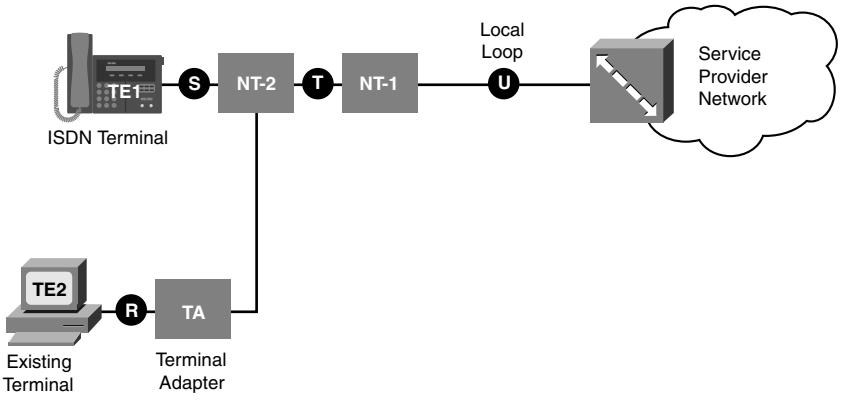


FIGURE 16.1 ISDN equipment and reference points.

When looking at this diagram, you can either get really deep into architecture, standards, and all other sorts of mish-mash. However, I prefer to keep things practical because this model can be quite useful if applied in that way. So here's how things work:

Imagine that you need an ISDN connection for your company. You call up an ISDN service provider, who is usually the telephone service provider in your area. They tell you ISDN service is available and then quote you some insanely priced installation charges. Reluctantly, you agree. The ISDN service technician arrives at your location and runs a new tap from the *local loop* to your property. The local loop is just the underground (or above-ground) line that all people tap into in your area to get telephone service. The line is then run to your business premises and neatly cabled into a wall jack in the room of your choice. If you take a look back at Figure 16.1, we are currently talking about the line labeled **U**. That wall jack is most likely the service provider's *demarcation* point. If anything breaks on your side of the wall jack, you'll be paying for repairs. If anything breaks on the service provider's side of the wall jack, you'll probably also pay for the repairs because the service provider will think of some way to make you believe that the problem on their side of the wall jack was caused by something on your side of the wall jack. But that's another part of the story.

So you're sitting in your chair, looking at the new ISDN wall jack. You decide to take some action and plug an RJ-45 ethernet cable into the wall jack and run it to a new ISDN interface you just installed in your Cisco router. The *type* of ISDN interface you install can be different based on where you are in the world. If you are in the United States, you are expected to supply your own *Network Termination, Type 1 (NT-1)*. This little device takes the two-wire ISDN line that comes in from the service provider and converts it to a four-wire connection that your internal equipment can use. Thankfully, Cisco has produced *ISDN U Interfaces* for your router that includes an integrated NT-1. The alternative interface you can purchase is an *ISDN S/T Interface*, which does *not* have an integrated NT-1 component. You would use this type of interface if you either purchased a standalone NT-1 device (a company called AdTran makes the most popular NT-1), or you live in Europe, where the service provider provides the NT-1 for you (those lucky dogs).

For sake of this example, imagine that you purchased a standalone NT-1 device and an S/T interface for your router. Now, this is where you have some flexibility in choosing to connect your ISDN line to one of three different device types. You can plug it directly into your router's ISDN S/T interface and, after some configuration, the router happily begins routing for the ISDN line. At that point, your router is filling the role of a *Terminal Endpoint, Type 1 (TE1)*, which is considered an ISDN-compatible terminal that is capable of handling a raw ISDN signal. By the way, the S/T interface is called an "S/T" interface because it represents the *S* and *T* reference points in the diagram in Figure 16.1. You could also choose to connect the cable from the NT-1 box to a *Network Termination, Type 2 (NT-2)* device. This is just an ISDN PBX, or to put it more in network terms, it's like a hub for ISDN connections. It enables you to take your ISDN line and split it off to multiple devices. An NT-2 can even take multiple incoming ISDN lines and aggregate them together into a higher-bandwidth connection. You don't have to have an NT-2 device (most people don't); it is just an option you can use. The third type of device that you can connect to the cable coming from the NT-1 is a PC. Or it can be a server. Or it can even be a Microsoft Xbox or Sony Playstation 2. These are all considered *Terminal Endpoint, Type 2 (TE2)* in the network diagram. These devices cannot understand a raw ISDN signal, so you need to squeeze a *Terminal Adapter (TA)* in between the NT-1 cable and the TE2 device. The TA is responsible for taking non-ISDN interfaces and signaling and converting them to something ISDN can understand.

So, let's summarize all these different pieces of the ISDN network:

- **Network Termination, Type 1 (NT-1)**—Converts from the two-wire ISDN line the service provider installs in your location to a four-wire connection that your internal devices can use.
- **Network Termination, Type 2 (NT-2)**—This optional device enables you to either split the ISDN signal or aggregate multiple ISDN connections into a single stream.
- **Terminal Endpoint, Type 1 (TE1)**—This is an ISDN-compatible endpoint, such as a router with an ISDN S/T or U interface.

- **Terminal Endpoint, Type 2 (TE2)**—This is an non-ISDN compatible endpoint, such as a router with no ISDN interfaces or an end-user PC, requiring a Terminal Adapter (TA) to understand the ISDN signal, such as a router with no ISDN interfaces or an end-user PC.
- **Terminal Adapter (TA)**—This device converts an ISDN signal into some other type of signaling.

EXAM ALERT

These ISDN components may be lightly tested during the CCNA exam. They are heavily tested in the Building Cisco Remote Access Networks (BCRAN) CCNP exam.

Configuring BRI Interfaces

It can be difficult to talk about the configuration of ISDN in one "Configuring BRI Interfaces" section. There are so many technologies that come together to make ISDN function, you can start to get lost and ask the question, "Is this really part of ISDN, or some other feature enhancement?" For example, getting the ISDN link between you and your service provider to activate is a piece of cake: Type in two commands and you're good to go. However, for your router to know what networks are on the other side of the connection, you need to set up static routes, which deal with IP routing. To use the static routes, you need to set up a dialer-map to dictate what phone number to dial to reach the networks on the other side, which deals with Dial-on-Demand routing. So, configuring ISDN itself is simple; it's configuring all the other pieces around it that can add the complexity. I'll start here with the simple stuff, and add the additional pieces as we go. To set the stage, imagine you've purchased an ISDN card and plugged it into your router. After you have installed an ISDN BRI interface into your router, it shows up as three different interfaces:

```
Lance#show ip interface brief
Interface         IP-Address      OK? Method Status                Protocol
BRI0              unassigned      YES unset  administratively down down
BRI0:1            unassigned      YES unset  administratively down down
BRI0:2            unassigned      YES unset  administratively down down
Ethernet0         unassigned      YES unset  administratively down down
Serial0           unassigned      YES unset  administratively down down
Serial1           unassigned      YES unset  administratively down down
Serial2           unassigned      YES unset  administratively down down
Serial3           unassigned      YES unset  administratively down down
```

Each interface represents a single channel of the connection. Remember BRI = two B channels, and a single D channel is used for signaling. In this case, the BRI0 interface represents the D channel; the entire logical configuration, such as IP address, encapsulation, and so on,

is applied to this interface. The two other interfaces, BRI0:1 and BRI0:2, represent the two B channels. These act like well-trained dogs: When the D channel tells them to sit, they sit. When told to connect to another router, they connect to another router. They just take orders from the signaling channel that you configure.

ISDN Switch Type

The first step in configuring the ISDN interface is to configure the ISDN switch type on your router. Take a look:

```
Lance#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Lance(config)#isdn switch-type ?
  basic-1tr6    1TR6 switch type for Germany
  basic-5ess    AT&T 5ESS switch type for the U.S.
  basic-dms100  Northern DMS-100 switch type
  basic-net3    NET3 switch type for UK and Europe
  basic-ni      National ISDN switch type
  basic-ts013   TS013 switch type for Australia
  ntt           NTT switch type for Japan
  vn3           VN3 and VN4 switch types for France
  <cr>
```

Which of these ISDN switch types should you choose? Whatever your service provider tells you to choose. These are all the different ISDN service provider switches that are in mainline use in the world today. Your switch type depends heavily on your location and the service provider you use. Don't think of these switch types in terms of better or worse; they all perform the same role. Just think of them as competing standards.

You may have noticed that this is a Global Configuration command. After you configure a switch type, all ISDN interfaces installed into this router use this single switch type. In an extraordinarily rare circumstance, you may have a single router connected to two different ISDN service providers that use different ISDN switch types. In this case, this command would be applied under the BRI configuration mode. Any ISDN switch type settings you set up under the interface overrule the ISDN switch type settings in Global Configuration mode.

SPIDs

After you have configured the ISDN switch type, the ISDN-specific settings are nearly complete. All you need to do is find out whether your service provider requires you to provide Service Provider IDentifiers (SPIDs) for the connection. A SPID is a number that you provide the service provider when you dial up your connection to identify yourself. You could consider it your User ID for the connection. Although it does provide some security for the service

provider, they primarily use the SPID number(s) for billing purposes because ISDN connections are billed on a per-minute basis. If your service provider uses SPIDs, you dial up the connection, provide your SPID number(s) and the billing begins.

To configure SPIDs on your router, you need to access the BRI configuration mode. Take a look:

```
ISDN_Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ISDN_Router(config)#interface BRI 0
ISDN_Router(config-if)#isdn ?
  all-incoming-calls-v120  Answer all incoming calls as V.120
  answer1                  Specify Called Party number and subaddress
  answer2                  Specify Called Party number and subaddress
  caller                   Specify incoming telephone number to be verified
  calling-number           Specify Calling Number included for outgoing
  fast-rollover-delay      Delay between fastrollover dials
  incoming-voice           Specify options for incoming calls.
  not-end-to-end           Specify speed when calls received are not isdn
  outgoing-voice           Specify information transfer capability
  send-alerting            Specify if Alerting message to be sent out before
                           Connect message
  sending-complete         Specify if Sending Complete included in outgoing
                           SETUP message
  spid1                    Specify Service Profile IDentifier
  spid2                    Specify Service Profile IDentifier
  static-tei               Specify a Static TEI for ISDN BRI
  switch-type              Select the Interface ISDN switch type
  tei-negotiation          Set when ISDN TEI negotiation should occur
  timeout-signaling        Flush D channel if a signaling packet can't be
                           transmitted in 1 second
  twait-disable            Delay National ISDN BRI switchtype
  x25                      Configure x25 over the D channel

ISDN_Router(config-if)#isdn spid1 ?
  WORD  spid1 string
ISDN_Router(config-if)#isdn spid1 115529
ISDN_Router(config-if)#isdn spid2 115530
```

As you can see, we have two different SPID numbers (spid1 and spid2). Depending on your service provider, you might have no SPIDs, one SPID, or two SPIDs. They'll give you the information; you just type it into your router.

After you have added your SPID information, you have enough configurations to bring up the D-channel of the ISDN connection with the service provider.

ISDN BRI Practical Example

Now take a look at a full example of what you've seen so far, adding a few other components to the picture that you've seen in prior chapters. For now, there is just a single router named Buttercup connected to a service provider that has been set up for ISDN. The service provider has an ISDN switch type of basic-5ess and requires a single SPID of 5550112.

```
Buttercup#show ip interface brief
Interface         IP-Address      OK? Method Status                Protocol
BRI0              unassigned      YES unset  administratively down down
BRI0:1            unassigned      YES unset  administratively down down
BRI0:2            unassigned      YES unset  administratively down down
Ethernet0         unassigned      YES unset  administratively down down
Serial0           unassigned      YES unset  administratively down down
Serial1           unassigned      YES unset  administratively down down
Serial2           unassigned      YES unset  administratively down down
Serial3           unassigned      YES unset  administratively down down
Buttercup#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Buttercup(config)#interface bri 0
Buttercup(config-if)#ip address 10.1.1.1 255.255.255.0
Buttercup(config-if)#encapsulation ppp
Buttercup(config-if)#isdn switch-type basic-5ess
Buttercup(config-if)#isdn spid1 5550112
Buttercup(config-if)#no shutdown
Buttercup(config-if)#
00:18:51:  isdn_Call_disconnect()

00:18:51: %LINK-3-UPDOWN: Interface BRI0:1, changed state to down
00:18:51:  isdn_Call_disconnect()

00:18:51: %LINK-3-UPDOWN: Interface BRI0:2, changed state to down
00:18:51: %LINK-3-UPDOWN: Interface BRI0, changed state to up
Buttercup(config-if)#
00:18:51: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0, TEI 66 changed to up
Buttercup(config-if)#^Z
Buttercup#
00:19:29: %SYS-5-CONFIG_I: Configured from console by console
Buttercup#show isdn status
Global ISDN Switchtype = basic-5ess
ISDN BRI0 interface
        dsl 0, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 66, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
```

```
Activated dsl 0 CCBs = 0
The Free Channel Mask:  0x80000003
Total Allocated ISDN CCBs = 0
```

Take a look at the bolded portions. As soon as the configuration was entered and `no shudown` command was used to bring up the interface, both BRI0:1 and BRI0:2 went down. The B-channels are not necessary until you need to transfer data to the other end of the connection. On the other hand, BRI0, which represents the D-channel, powered up. The key message that you can see is the `%ISDN-6-LAYER2UP: Layer 2 for Interface BR0, TEI 66 changed to up`. This indicates that you have begun communicating with the service provider. The `TEI` stands for *Terminal Endpoint Identifier*. It's the Layer 2 addressing that the ISDN connections use (very similar to the MAC address of ethernet and the DLCI number of Frame Relay). Your TEI address is dynamically assigned to you when you connect to the service provider.

One of the most useful verification commands is `show isdn status`. This key command enables you to see all three layers of the ISDN connection. Layer 1 (Physical) is shown as active. Layer 2 (Data Link) shows the TEI address and the fact that you've sent/received multiple frames from the service provider. Layer 3 (Network) will not go active until you complete an end-to-end call with another ISDN router.

Configuring PRI Interfaces

Although the number of BRI connections is quickly diminishing in the United States, PRI connections are still quite popular. This is the ISDN equivalent of a T1 line. The configuration of PRI is very similar, but has a slight twist. Cisco decided to release a "combo T1 interface," that is, an interface that is capable of handling a T1 CAS connection (non-ISDN) or a T1 CCS connection (ISDN). This is pretty stellar for you because you get one interface that can handle two totally different connection types. However, when you install the interface, it needs to be configured for one or the other (CAS or CCS). Let me get into the configuration and I'll explain as I go:

```
Snuggles#show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
FastEthernet0/0    192.168.100.10  YES NVRAM  up                    up
FastEthernet0/1    unassigned      YES NVRAM  administratively down down
```

At an initial glance, it seems the router does not have an ISDN interface, or at least not one that shows up in the interface list. This is because Cisco calls T1 interfaces "controllers." Take a look:

```
Snuggles#show controllers t1
T1 0/1/0 is down.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
```

```
  Transmitter is sending remote alarm.
  Receiver has loss of signal.
  alarm-trigger is not set
  Version info Firmware: 20041023, FPGA: 16, spm_count = 0
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  CRC Threshold is 320. Reported from firmware  is 320.
  Data in current interval (548 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 548 Unavail
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 86400 Unavail
```

You can see that this router is equipped with a T1 controller in slot 0/1/0 that is currently down. Now it's time to get started with the PRI configuration.

ISDN Switch Type

The first move is the same as it was before. You need to configure the ISDN switch type on the router to indicate what type of ISDN switch the service provider is using.

```
Snuggles#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Snuggles(config)#isdn switch-type ?
  primary-4ess    Lucent 4ESS switch type for the U.S.
  primary-5ess    Lucent 5ESS switch type for the U.S.
  primary-dms100  Northern Telecom DMS-100 switch type for the U.S.
  primary-dpnss   DPNSS switch type for Europe
  primary-net5    NET5 switch type for UK, Europe, Asia and Australia
  primary-ni      National ISDN Switch type for the U.S.
  primary-ntt     NTT switch type for Japan
  primary-qsig    QSIG switch type
  primary-ts014   TS014 switch type for Australia (obsolete)
Snuggles(config)#isdn switch-type primary-5ess
```

Notice that all the switch types begin with `primary` instead of the `basic` BRI switch types. In this case, the service provider is using the `primary-5ess` switch type.

PRI Groups

Now that you've told the router the service provider switch type, you need to allocate your ISDN channels. This is a pretty interesting process that requires you to understand a little background.

When you purchase a PRI line from the service provider, it can be used for data transmissions from site to site or for your PBX system. The PBX system provides telephone service to your entire internal phone network and requires outside lines to the PSTN. This was the beauty of ISDN: The same connection got you data service for your network and Public Switched Telephone Network (PSTN) service for your Private Branch Exchange (PBX). All that you needed was a multiplexer (a device used to combine or split multiple channels into single or multiple streams) to take the incoming B-channels and splice them up in the two directions. Figure 16.2 gives a visual representation of this concept.

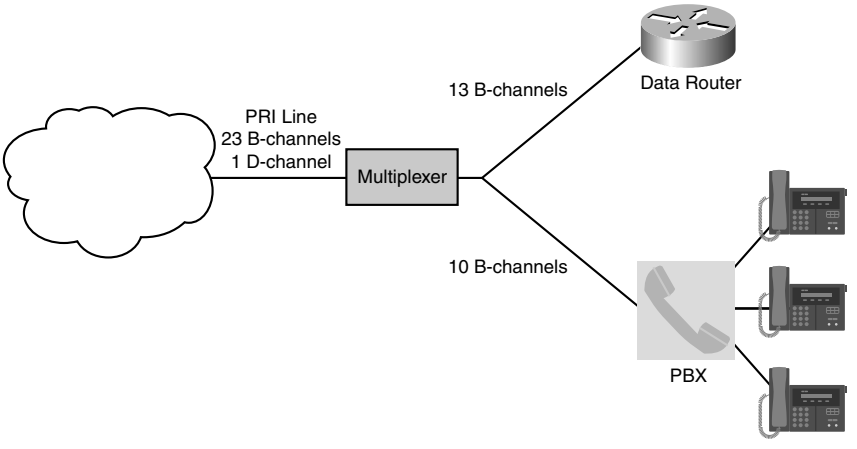


FIGURE 16.2 Using a multiplexer to manage incoming PRI lines.

As you can see, the PRI line comes in from the service provider. The multiplexer (you could also call this a de-multiplexer because it splits the channels up) takes these channels and divides them. 13 of the B-channels go to the data side, giving it 832Kbps (64Kbps per B-channel×13) and 10 of the B-channels go to the PBX system, allowing 10 concurrent PSTN calls (each PSTN call consumes a single B-channel). You can divide these B-channels up however you'd like, but you need to tell the router which B-channels it is able to use. Because of the flexibility of splicing up B-channels, service providers are able to sell fractional T1 lines at lower rates that have fewer B-channels than a full PRI line.

With this in mind, here's how you configure the router so it knows what B-channels it can use. For this example, the router consumes the full PRI line (all 23 B-channels and the D-channel).

```
Snuggles#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Snuggles(config)#controller t1 0/1/0
Snuggles(config-controller)#pri-group timeslots 1-24
Snuggles(config-controller)#^Z
```

```
Snuggles#show ip interface brief
Interface                  IP-Address      OK? Method Status        Protocol
FastEthernet0/0            192.168.100.10  YES NVRAM  up            up
FastEthernet0/1            unassigned      YES NVRAM  down          down
Serial0/1/0:0              unassigned      YES unset  down          down
Serial0/1/0:1              unassigned      YES unset  down          down
Serial0/1/0:2              unassigned      YES unset  down          down
Serial0/1/0:3              unassigned      YES unset  down          down
Serial0/1/0:4              unassigned      YES unset  down          down
Serial0/1/0:5              unassigned      YES unset  down          down
Serial0/1/0:6              unassigned      YES unset  down          down
Serial0/1/0:7              unassigned      YES unset  down          down
Serial0/1/0:8              unassigned      YES unset  down          down
Serial0/1/0:9              unassigned      YES unset  down          down
Serial0/1/0:10             unassigned      YES unset  down          down
Serial0/1/0:11             unassigned      YES unset  down          down
Serial0/1/0:12             unassigned      YES unset  down          down
Serial0/1/0:13             unassigned      YES unset  down          down
Serial0/1/0:14             unassigned      YES unset  down          down
Serial0/1/0:15             unassigned      YES unset  down          down
Serial0/1/0:16             unassigned      YES unset  down          down
Serial0/1/0:17             unassigned      YES unset  down          down
Serial0/1/0:18             unassigned      YES unset  down          down
Serial0/1/0:19             unassigned      YES unset  down          down
Serial0/1/0:20             unassigned      YES unset  down          down
Serial0/1/0:21             unassigned      YES unset  down          down
Serial0/1/0:22             unassigned      YES unset  down          down
Serial0/1/0:23             unassigned      YES unset  down          down
```

Wow! Take a look at that! Interfaces appearing like magic. The router has taken the T1 line and spliced it up into 24 (numbered 0–23) individual channels. These represent the 23 B-channels of the connection and the D-channel (which is inconspicuously labeled Serial0/1/0:23).

Just like BRI, all logical configuration is applied to the D-channel, which controls all the B-channels. From here on out, the rest of the configuration for PRI is identical to BRI; you just have more B-channels to work with.

EXAM ALERT

Although both the BRI and PRI flavors of ISDN could potentially be on the CCNA exam, it would be a safe bet to say that most of the questions will focus on the BRI concepts and configuration. PRI is usually reserved for the BCRAN CCNP exam.

Dial-on-Demand Routing

Because ISDN must dial to make a connection to another location, it is nearly impossible to talk about ISDN configuration without also discussing the partner technology, dial-on-demand routing (DDR). DDR configurations enable you to make a connection as resources are required and then disconnect when those resources are no longer needed. DDR is considered a separate technology from ISDN because it can also be used for other PSTN connections. For example, you might have a primary Frame Relay connection between your sites. If that fails, your ISDN link dials up as a backup connection. If that fails, a standard 56Kbps modem dials up as a final backup.

DDR connections are handy when you have small amounts of data to send periodically. Because ISDN is charged on a per-minute basis, the less you use the connection, the more it benefits your company's pocket book. If you are sending large amounts of data throughout the day, the cost of your low-speed ISDN connection may exceed the cost of purchasing a higher-speed, always-connected WAN link.

DDR Operation

Before you jump straight into the configuration, you need to learn at least the high points of how DDR works. ISDN configuration is a step-by-step process, so look at Figure 16.3 to see a visual of a network situation. The following list describes the process of a DDR connection on a Cisco router.

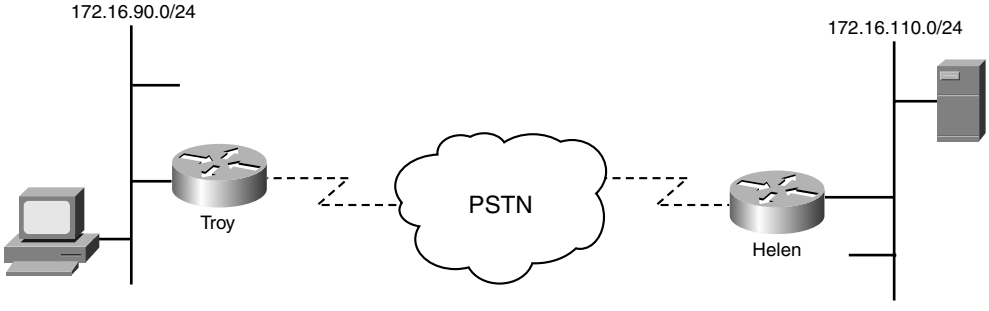


FIGURE 16.3 ISDN scenario.

1. The client on the 172.16.90.0 network decides to send some traffic to the server on the 172.16.110.0 network. The Troy router looks up the route in its routing table and determines that the next hop address is across the ISDN connection.
2. Troy checks to see whether the traffic being sent to the server classifies as "interesting traffic," as not all traffic is considered worthy enough to bring up the ISDN connection.

3. Troy looks up the phone number it needs to dial to reach the next hop address to the 172.16.110.0 network. This is the Helen router.
4. A phone call is placed and a connection made, and data is transmitted.
5. After a certain pre-configured time with no interesting traffic being sent, the Troy router hangs up the connection.

Traditional DDR Configuration

DDR configuration is not so much difficult as it is tedious. There are so many pieces of the configuration to remember that even the most seasoned Cisco technician can begin to forget pieces of DDR setup. Before you get into this configuration, you may be wondering, "Why is this section called 'traditional' DDR configuration?" It's called this because this is the simplest and oldest method to configure DDR. This method does lack some flexibility, however, so if you have just a single destination you are attempting to dial, traditional DDR is the way to go. The newer method, called Dialer Profiles, is discussed a little later in the chapter.

Even though there are many configuration pieces, setting up traditional DDR boils down to three major steps:

1. Configure static routes describing the remote network(s) accessible over the DDR connection.
2. Define the traffic type(s) that are "interesting" enough to bring up the DDR connection.
3. Map the remote IP address of the destination you are trying to reach to the phone number you need to dial to get there.

Now that you know the steps, it's time to talk about how to set up each one of them.

Configuring Static Routes

Throughout this book, we've talked about many different methods of populating a routing table—RIP, EIGRP, OSPF, and the list goes on. With all these different options, it might seem strange that you need to use the most primitive of all the routing methods, static routing, for your DDR connections. The reason behind this is that all the routing protocols generate some type of network traffic. With RIP it's broadcast traffic. With EIGRP and OSPF it's Hello messages. Any type of network traffic like this keeps the ISDN DDR connection active at all times, which can shoot the cost of your connection way up. Instead, defining a static route informs your router of the network(s) that are available remotely without generating any traffic on any of the router interfaces. Before you get into the syntax of this, take a look at the network diagram in Figure 16.4.

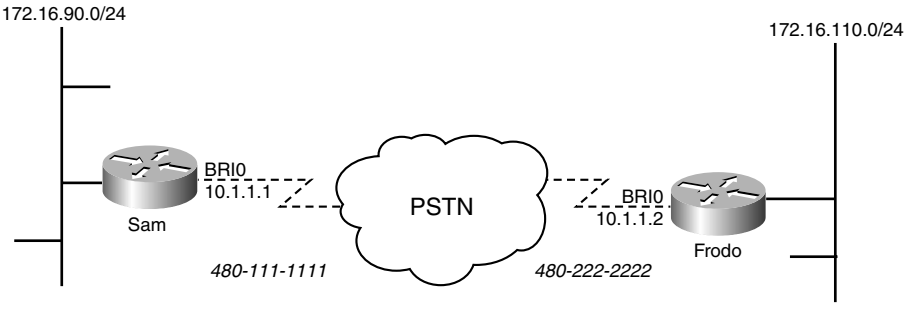


FIGURE 16.4 ISDN configuration scenario.

So you are able to get the big picture, look at the configuration of both routers. All you need to do initially is create a static route to tell the Sam and Frodo routers of the networks they can reach with the ISDN connection:

```
Sam#show ip interface brief
Interface                  IP-Address      OK? Method Status        Protocol
BRI0                       10.1.1.1        YES manual up            up
BRI0:1                     unassigned      YES unset  down          down
BRI0:2                     unassigned      YES unset  down          down
Ethernet0                  172.16.90.1     YES manual up            up
Sam#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sam(config)#ip route 172.16.110.0 255.255.255.0 10.1.1.2

Frodo#show ip interface brief
Interface         IP-Address      OK? Method Status                Protocol
BRI0              10.1.1.2        YES manual up                    up
BRI0:1            unassigned      YES unset  down                  down
BRI0:2            unassigned      YES unset  down                  down
Ethernet0         172.16.110.1    YES manual up                    up
\
Frodo#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Frodo(config)#ip route 172.16.90.0 255.255.255.0 10.1.1.1
```

At this point, the Sam and Frodo routers now know that they are able to reach each other's LAN network by using the ISDN connection. Looking at the interface status from `show ip interface brief`, it may be tempting to stop there; the BRI0 interface is showing a status of up, but this only means that the connection to the local service provider is working. You still do not have end-to-end connectivity. On to Step 2.

EXAM ALERT

Know that the reason why you do not use dynamic routing protocols over the ISDN connection is to ensure the line does not remain connected unnecessarily.

Defining Interesting Traffic

Cisco calls it "interesting traffic"; however, I prefer to call it "worthy traffic," as in, "This traffic is worthy enough to bring up my ISDN connection that charges me on a per-minute basis." Regardless of what you call it, you need to define the traffic types that will initiate the ISDN connection. You could be as broad as saying, "Any TCP/IP-based communication can bring up the ISDN link." Or you could say, "Only HTTP and FTP traffic can bring up the ISDN link."

You configure interesting traffic by using something known as a *dialer list*. Let me walk you through the general syntax, and then we'll get fancy.

```
Frodo(config)#dialer-list ?
  <1-10>  Dialer group number
```

The first thing you'll notice is that the `dialer-list` command is set up in Global Configuration mode. As a matter of fact, the general feel of a dialer list is similar to an access list. You create your dialer list entries in Global Configuration mode and then apply them under Interface Configuration mode, using a `dialer-group` command (just like the access list/access group relationship). At this point, you are prompted for a dialer list number. The version of IOS this router uses enables you to create up to 10 different dialer lists. The number you choose is not really significant, as long as it is a unique dialer list number on the router; again, this is just like the access list numbers.

```
Frodo(config)#dialer-list 1 ?
  protocol  Permit or Deny based on protocols
```

I decided to use dialer list number 1. Now the router requires that you type in the `protocol` keyword to choose what protocol you would like to permit or deny.

```
Frodo(config)#dialer-list 1 protocol ?
  appletalk         AppleTalk
  bridge            Bridging
  clns              OSI Connectionless Network Service
  clns_es           CLNS End System
  clns_is           CLNS Intermediate System
  decnet            DECnet
  decnet_node       DECnet node
  decnet_router-L1  DECnet router L1
  decnet_router-L2  DECnet router L2
  hpr               HPR
  ip                IP
  ipx               Novell IPX
  llc2              LLC2
  netbios           NETBIOS
  vines             Banyan Vines
  xns               XNS
```

The number of protocols you'll see in this list depends on the IOS version and feature set you are running. For almost everything we do in networks nowadays, you will be choosing the IP protocol.

```
Frodo(config)#dialer-list 1 protocol ip ?
  deny    Deny specified protocol
  list    Add access list to dialer list
  permit  Permit specified protocol
```

Now it's time to choose what you would like to permit and deny. Now, this is a major HUGE point: Creating a dialer list only *defines* the traffic that is permitted to initiate the ISDN connection, that is, that interesting (or "worthy") traffic. A dialer list *does not* dictate what traffic is allowed or not allowed over the connection. I realize this may sound like a contradictory statement, so let me explain a little further.

For this initial configuration, I am going to say that all IP traffic is permitted to initiate the ISDN connection. So, if the ISDN line is not connected and IPX or Appletalk traffic comes along, the line does not become active. The IPX and Appletalk traffic will be dropped. However, imagine that a packet of IP traffic comes along. Immediately, the ISDN line connects because IP traffic is considered interesting. Now, after the line is connected, the same IPX or Appletalk traffic comes to try to reach the other side. Now the traffic *will be sent* because the ISDN line is already connected. Just to highlight one more time, the dialer list does not say what traffic is allowed or denied across the ISDN link, just what traffic is allowed or not allowed to initiate (or dial) the ISDN link. With that understanding in place, it's time to finish the command:

```
Frodo(config)#dialer-list 1 protocol ip permit ?
  <cr>
```

At this point, there is a single dialer list that dictates all IP traffic as being considered worthy to bring up the line. However, the router now needs to know *what* line is to be brought up. Dialer lists do not have any effect on anything until they are applied.

```
Frodo(config)#interface bri 0
Frodo(config-if)#dialer-group 1
```

That's it! Now, if any IP traffic hits the Frodo router that attempts to reach any destination on the Sam router, the Frodo router knows to initiate the BRI 0 interface (which is the ISDN connection). Now add the same configuration to the Sam router to ensure it can initiate a connection to Frodo.

```
Sam(config)#dialer-list 1 protocol ip permit
Sam(config)#interface bri 0
Sam(config-if)#dialer-group 1
```

One quick note before we move on. I mentioned earlier that dialer lists have the capability to be restrictive enough to allow only certain traffic types (such as HTTP or FTP) to initiate DDR connections. They do so by combining access lists with dialer lists. Let me show you an example that allows only HTTP or FTP traffic to initiate an ISDN connection:

```
Sam(config)#access-list 100 permit tcp any any eq 80
Sam(config)#access-list 100 permit tcp any any eq 21
Sam(config)#dialer-list 2 protocol ip list 100
Sam(config)#interface bri 1
Sam(config-if)#dialer-group 2
```

Only TCP traffic that uses port 80 or port 21 (HTTP and FTP) from any source to any destination will be considered "interesting" to dialer list 2. The dialer list 2 was then applied to the BRI 1 interface. As you can see, by combining access lists with dialer lists, you can be as detailed as you want with what types of traffic you consider interesting enough to initiate your connection.

EXAM ALERT

Be sure to remember that a dialer list does not dictate what traffic is allowed or denied to cross the ISDN connection. That's the job of an access list. A dialer list simply dictates what traffic is considered interesting enough to activate the ISDN connection.

Map Remote Addresses

Now it's time to take the third and final step of setting up a traditional ISDN DDR connection. You need to map a Layer 2 ISDN address to the Layer 3 IP address it can reach. Simply put, you need to tell the ISDN interface what phone number to dial to reach the other side of the connection. You do this from interface configuration mode, using the `dialer map` command. Look at the following to walk through it step by step for Sam and Frodo:

```
Sam(config)#interface bri 0
Sam(config-if)#dialer map ?
  appletalk  AppleTalk
  bridge     Bridging
  clns       ISO CLNS
  decnet     DECnet
  hpr        HPR
  ip         IP
  ipx        Novell IPX
  llc2       LLC2
  netbios    NETBIOS
  pppoe      PPP over Ethernet
  snapshot   Snapshot routing support
```

```
  vines      Banyan VINES
  xns        Xerox Network Services

Sam(config-if)#dialer map ip ?
  A.B.C.D  Protocol specific address
```

Remember that the goal in this: You need to tell the Sam router what phone number it should dial to reach Frodo's IP address. So, in this case, you are going to map Frodo's BRI 0 interface address to the phone number you dial to get there. Looking back at Figure 16.4, you can see that Frodo's IP address is 480-222-2222 (I am using an ISDN simulator, which is why the phone number looks a little cheesy).

```
Sam(config-if)#dialer map ip 10.1.1.2 ?
  WORD           Dialer string (quote strings containing #)
  broadcast      Broadcasts should be forwarded to this address
  class          dialer map class
  modem-script   Specify regular expression to select modem dialing script
  name           Map to a host
  spc            Semi Permanent Connections
  speed          Set dialer speed
  system-script  Specify regular expression to select system dialing script
```

Wow! Lots of options you can set up. Before I explain the highlighted commands, let me first say that the only thing you need to do to get the ISDN connection working is to type in the phone number (shown here in context-sensitive help as `WORD`). I've highlighted the most common options that administrators add to the dialer map. Just as in the world of Frame Relay, the `broadcast` keyword allows broadcast and multicast packets to cross the ISDN connection. This is critical if you would like your routing protocols to work over the ISDN line. The `name` keyword enables you to type in the name of the remote router. This is necessary if you are using CHAP or PAP PPP-based authentication on your ISDN connection (discussed fully in the WAN protocols chapter of this book). In this configuration, you can add the `broadcast` keyword to allow routing protocols to function.

```
Sam(config-if)#dialer map ip 10.1.1.2 broadcast 4802222222
```

There you go. Now, add the necessary command to the Frodo router:

```
Frodo(config-if)#dialer map ip 10.1.1.1 broadcast 4801111111
```

And that's all there is to it! Now, I know the commands have become a little chopped up with all the commentary in between. So now take a look at the complete configuration for both sides of the connection one last time before we test everything out.

EXAM ALERT

Be sure to remember what the `broadcast` keyword does, for both ISDN and Frame Relay connections.

Complete DDR Configuration

Listed here are the complete configurations of the Sam and Frodo routers:

```
Sam#show run
!
!--<unneccesary output omitted>--!
!
interface Ethernet0
 ip address 172.16.90.1 255.255.255.0
!
interface BRI0
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 dialer map ip 10.1.1.2 broadcast 48022222222
 dialer-group 1
 isdn spid1 111
 isdn switch-type basic-5ess
!
ip route 172.16.110.0 255.255.255.0 10.1.1.2
dialer-list 1 protocol ip permit

Frodo#show run
!
!--<unneccesary output omitted>--!
!
interface Ethernet0
 ip address 172.16.110.1 255.255.255.0
!
interface BRI0
 ip address 10.1.1.2 255.255.255.0
 encapsulation ppp
 dialer map ip 10.1.1.1 broadcast 4801111111
 dialer-group 1
 isdn spid1 222
 isdn switch-type basic-5ess
!
ip route 172.16.90.0 255.255.255.0 10.1.1.1
dialer-list 1 protocol ip permit
```

Verification

With held breath, you can now move into testing the ISDN configuration. It is not too difficult to make sure everything is working; all you should need to do is attempt to ping from one side of the connection to the other. For example, you could get on the Sam router and ping the LAN interface of the Frodo router. Here's the flow of what will happen (understanding this is key to understanding why the DDR connection initiates):

1. On the Sam router, ping 172.16.110.1, which is the LAN interface of the Frodo router.
2. Sam looks at its routing table and finds out that it has a static route to the 172.16.110.0/24 network with 10.1.1.2 listed as the next-hop-address. The best route to reach that address is its BRI0 interface, which is directly connected to the 10.1.1.0/24 network.
3. The BRI0 is recognized as a DDR interface. The Sam router checks to see whether the ping message is considered "interesting traffic" by looking at the dialer-list/dialer-group commands.
4. After the traffic is identified as interesting, the dialer-map is checked to see what phone number is necessary to reach the 10.1.1.2 address. The phone number is dialed.
5. The Frodo router answers the incoming call, negotiates PPP options, and the link is connected. The ping message goes through.

This entire process happens in 1–2 seconds. To verify the process, you can use a couple of the troubleshooting commands, `debug dialer` and `debug isdn events`, to watch the progress.

```
Sam#debug dialer
Dial on demand events debugging is on
Sam#debug isdn events
ISDN events debugging is on
Sam#ping 172.16.110.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.110.1, timeout is 2 seconds:

1d05h: BR0 DDR: Dialing cause ip (s=10.1.1.1, d=172.16.110.1)
1d05h: BR0 DDR: Attempting to dial 4802222222
1d05h: ISDN BR0: Outgoing call id = 0x8009, dsl 0
1d05h: ISDN BR0: Event: Call to 4802222222 at 64 Kb/s
1d05h: ISDN BR0: process_bri_call(): call id 0x8009, called_number
4802222222, speed 64, call type DATA
1d05h: CCBRI_Go Fr Host InPkgInfo (Len=25) :
1d05h: 1 0 1 80 9 0 4 2 88 90 18 1 83 2C A 34 38 30 32 32 32 32 32 32 32
1d05h:
1d05h: CC_CHAN_GetIdleChanbri: dsl 0
1d05h:     Found idle channel B1
1d05h: CCBRI_Go Fr L3 pkt (Len=7) :
1d05h: 2 1 9 98 18 1 89
1d05h:
1d05h: ISDN BR0: LIF_EVENT: ces/callid 1/0x8009 HOST_PROCEEDING
1d05h: ISDN BR0: HOST_PROCEEDING
1d05h: ISDN BR0: HOST_MORE_INFO
1d05h: CCBRI_Go Fr L3 pkt (Len=4) :
1d05h: 7 1 9 91
```

```
1d05h:
1d05h: ISDN BR0: LIF_EVENT: ces/callid 1/0x8009 HOST_CONNECT
1d05h: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 32/35/36 ms
Sam#
1d05h: ISDN: get_isdn_service_state(): idb 0x23D644 bchan 2 is_isdn 1
1d05h: ISDN BR0: Event: Connected to 4802222222 on B1 at 64 Kb/s
1d05h: BR0:1 DDR: dialer protocol up
Sam#
1d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
state to up
Sam#
1d05h: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 4802222222
```

Watching all that happen is like watching a good fireworks show. Now, there's plenty of information to weed through, but take a look at the action. As soon as the `ping 172.16.110.1` command is entered, the router goes into gear. It first shows the cause of the dialing event: "The source IP 10.1.1.1 is trying to access the destination 172.16.110.1." Right after that, it quickly says, "I'm trying to dial 4802222222." A flurry of messages follows, up to the `HOST CONNECT`. Do you notice the `.!!!!` right after the BRI0:1 goes up? That's the result of the ping attempts. It looks like the first `.` is the period at the end of the sentence, but actually, it's a dropped ping. In the time it took the router to bring up the ISDN connection, a single ping message was dropped. The other four exclamation points indicate success for all the following ping messages.

Let me show you two verification commands before we move on. They are the `show dialer` and `show isdn status` commands:

```
Sam#show dialer

BRI0 - dialer type = ISDN

Dial String      Successes   Failures    Last DNIS   Last status
4802222222               5          0    00:00:57       successful
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.

BRI0:1 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: ip (s=10.1.1.1, d=172.16.110.1)
Time until disconnect 64 secs
Connected to 4802222222

BRI0:2 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

The `show dialer` command gives you some key information describing DDR operations. You can see that I've been having a little fun in the background because it shows five successful dials of 480-222-2222. I have dialed on five different occasions because the default idle-timer for DDR connections is 120 seconds. If the ISDN connection does not see any interesting traffic for 2 minutes, the line is disconnected. Unfortunately, it has taken me 10 minutes to type all the information you've read from the beginning of the ISDN test until now, causing the ISDN connection to drop on five occasions. This default timer is usually a good thing because ISDN connections can be costly if you keep them connected too long. However, if you ever want to change it (or turn off the idle disconnect completely), just use the `dialer idle-timeout` command under the interface configuration mode.

```
Sam#show isdn status
Global ISDN Switchtype = basic-5ess
ISDN BRI0 interface
        dsl 0, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 66, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
        I_Queue_Len 0, UI_Queue_Len 0
        TEI 66, ces = 1, state = 8(established)
            spid1 configured, spid1 sent, spid1 valid
            Endpoint ID Info: epsf = 1, usid = 1, tid = 2
    Layer 3 Status:
        1 Active Layer 3 Call(s)
        CCB:callid=800A, sapi=0, ces=1, B-chan=1, calltype=DATA
    Active dsl 0 CCBs = 1
    The Free Channel Mask:  0x80000002
    Number of L2 Discards = 0, L2 Session ID = 5
```

The `show isdn status` command is always handy to use because it will give you each layer of your ISDN connectivity and show any problems that occur at each. For example, when I was setting everything up that you see here, I mistyped the SPID for the connection. When I issued the `show isdn status` command, it flagged me right under the Layer 2 Status section that SPID1 was invalid.

Dialer Profile Configuration

You now know enough that you can move from the world of traditional DDR configurations into the more flexible, but slightly more complex idea of DDR that uses dialer profiles.

What's Wrong with Traditional DDR?

To answer the question directly, there's nothing wrong with traditional DDR. It works just fine for fairly simple configurations; however, it doesn't give you the flexibility you need to change

interface configurations based on the location you are dialing. For example, take a look at Figure 16.5.

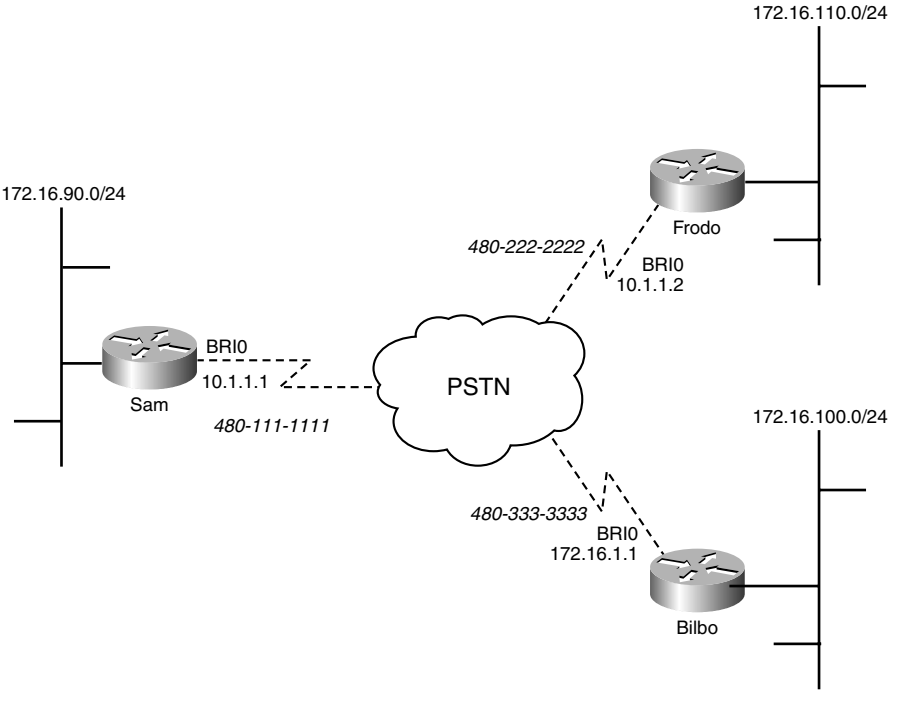


FIGURE 16.5 ISDN connections with multiple destinations.

It's the same story as before: The Sam and Frodo routers are connected to each other via ISDN. But now a new character has joined the tale: Bilbo. Do you see any problem with connecting to the Bilbo router? Check out the IP address assigned to the BRI0 interface. It's on a different network than the Sam and Frodo routers. Sam (or Frodo) could dial up the Bilbo router, but after they connected, the interfaces would not be able to communicate. Now you might be thinking, "Why don't you just change the Bilbo IP address to something on the 10.1.1.0/24 network?" Well, it just so happens that the Bilbo router receives calls from the Gandalf router (not pictured) that is under government regulations to be assigned the IP address 172.16.1.2. Therefore, Bilbo's address cannot be changed…now what? Traditional DDR comes up short because everything is manually assigned to the interface. Welcome to dialer profiles.

Dialer Profile Concepts

You may be familiar with Windows user profiles if you've had any experience in the Microsoft side of the game. If not, let me give you an overview. In a network, every user is different.

They all like different screensavers, different backgrounds, different icons on the desktop. To keep it all straight, Microsoft Windows creates a profile for each user, which remembers the exact settings used with each login to the computers.

Dialer profiles are a very similar concept. You create profiles for each unique interface configuration you require for your network environment. These profiles contain all your logical settings that you would usually assign to the BRI interface, such as IP addressing, authentication, dialed numbers, and so on. You then tell those profiles which physical interface(s) they can use if called upon, and you're good to go. The toughest thing to learn about this configuration is the terms. Figure 16.6 gives a visual representation of the components of dialer profiles.

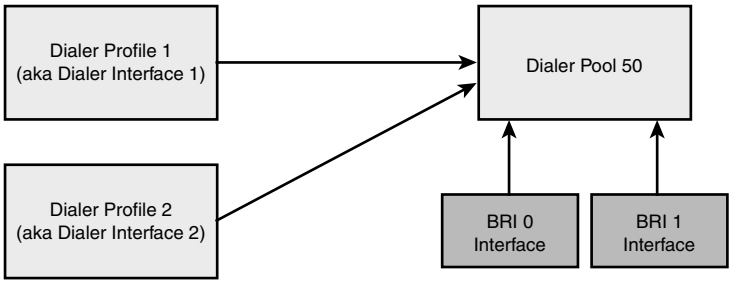


FIGURE 16.6 Cisco dialer profiles.

When configuring dialer profiles, the first step is not typically setting up the profile itself. You'll first configure your *dialer pools*. Dialer pools are just a logical group of physical interfaces that these profiles will be able use if needed. Think back to playing team sports in grade school. You usually had a couple team captains who would pick the players they would like on their team. The kids "not yet picked" would stand in a big blob in hopeful expectation of being picked next. That's all a dialer pool is: a big blob of one or more ordered, physical interfaces. For example, I could create a dialer pool that looked something like this:

Dialer Pool 50

- First Pick: BRI0 interface
- Second Pick: BRI1 interface
- Third Pick: AUX Modem

I'd then associate that dialer pool with a dialer profile, which contains the entire logical configuration for the connection. The call flow would then look something like this:

Router# ping 172.16.100.1

(*begin router's inner monologue*)

Router Processor: "Hey! We just got an outgoing call for the Gandalf router—use the configuration in Dialer Profile #2!"

Dialer Profile #2: "I'm ready to go. Let me just grab an interface from Dialer Pool 50. Who's listed first?"

BRI0 Interface: "I'm listed first, but unfortunately, I'm currently in use."

Dialer Profile #2: "All right then, who's listed second?"

BRI1 Interface: "I'm second, and I'm ready for action."

Dialer Profile #2: "Alright BRI1, here's the IP address, encapsulation, and phone number I want you to use."

(end router's inner monologue)

From there, all the logical configuration you've configured in Dialer Profile #2 is applied to the BRI1 interface and the call goes through. After the router completes the call, all the logical configuration is removed from the BRI1 interface and it returns as a "generic interface" to the Dialer Pool 50.

Now that you've seen the flow of a typical dialer profile-based call, here's how you will usually set up the configuration:

1. Add physical interfaces to the dialer pool.
2. Configure dialer profiles (aka dialer interfaces) for each configuration you need applied to the ISDN interface.
3. Associate dialer interfaces with a dialer pool.

The following sections walk through these actions one at a time.

Configuring Dialer Pools

Dialer pools are a little more theoretical than most Cisco configurations. They are more of an "implied" configuration than an actual line item. You will never create a dialer pool explicitly; rather, you'll just begin adding physical interfaces to a pool, causing it to be implicitly created. Take a look:

```
Sam#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sam(config)#interface bri 0
Sam(config-if)#dialer pool-member ?
  <1-255>  Dialer pool number

Sam(config-if)#dialer pool-member 50
Sam(config-if)#exit
Sam(config)#interface bri 1
Sam(config-if)#dialer pool-member 50
```

I never went and defined Dialer Pool 50 on the Sam router; instead, it was implicitly created when the BRI0 and BRI1 interfaces were added to it. That's all there is to this step, but before you move on, let me mention a few dialer pool rules:

- An interface can be a member of multiple dialer pools.
- A dialer profile can use only a single dialer pool.
- Multiple dialer profiles can use the same dialer pool.

Configuring Dialer Interfaces and Associating Dialer Pools

After you have associated the physical interfaces with the dialer pools, you can create your dialer interfaces. A dialer interface is the same thing as a dialer profile; it's just the practical application of the theory (that is, a dialer interface is the configuration; a dialer profile is the theory). The concepts are the same as those involved in configuring traditional DDR, however, some of the syntax is different. I'll set up the Sam router to operate in the scenario given previously in Figure 16.5.

```
Sam(config)#interface dialer 1
Sam(config-if)#description CONNECTION TO FRODO
Sam(config-if)#ip address 10.1.1.1 255.255.255.0
Sam(config-if)#encapsulation ppp
Sam(config-if)#dialer pool 50
Sam(config-if)#dialer string 4802222222
Sam(config-if)#dialer-group 1
Sam(config-if)#exit
Sam(config)#interface dialer 2
Sam(config-if)#description CONNECTION TO GANDALF
Sam(config-if)#ip address 172.16.1.2 255.255.255.0
Sam(config-if)#encapsulation ppp
Sam(config-if)#dialer pool 50
Sam(config-if)#dialer string 4803333333
Sam(config-if)#dialer-group 1
Sam(config-if)#exit
Sam(config)#^Z
Sam#show ip interface brief
Interface                  IP-Address      OK? Method Status       Protocol
BRI0                       unassigned      YES manual up           up
BRI0:1                     unassigned      YES unset  down         down
BRI0:2                     unassigned      YES unset  down         down
BRI1                       unassigned      YES manual up           up
BRI1:1                     unassigned      YES unset  down         down
BRI1:2                     unassigned      YES unset  down         down
Dialer1                    10.1.1.1        YES manual up           up
Dialer2                    172.16.1.2      YES manual up           up
Ethernet0                  172.16.90.1     YES manual up           up
```

You can see that you now have two different dialer interfaces that have magically appeared on the router. These are the dialer profiles. The configuration of the interface uses all the same components as the traditional DDR configuration; however, the `dialer map` command has been replaced by `dialer string` because each dialer profile can connect to only a single destination. Both these dialer interfaces are pulling from the same Dialer Pool 50, which includes both the BRI0 and BRI1 interfaces. This configuration removes nearly the entire configuration from the physical BRI interfaces. However, just a few commands must be in place:

```
Sam(config)#interface bri 0
Sam(config-if)#encapsulation ppp
Sam(config-if)#ppp authentication chap
Sam(config-if)#dialer pool-member 50
Sam(config-if)#exit
Sam(config)#interface bri 1
Sam(config-if)#encapsulation ppp
Sam(config-if)#ppp authentication chap
Sam(config-if)#dialer pool-member 50
```

This base configuration enables the BRI0 and BRI1 interfaces to receive incoming calls. When an incoming call arrives on the ISDN interface, it needs to perform a ground-level negotiation with the other side to determine which dialer profile to use. If CHAP authentication is enabled, it asks the incoming caller for a username. The other side supplies the username, and the router can check for the dialer profile that uses this username. If CHAP authentication is not used, Caller-ID information can be used to determine which dialer profile matches the incoming caller.

Additional Dialer Configurations

As with anything in the Cisco world, there are many ways that you can modify and tune your DDR operations to be the most efficient for your organization. This section talks about the most common tuning methods. However, keep in mind that there is an entire CCNP course and exam dedicated to fully discussing all the options at your disposal: BCRAN. What is discussed at the CCNA level is only an introduction.

Dialer Timers

As you've already discovered, DDR connections are not meant to be connected continually. They connect when needed and then disconnect when their time is through. By default, the dialer disconnects after 2 minutes of "idle time." This does not mean that traffic is not using the connection; it just means that two minutes have passed without the router seeing any interesting traffic. Two configuration commands can affect this timer:

```
Frodo(config-if)#dialer ?
  callback-secure        Enable callback security
  caller                 Specify telephone number to be screened
  enable-timeout         Set length of time an interface stays down
  fast-idle              Set idle time before disconnecting line with an
                         unusually high level of contention
  hold-queue             Configure output hold queue
  idle-timeout           Specify idle timeout before disconnecting line
  load-threshold         Specify threshold for placing additional calls
  map                    Define multiple dial-on-demand numbers
  pool-member            Specify dialer pool membership
  priority               Specify priority for use in dialer group
  rotary-group           Add to a dialer rotary group
  snapshot               Specify snapshot sequence number
  string                 Specify telephone number to be passed to DCE device
  wait-for-carrier-time  How long the router will wait for carrier
  watch-disable          Time to wait before bringing down watched route link
  watch-group            Assign interface to dialer-watch-list
```

These two commands are known as the `idle-timeout` and the `fast-idle`. I wanted to flash up the context-sensitive help for the dialer command just to show you that there are many other ways to tune the DDR connection. This should give you an idea of a few of those methods.

The `dialer idle-timeout` command is used to specify, in seconds, how long the router should wait without seeing interesting traffic before disconnecting the DDR connection.

```
Frodo(config-if)#dialer idle-timeout ?
  <0-2147483>  Idle timeout beforedisconnecting a call
```

As you can see, the router is quite flexible with the length of time you can select. By setting the idle-timeout to zero, you effectively disable the idle timer. After the DDR connection is dialed, it remains connected until you manually disconnect the interface.

The `dialer fast-idle` is a handy sidekick to the `idle-timeout` syntax. This is used to override the idle timer if there is another call waiting to be placed. For example, you might have sent some traffic from the Sam router to the Frodo router. Meanwhile, another application is attempting to send traffic to the Gandalf router. Without the fast idle timer, that traffic needs to wait until the full idle timer is reached. However, if you configure the fast idle timer, the router can lessen the wait time before dialing.

```
Sam(config-if)#dialer fast-idle ?
  <1-2147483>  Fast idle in seconds
```

As you can see, the router is just as flexible with the range for your fast idle timer. Keep in mind that this value should be significantly less than your normal idle timer to be effective.

Bandwidth on Demand and PPP Multilink

I don't know whether you noticed, but when the initial connection was established between the Sam and Frodo routers (in the previous Traditional DDR section), only one of the ISDN B-channels activated. In an ISDN BRI connection there are always two B-channels at your disposal. However, the router uses only one of them unless you specifically configure it to use more. Even the PRI connection, which has 23 B-channels, uses the first B-channel unless you activate more. The method of activation used is called PPP Multilink.

PPP Multilink is one of the LCP options discussed back in Chapter 15. It enables multiple WAN connections to be bundled into a single pipe of bandwidth. Even though you have only a single ISDN connection, you must employ the features of PPP Multilink to actively use and load balance traffic across all the B-channels the ISDN line provides. Thankfully, PPP Multilink is an industry standard feature. All routers supporting the PPP protocol must also support PPP Multilink, which means that this feature can function between Cisco routers and non-Cisco routers.

If you do decide to use Cisco routers to manage your ISDN connections, you gain an additional feature: Bandwidth on Demand (BOD). Here's the concept: Each B-channel that you connect in your ISDN bundle begins incurring cost. The service provider charges you on a per-minute basis for each additional B-channel you add to your connection. If you activate PPP Multilink, no matter what traffic is sent across the connection, all the B-channels become active. Even if there is just a single, small ICMP ping message sent across the line, every single B-channel in the bundle quickly connects until the idle timer is reached. This is not cost efficient. To address this issue, Cisco's BOD enables the router to watch the ISDN connection. As the load on the interface rises, more B-channels are activated. As the interface load lessens, the B-channels are disconnected. Take a look at the configuration. The Sam and Frodo routers in the base configuration depicted in Figure 16.4 are used for this example.

```
Sam#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sam(config)#interface bri 0
Sam(config-if)#ppp multilink
Sam(config-if)#dialer load-threshold ?
  <1-255>  Load threshold to place another call

Sam(config-if)#dialer load-threshold 127 ?
  either    Threshold decision based on max of inbound and outbound traffic
  inbound   Threshold decision based on inbound traffic only
  outbound  Threshold decision based on outbound traffic only
  <cr>

Sam(config-if)#dialer load-threshold 127 either
```

Before you configure the Frodo router, take a look at this. The `ppp multilink` features were activated first, which enables the router to bundle multiple B-channels into a single pipe of bandwidth. Then the Cisco BOD feature was activated with the `dialer load-threshold` syntax. The interesting thing is that it provides a range of 1–255 to use for the load value. Cisco uses this rather odd numbering scheme to represent a percentage. A load value of 1 represents a value of nearly 0%. A load value of 255 represents a value of 100%. Setting the BOD load value to 1 causes all your ISDN B-channels to activate as soon as traffic is sent. In this example, the BOD load value is set to 127, which represents roughly 50%. This means that if the ISDN B-channels are at a load of 50% in either direction (because of the `either` command typed at the end), the router activates more B-channels. Now it's time to set up the Frodo side of things:

```
Frodo#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Frodo(config)#interface bri 0
Frodo(config-if)#ppp multilink
Frodo(config-if)#dialer load-threshold 127 either
```

Technically, because the Sam and Frodo routers are the only two routers in this picture, you need to turn on BOD on only one side of the connection because you are using the `either` keyword to watch both inbound and outbound traffic levels. Do note that the `ppp multilink` command is needed on both sides of the connection for this to work properly. The last thing you need to do is to test your configuration. To generate 50% traffic load, I'm going to use an extended `ping` command and increase the size of packet that is sent over the ISDN line to a reasonable amount.

```
Sam#ping
Protocol [ip]:
Target IP address: 10.1.1.2
Repeat count [5]: 1000
Datagram size [100]: 800
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1000, 800-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

03:06:55: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up..
03:06:57: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up!!!!
03:06:58: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
➥state to up
03:06:59: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
➥changed state to up!!!!!!!!!!
03:07:01: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 4802222222
➥Frodo!!!!!!!!!!
03:07:22: %LINK-3-UPDOWN: Interface BRI0:2, changed state to up!!!!!!!!!
03:07:23: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed
```

```
➥state to up!!!!!!!!!!!!!!!!!!!!!!!!.
Success rate is 98 percent (156/159),
➥round-trip min/avg/max = 116/185/464 ms
Sam#
03:07:28: %ISDN-6-CONNECT: Interface BRI0:2 is now connected to
➥4802222222 Frodo
```

This output might look a little confusing at first. A ping is initiated from Sam to Frodo. Initially, the BRI0:1 interface (the first B-channel) went active and was the only one that stayed active for a significant amount of time. Finally, the BRI0:2 went active and joined the Virtual-Access1 interface. This Virtual-Access1 interface is created dynamically by PPP Multilink to join the multiple B-channels into a single, logical connection.

The reason the BRI0:2 channel took so long to go active is because the Cisco router handles all the interface load on a 5-minute average, by default. Take a look at the `show interface` output for the first B-channel:

```
Sam#show interface bri 0:1
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 59/255, rxload 59/255
  Encapsulation PPP, loopback not set
!--<excessive output cut out>--!
```

The `txload` parameter is the amount of load the interface has in the outbound (send) direction. The `rxload` parameter is the amount of load the interface has in the inbound (receive) direction. Using a 5-minute average causes these values to move up or down a little slower than you might expect. This is good because you don't want your B-channels constantly going up and down as traffic load goes up and down many times every few seconds. Averaging out the load lets you see the overall performance rather than a snapshot of instantaneous network performance.

EXAM ALERT

Be sure you remember that interface load and BOD configuration use a scale of 1–255, where 1 represents nearly 0% and 255 represents 100%.

Troubleshooting ISDN

Thankfully, ISDN connections are one of the easiest connections to troubleshoot because of the numerous `show` and `debug` commands that enable you to focus on each portion of the ISDN configuration. Most of these commands you have already seen in action over the course

of this chapter, so I present just a list describing each command, the area it monitors, and a sample output.

- `show dialer`—This command enables you to view the overall status of your DDR connections. It shows the number dialed, how many successes and failures the connection has had, and the majority of your idle timers.

```
Sam#show dialer

BRI0 - dialer type = ISDN

Dial String      Successes   Failures    Last DNIS   Last status
4802222222               6          1    00:11:35       successful
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.

BRI0:1 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

BRI0:2 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

- `show isdn active`—This shows the current, active ISDN calls on your router.

```
Sam#show isdn active
------------------------------------------------------------------------
                                ISDN ACTIVE CALLS
------------------------------------------------------------------------
Call Calling Called Remote Seconds Seconds Seconds Charges
Type Number Number Name Used Left Idle Units/Currency
------------------------------------------------------------------------
Out   ---N/A--- 4802222222     Frodo     14 Unavail   -       0
------------------------------------------------------------------------
```

- `show isdn status`—One of the handiest commands in my opinion. Shows all three layers of ISDN connectivity (Physical through Network) and the status of each.

```
Sam#show isdn status
Global ISDN Switchtype = basic-5ess
ISDN BRI0 interface
        dsl 0, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 66, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
```

```
        Layer 3 Status:
            1 Active Layer 3 Call(s)
            CCB:callid=8008, sapi=0, ces=1, B-chan=1, calltype=DATA
        Active dsl 0 CCBs = 1
        The Free Channel Mask:  0x80000002
        Number of L2 Discards = 0, L2 Session ID = 11
        Total Allocated ISDN CCBs = 1
```

- `debug isdn q921`—Shows messages related to the setup of the ISDN connection between your router and the service provider (Layer 2 information).
- `debug isdn q931`—Shows messages related to the setup of the ISDN connection between your router and the destination router (Layer 3 information).
- `debug dialer`—Enables you to monitor the progress of DDR connections as they dial and disconnect.

EXAM ALERT

Be familiar with the output and purpose of the `show isdn status` and `show dialer` commands.

Chapter Summary

Even though ISDN is a slowly disappearing technology, it is still in widespread use in major cities around the world and will probably stay around for many years to come. The beauty of understanding the ISDN connections is that you now have gained the knowledge of DDR, which can be applied to many other on-demand connections other than ISDN.

ISDN comes in two flavors: BRI and PRI. The type of ISDN connection you use dictates the number of B-channels assigned to your bundle. The B-channels are designed to carry data and have 64Kbps each. The D-channel is used for signaling and uses 16Kbps on BRI ISDN connections or 64Kbps on PRI ISDN connections. BRI is still in widespread use outside the United States, where PRI seems to be the more popular flavor.

ISDN connections are charged on a per-B-channel, per-minute basis, which introduces the need for DDR routing. DDR watches for interesting traffic that attempts to cross the ISDN connection. Traffic is considered interesting if it matches the criteria you have defined in your dialer list. After the router sees interesting traffic, the ISDN connection is activated and transmits the data. The ISDN connection remains active as long as interesting traffic continues to cross the link. If there is no interesting traffic, the router waits the amount of time you have defined in the `dialer idle-timeout` syntax, which is 2 minutes by default, and then disconnects the line.

ISDN connections can be made more efficient through the use of PPP Multilink and Cisco's BOD. These two features enable you to activate more than one B-channel at a time as the bandwidth demands require. As the network traffic begins to settle down, the B-channels steadily disconnect. This gives you an automated cost-control mechanism that will keep unnecessary B-channels from becoming or staying connected longer than they are needed.

Key Terms

- Integrated Service Digital Network (ISDN)
- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)
- Bearer channel (B-channel)
- Delta channel (D-channel)
- Common Channel Signaling (CCS)
- Channel Associated Signaling (CAS)
- Q.921
- Q.931
- Network Termination, Type 1 (NT-1)
- Network Termination, Type 2 (NT-2)
- Terminal Endpoint, Type 1 (TE1)
- Terminal Endpoint, Type 2 (TE2)
- Terminal Adapter (TA)
- ISDN switch type
- Service Provider IDentifiers (SPIDs)

- dial-on-demand routing (DDR)
- interesting traffic
- dialer map
- dialer list/dialer group
- dialer profile
- dialer pool
- dialer interface
- idle timer/fast idle timer
- Bandwidth on Demand (BOD)
- PPP Multilink

Apply Your Knowledge

Exercises

16.1 Identifying the Pieces of ISDN

Understanding the physical layout of ISDN connections is a key element in Cisco certification exams. Fill in each piece of Figure 16.7, using the following terminology reference. Use Figure 16.1 at the beginning of the chapter to check your work.

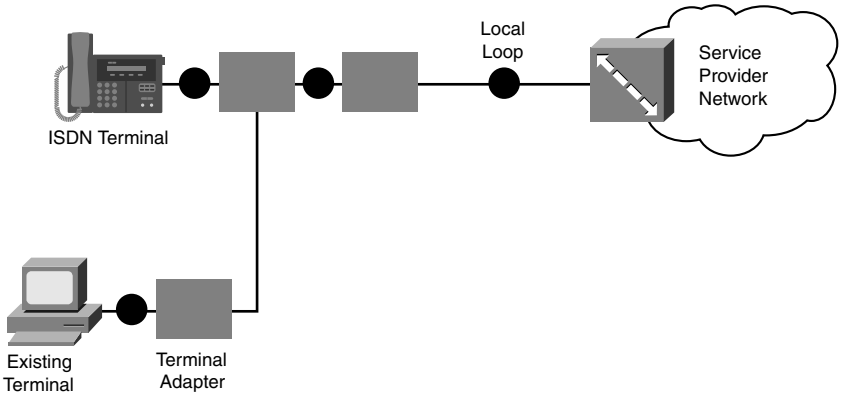


FIGURE 16.7 ISDN equipment and reference points.

Equipment:

- **Network Termination, Type 1 (NT-1)**—Converts from the two-wire ISDN line the service provider installs in your location to a four-wire connection that your internal devices can use.
- **Network Termination, Type 2 (NT-2)**—This optional device enables you to either split the ISDN signal or aggregate multiple ISDN connections into a single stream.
- **Terminal Endpoint, Type 1 (TE1)**—This is an ISDN-compatible endpoint, such as a router with an ISDN S/T or U interface.

- **Terminal Endpoint, Type 2 (TE2)**—This is a non-ISDN–compatible endpoint, such as a router with no ISDN interfaces or an end-user PC, requiring a Terminal Adapter (TA) to understand the ISDN signal, such as a router with no ISDN interfaces or an end-user PC.
- **Terminal Adapter (TA)**—This device converts an ISDN signal into some other type of signaling.

Reference Points:

- **U**—Identifies the connection leading up to the NT-1 device
- **T**—Identifies the connection between the NT-1 and NT-2 devices
- **S**—Identifies the connection between the NT-2 and TE1 devices
- **R**—Identifies the connection between the TA and TE2 devices

Estimated Time: 5 minutes

Review Questions

1. ISDN connections comprise B-channels and D-channels. Explain the difference between these channels.
2. What are the two different types of ISDN BRI interfaces you can purchase for your router? In what circumstance would you use each?
3. You are troubleshooting the ISDN communication between your router and the service provider. What debug command would key in on this communication? In addition, what debug command would you use if you were troubleshooting the end-to-end connectivity between two ISDN routers?
4. Configuring dial-on-demand routing (DDR) on a Cisco router can be a complex processes. Recount the general steps to follow when performing this configuration.
5. When would you choose to use a dialer profile configuration with ISDN?

Exam Questions

1. Which of the following ISDN configurations has two B-channels and one D-channel?
   - ❍ **A.** BRI
   - ❍ **B.** PRI
   - ❍ **C.** DDR
   - ❍ **D.** JRI

2. During normal operation, what is the status of the D-channel of the ISDN connection if your verification techniques use the `show interface` syntax?

   - ❍ **A.** Interface Down, Line Protocol Down
   - ❍ **B.** Interface Up, Line Protocol Down
   - ❍ **C.** Interface Up, Line Protocol Up (Spoofing)
   - ❍ **D.** None of the above

3. Which of the following ISDN components would represent a Cisco router equipped with an ISDN U-interface?

   - ❍ **A.** NT-1
   - ❍ **B.** NT-2
   - ❍ **C.** TE-1
   - ❍ **D.** TE-2
   - ❍ **E.** TA

4. Which of the following commands maps the remote IP address 10.1.1.2 to the phone number 602-555-1212 and allows routing updates to cross the ISDN connection?

   - ❍ **A.** `dialer map ip 10.1.1.2 broadcast 6025551212`
   - ❍ **B.** `dialer map 10.1.1.2 6025551212`
   - ❍ **C.** `dialer map 6025551212 10.1.1.2 broadcast`
   - ❍ **D.** `dialer map ip 10.1.1.2 6025551212 broadcast`

5. Which of the following commands would show communication messages between the two ISDN router TE-1 devices?

   - ❍ **A.** `debug dialer`
   - ❍ **B.** `debug q921`
   - ❍ **C.** `debug isdn q921`
   - ❍ **D.** `debug isdn q931`

6. Which of the following commands takes a T1 controller and dedicates all the channels to an ISDN PRI connection?

   - ❍ **A.** `Router(config)#pri-group timeslots 1-2`
   - ❍ **B.** `Router(config)#pri-group timeslots 0-23`
   - ❍ **C.** `Router(config-controller)#pri-group timeslots 0-23`
   - ❍ **D.** `Router(config-controller)#pri-group timeslots 1-24`

7. You have entered the following configuration on your router:

```
Router(config)#access-list 150 permit tcp any any eq 23
Router(config)#dialer-list 1 protocol ip list 150
Router(config)#interface bri 0
Router(config-if)#dialer-group 150
```

   One of your internal PCs attempts to telnet to a remote site using the BRI 0 connection. What happens?

   - ❍ **A.** The DDR connection dials because of the correct interesting traffic being seen.
   - ❍ **B.** The telnet traffic drops a few packets while the ISDN line is initiating, and then successfully connects to the other side.
   - ❍ **C.** Telnet traffic is implicitly denied over ISDN connections regardless of access list configuration.
   - ❍ **D.** The router does not dial a connection and the telnet traffic is dropped.

8. Which command would be used to activate additional B-channels when the interface load passes a certain amount?

   - ❍ **A.** `dialer-group`
   - ❍ **B.** `ppp multilink`
   - ❍ **C.** `dialer load-threshold`
   - ❍ **D.** `dialer interface`

9. You have entered the following configuration on your router:

```
Router(config)#access-list 150 deny tcp any any eq 23
Router(config)#access-list 150 deny tcp any any eq 25
Router(config)#access-list 150 permit ip any any
Router(config)#dialer-list 1 protocol ip list 150
```

   What traffic would trigger a DDR call?

   - ❍ **A.** Any IP traffic
   - ❍ **B.** Only telnet and SMTP
   - ❍ **C.** Any IP traffic except FTP and telnet
   - ❍ **D.** Any IP traffic except telnet and SMTP

10. Which of the ISDN verification commands shows you the status of the bottom three layers of the OSI model as they relate to your ISDN connection?

    - ❍ **A.** `show dialer`
    - ❍ **B.** `show isdn events`
    - ❍ **C.** `show isdn q931`
    - ❍ **D.** `show isdn status`

Answers to Review Questions

1. B-channels (short for bearer channels) are used to carry data traffic and offer 64Kbps for each channel. The D-channel (short for delta channel) is used to carry signaling information. Depending on the type of ISDN connection you are using, it could be 16 or 64Kbps.
2. The two types of ISDN BRI interfaces you can purchase are the U and S/T interfaces. The U interface is used in the United States and Japan, whereas the S/T interface is used on all other continents.
3. Use the command `debug isdn q921` to focus on the router-to-service provider communication. The command `debug isdn q931` is used to troubleshoot end-to-end connectivity.
4. When configuring DDR, first define static routes that inform the router about the networks it can reach over the DDR connection. You can then use a dialer list to define the interesting traffic that is able to initiate the DDR connection. Finally, you need to create dialer maps that dictate the numbers to dial to reach the remote IP addresses.
5. You can use a dialer profile configuration with ISDN interfaces any time you'd like. However, these configurations are usually applied when the ISDN either makes calls to different destinations or receives calls from different sources. The dialer profile can then change the logical configuration of the ISDN interface, based on the remote router configuration.

Answers to Exam Questions

1. **A.** Basic Rate Interface (BRI) connections provide 128Kbps throughput for data by using two B-channels and a single 16Kbps D-channel. Answer B is incorrect because Primary Rate Interface (PRI) provides 23 B-channels. Answer C describes a configuration that can dial connections when needed. Answer D is not a valid ISDN technology acronym.

2. **C.** The status of the D-channel is shown as Interface Up, Line Protocol Up (Spoofing) during normal operation. The spoofing command is unique to ISDN connections. It implies that the D-channel is connected (as it always should be), but the B-channels may or may not be active. Answers A and B are seen only if the D-channel is experiencing some problem in communicating with the service provider.

3. **C.** The Terminal Endpoint, Type 1 is an ISDN-compatible device, which is exactly what a Cisco router equipped with any ISDN interface would be considered. Answer A is incorrect because an NT-1 device converts from the two wires provided by the ISDN service provider to a four-wire internal connection. Although the U interface comes equipped with an NT-1 built in, this does not change the fact that the Cisco router is still considered a TE-1. Answer B represents an ISDN PBX-like device. Answer D indicates a non-ISDN compatible endpoint, such as a PC. And finally, Answer E is a device used to adapt a TE-2 device to work with an ISDN connection.

4. **A.** The correct syntax of the `dialer map` command is `dialer map <protocol> <remote_address> <options> <phone_number>`. All the other answers use invalid syntax. Answer D is close, but after you type in the phone number, the Cisco router does not allow you to add any more options.

5. **D.** The `debug isdn q931` command watches Layer 3 communication between the two router endpoints connected to the ISDN service provider (aka TE-1). Answers A and C are incorrect because they watch communication between the TE-1 device and the local service provider. Answer B uses invalid syntax.

6. **D.** The `pri-group` command is issued under T1 controller configuration mode. It tells the Cisco router which B-channels it should use (in case the PRI connection was de-multiplexed earlier in the physical connection). The numbering for the timeslots begins counting from 1 and goes up to 24. Answers A and B are issued from the wrong configuration mode and Answer C begins counting from zero.

7. **D.** This question is scandalous because the entire configuration is correct up to the `dialer-group` command. The `dialer-group` command should reference dialer-list 1; however, it mistakenly references access-list 150, which is not possible. If the `dialer-group` command was correctly configured, Answer A and Answer B would both be correct. Answer C is totally bogus because ISDN connections allow telnet traffic just fine.

8. **C.** The `dialer load-threshold` command is used to activate the Cisco Bandwidth on Demand (BOD) enhancement to Multilink PPP. Answer A is incorrect because the `dialer-group` command is used to define interesting traffic on an interface. Answer B is incorrect because PPP Multilink is used to bundle together multiple B-channels, but does not have the capability to enable additional B-channels as interface load increases. Answer D is incorrect because dialer interfaces are used to set up multiple dialer profiles for a connection.

9. **D.** Because the access list denies SMTP (port 25) and telnet (port 23) traffic, these traffic types cannot bring up a DDR connection. This does *not* mean that these traffic types cannot be sent after a DDR connection is established. All the other answers are wrong.

10. **D.** The `show isdn status` command is one of the quickest ways to find problems with your ISDN connection because it shows the status of each layer of the ISDN connection. Answer A is incorrect because the `show dialer` command just shows the ISDN information as it relates to the DDR configuration. Answers B and C produce invalid syntax.

Suggested Reading and Resources

1. Cisco TAC Configuring ISDN BRI, http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca71c.html.

2. Ward, Chris and Cioara, Jeremy. *Exam Cram 2 CCNA Practice Questions*. Que Publishing, 2004.

3. Bokotey, Dmitry, et al. *CCNP Practical Studies: Remote Access (CCNP Self-Study)*. Cisco Press, 2004.

CHAPTER 17

Frame Relay

Objectives

Describe the terminology associated with packet-switched networks and Frame Relay

Understand the design strategies of a Frame Relay network

Configure Frame Relay in a point-to-point and multipoint environment

Verify Frame Relay configuration and operations

- Packet-switched networks are a completely different breed of WAN connection when compared to the leased-line variety. To fully understand these networks, you must fully understand a new group of terms and concepts.
- The proper design of a Frame Relay network rests heavily on a company's budget and desired redundancy level. This chapter presents a variety of design strategies that can fit these varying requirements.
- When moving into the configuration of a Frame Relay network, you can choose to employ a point-to-point or multipoint design. Each configuration offers its own advantages and disadvantages.
- This chapter discusses the commands used to troubleshoot and ensure correct operation after the Frame Relay connection has been configured.

Outline

Study Strategies

- Read the information presented in the chapter, paying special attention to tables, Notes, and Exam Alerts.
- Spend as much time as you find necessary on the terms and concepts of Frame Relay. After you fully understand the operation, the configuration is not very difficult.
- Although configuration questions may exist, the CCNA exam typically focuses on the concepts behind Frame Relay, with many of the configurations reserved for the CCNP BCRAN exam.

Introduction

Up until now, most of the WAN connection types discussed so far have provided dedicated bandwidth. For example, if you purchase a point-to-point leased-line connection at a T1 speed, you have 1.544Mbps at your disposal, 24 hours a day. This bandwidth is there regardless of whether you use it or not. Likewise, if you are using a ISDN BRI connection and dial the line up, you have 128Kbps of bandwidth at your disposal. Your network might not choose to send a single packet across the line; regardless, the 128Kbps of bandwidth sits there waiting. But with Frame Relay (and packet-switched networking, in general), the service providers had a novel idea: If you're not using your bandwidth, should it just sit there? I think not.

Welcome to the world of Frame Relay, the first connection type where lightning-bolt WAN links terminate into some sort of fluffy cloud rather than going directly to another router. This is a place where your destination address is not actually at the destination, but rather, terminates at the source. With Frame Relay, the bandwidth you pay for might just be the beginning of the bandwidth you get. Yes, my friends, you have entered the WAN Link Twilight Zone.

Frame Relay Overview

Frame Relay is by far the most conceptually complex topic in the CCNA-level material. Much as with subnetting, though, after you get it, you'll think it's the greatest thing since sliced bread. However, until you get to that point, you'll probably think people that use Frame Relay are insane. Unfortunately (or fortunately, depending on your perspective), Frame Relay is one of the most popular WAN connection types in use in production networks. It offers the high speed demanded by the networks of today at cut-rate prices that managers love.

Frame Relay connections work quite differently than the typical WAN connections discussed thus far. Rather than have a single connection from a location to another location (also known as point-to-point), you might have a connection going from one location to five other locations out a single, physical serial interface. You start to get the feel that this is an ethernet-style connection where any device connected to a hub can reach any other device plugged into the same hub. Depending on your Frame Relay configuration, this may not be far from the truth. Rather than connect sites together through individual physical interfaces, Frame Relay connects sites together with virtual circuits.

Virtual Circuits

Virtual circuits are logical links through service provider networks that give routers the impression that they are linked directly together. Take a look at Figure 17.1. You have a router on each side of the service provider cloud, connected through a virtual circuit, signified by a

dotted line through the cloud. These routers believe they are connected directly together (as if the cloud weren't there). You could even do a `traceroute` command between these routers and it would show only a single hop. However, if you peeled back that cloud, you would find that these routers are nowhere near directly connected. They would be going through many service provider routers, through many different networks. Truth be told, the technology underneath that Frame Relay cloud probably isn't even Frame Relay. When a frame gets sent through that cloud, its headers are most likely stripped and replaced many times; it's shaken, stirred, and spun around. But by the time it reaches the other end of the virtual circuit, the original Frame Relay headers are placed back on and a dazed and confused packet walks out of the cloud reporting that it traveled only a single hop between the source and the destination. For now, it's best to say that what happens in the cloud, stays in the cloud. Unless you're a service provider, this is how most network administrators prefer to leave it.

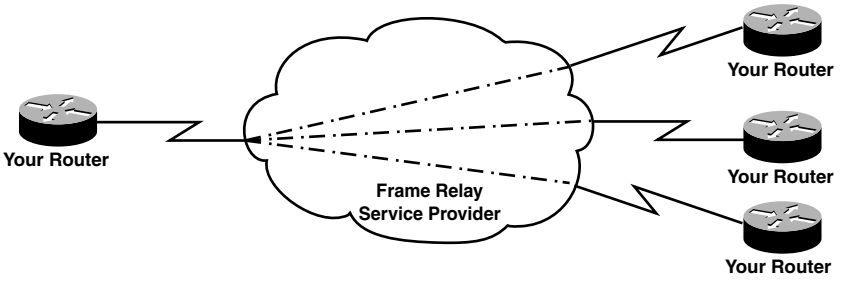


FIGURE 17.1 Typical Frame Relay network diagram.

Although you aren't concerned with what happens within the cloud, you do need to understand the circuits that ride over the cloud. These virtual circuits define the devices you are able to reach. The more virtual circuits you purchase to connect your various locations, the more redundant the connections will be; at the same time, the monthly cost will rise significantly. Therefore, there are three major design strategies to provisioning Frame Relay virtual circuits.

Hub and Spoke Design

Every network looks for cost efficiency. Redundancy is often sacrificed on the altar of monthly cost. Thus, the hub and spoke Frame Relay network design is one of the more common. In this configuration, you pick a centralized location (most likely, your largest, most connected office) as the "hub" of the network. All other locations are considered "spokes" and have a single virtual circuit connection back to the hub. Figure 17.2 gives a visual of what this looks like.

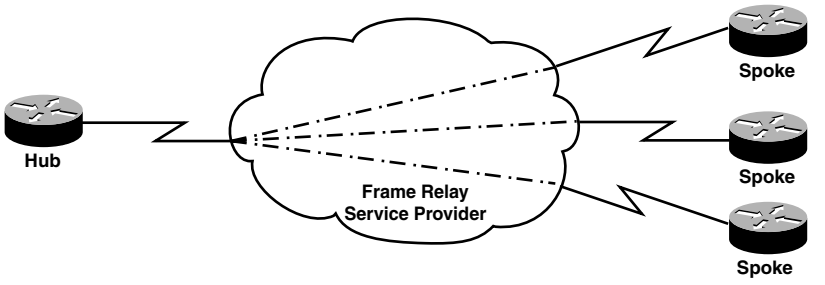


FIGURE 17.2 Hub and spoke Frame Relay design.

Initially, it appears as though the spoke offices will be unable to reach each other. However, you can configure them to traverse through the hub location if they ever need to communicate. Typically, in this network design, the spoke offices rarely communicate with each other. Rather, they access servers, store information, send email, and so on through the hub office.

The major advantage of this configuration is the cost. It offers the cheapest monthly price tag, which cost-cutting corporations enjoy. The disadvantages are beginning to mount against this design, however. The redundancy is sorely lacking. If a single router (the central router) loses connectivity for any reason (if the router crashes, if a trenching company cuts through the line), your entire WAN goes down. The other disadvantage of this design is beginning to eclipse even redundancy. It is the disadvantage of tandem switching. Any time the spoke offices need to reach each other, they must go through the hub office. This is considered a *tandem switch*. Tandem switching takes time and adds delay for the end-to-end connection. Up until modern times, this was no big deal; file transfers between spoke offices would just move a little slower. One technology has pushed tandem switching from a priority level of "No big deal" to "Heaven help us, the sky is falling." That technology is Voice over IP (VoIP).

VoIP technology involves moving the telephone system from running on its own network to using the data network as a backbone for communication. VoIP has very strict delay requirements that can be easily exceeded anytime sources of delay (such as a tandem switch) are introduced. Now, anytime employees working in the spoke offices call each other (which happens quite a bit more frequently than file transfer), the call quality may sound like a bad cell phone call. Therefore, most companies that are looking to move into a VoIP environment typically redesign their Frame Relay network to minimize the number of tandem switches that occur.

Partial Mesh Design

You can think of the partial mesh Frame Relay design as the compromise between network administrators and cost-saving managers. In this configuration, key sites have redundant virtual circuit connections through the cloud, as shown in Figure 17.3.

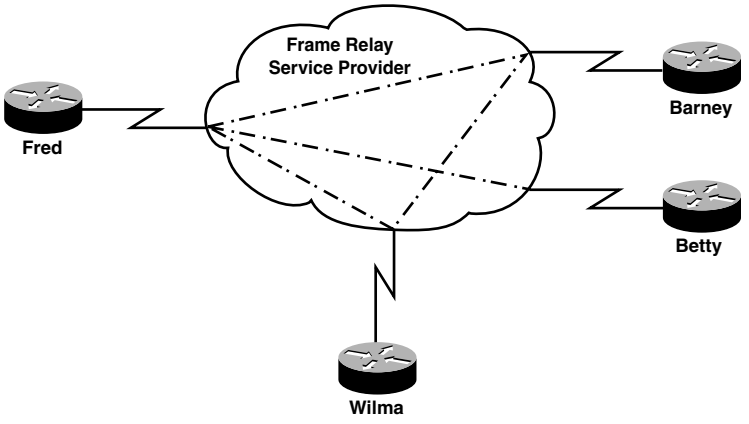


FIGURE 17.3 Partial mesh Frame Relay design.

This gives them a level of redundancy and minimizes the number of tandem switches required for them to communicate. Less critical locations have fewer virtual circuit connections, which keeps the cost lower.

Full Mesh Design

If the partial mesh design is a compromise between the network administrators and managers, then the full mesh design implies that the network administrators won. This design is every Cisco network administrator's picture of perfection over a Frame Relay cloud. It gives every site a direct virtual circuit to every other site, as shown in Figure 17.4. This design gives maximum redundancy and minimum packet latency (latency describes how long it takes a packet to reach each location). Of course, this type of service comes at a cost, the highest cost of all Frame Relay network designs.

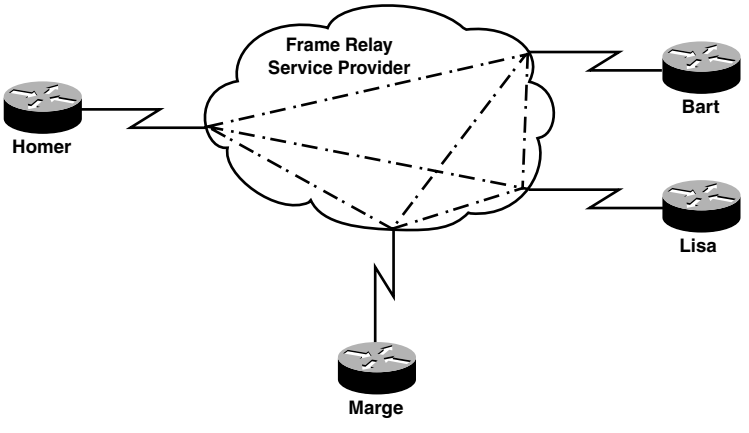


FIGURE 17.4 Full mesh Frame Relay design.

Frame Relay Terminology

As with most Cisco concepts, you'll find that the configuration piece of Frame Relay is fairly simple; the difficulty appears when you try to understand the concepts behind the configuration. Frame Relay introduces a plethora of new terms that describe the end-to-end communication. The first term you have already seen: a virtual circuit. You'll now find out that there are two types of virtual circuits.

Permanent Virtual Circuit

A permanent virtual circuit (PVC) is a permanently established circuit through the Frame Relay service provider network. It enables the routers at each end to communicate with each other without any setup process. A PVC closely emulates a leased-line connection between your devices.

Switched Virtual Circuit

A switched virtual circuit (SVC) gives you an "on-demand" connection through the Frame Relay cloud. The connection from end-to-end is built as the routers require it and may be billed on a usage basis (very much like ISDN connections). SVC connections have largely decreased in use in recent years (almost to the point of non-existence) because service providers no longer have true end-to-end Frame Relay connections, but rather, convert from Frame Relay to some other network type after you transmit data into the cloud. If this seems odd, remember: What happens in the cloud, stays in the cloud.

Local Management Interface

The local management interface (LMI) signaling is the "language of love" between your router and the service provider. Using LMI, the service provider can transmit status information about the state of your virtual circuits to your router. In recent versions of the IOS, your router can auto-detect what LMI language the service provider uses. In older IOS versions, this must be manually configured under the interface.

Data Link Connection Identifier

It is a little known fact that router serial interfaces do not have MAC addresses. MAC addresses are related only to LAN connections. WAN connections therefore all have different Layer 2 addresses that they use to identify the other side of the connection. In the case of Frame Relay, this is known as a *Data Link Connection Identifier* (DLCI). Communicating through DLCIs is unlike most other network communication that you've seen thus far. Rather than

access a destination DLCI number to reach the remote router, you *leave on a local* DLCI number to reach a remote router. This is very similar to the way airline travel works. When you want to fly to a remote destination, say North Dakota, you might leave on flight #4513. When you want to return from North Dakota to your original location, you might leave on fight #4839. This means that the DLCI numbers you use are *locally significant*; the DLCIs you have in Arizona matter only to the router in Arizona. The DLCIs you have in North Dakota matter only to the router in North Dakota. Look at Figure 17.5 for a network diagram.

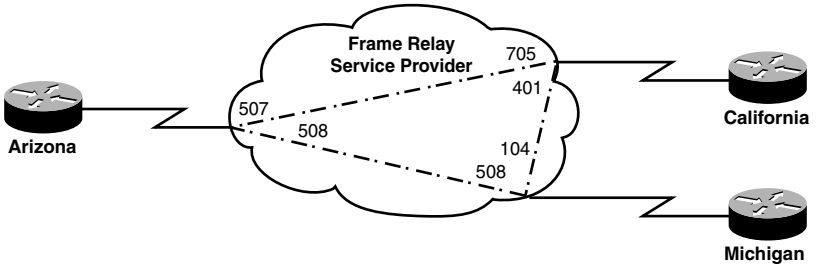


FIGURE 17.5 Frame Relay DLCIs.

Figure 17.5 shows a full mesh design with three locations: Arizona, California, and Michigan. At each location, the routers have two virtual circuits that enable them to reach the other locations. Now remember, the way DLCIs work is you leave on a local DLCI number rather than access a remote DLCI, so if Arizona wants to reach California, it uses DLCI number 507 to get there. If California wants to get back to Arizona, it uses DLCI 705. Likewise, California uses DLCI 401 to reach the router in Michigan.

Because DLCIs are locally significant, service providers can do whatever they want with them. Take a look at the DLCI connection between Arizona and Michigan. It's not a mistype! Arizona is assigned to use DLCI 508 to reach Michigan. Michigan also uses DLCI 508 to reach Arizona. This seems to make no sense until you realize that the DLCI number 508 means something totally different if it is received in Arizona than if it is received in Michigan. Remember: *locally* significant. The service provider probably has DLCI 508 in use in many locations for many different customers. As long as the set of DLCIs is unique at each location, everything is fine with the Frame Relay standards.

Local Access Rate

The Local Access Rate (commonly called the *line speed*) is the maximum physical speed that your Frame Relay connection can attain. Today's Frame Relay connections can usually reach up to T3 speeds (just over 44Mbps). This maximum can vary depending on the area in which you are and the service provider you are using. This does not define how fast your virtual circuits can travel. That's the job of the Committed Information Rate (which is covered next). However, the accumulation of all the bandwidth on all your virtual circuits can never exceed the router's Local Access Rate.

Committed Information Rate

With a Frame Relay connection, really just two things heavily affect the price of the connection: first, the number of virtual circuits you purchase, and second, the Committed Information Rate (CIR) for each one of those virtual circuits. The CIR is the minimum speed the service provider commits to give you for the circuit at all times. It's your guarantee. Typically, you get more bandwidth than what your CIR dictates, but if the service provider starts running thin on bandwidth allocations, it can contractually cut your location's virtual circuits down to the minimum amount of bandwidth defined by your CIR.

Now here's the major concept: Each PVC you purchase has its own CIR. This can be mind-boggling because you just learned about the Local Access Rate, which defines the maximum physical speed of the connection. Frame Relay enables you to divide up your connections, assigning a CIR for each PVC destination. Take a look at Figure 17.6.

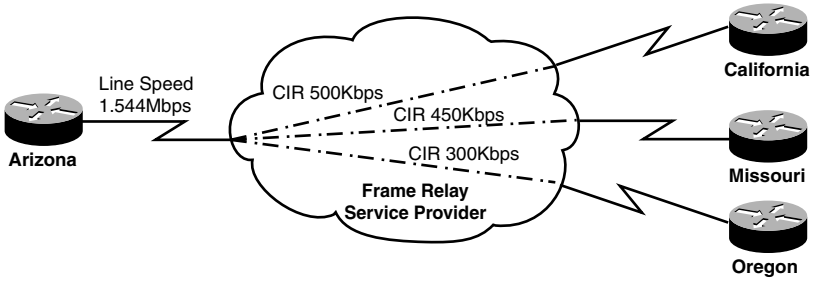


FIGURE 17.6 Frame Relay CIR.

You now have a hub and spoke Frame Relay design where Arizona is connected to California, Missouri, and Oregon. Focus for the moment on Arizona: The Local Access Rate is shown as T1 speed—1.544Mbps. Each PVC has its own CIR: The PVC to California is rated at a CIR of 500Kbps, the PVC to Missouri uses a CIR of 450Kbps, and the connection to Oregon uses a 300Kbps CIR. Notice that the total bandwidth of all the PVCs does not exceed the Local Access Rate of the line. Remember, the CIR is the minimum amount of bandwidth the service provider gives you. If you oversubscribe your Local Access Rate with the sum of all the CIRs, you may be physically limiting how much bandwidth the service provider would be willing to give you (and paying too much for your connection).

Many service providers offer extremely low-cost Frame Relay connections that are rated at a zero CIR. This means that you'll probably get bandwidth, but the service provider does not guarantee anything. When signing up for one of these connections, be sure to use a reputable service provider because some of the smaller service providers may be oversubscribing their network with these connections and not have enough bandwidth to give you a reliable connection.

Backwards Explicit Congestion Notification

Because service providers allow you to burst above your CIR (using more bandwidth than you're paying for), you have the potential of taking advantage of the service provider. If not configured differently, your router will attempt to send across all PVCs at the maximum speed the physical interface can handle (your Local Access Rate). If there is a large mismatch between your CIR and the Local Access Rate, your PVC will soon begin to become congested. The service provider will send messages to the router sending the large amount of traffic attempting to tell it to slow down. This is known as a Backwards Explicit Congestion Notification (BECN) message. The method the service provider uses to send this notification is important to understand.

Because of the way PVCs are engineered, the service provider cannot communicate directly to the router sending the data. Instead, it modifies the headers of return traffic to notify the person sending the excessive amount of data. For example, imagine that you were sitting at the Arizona location (from the prior Figure 17.6) transferring a large file to the California location via FTP. The entire time you are sending this file, the California site is sending TCP Acknowledgments (ACKs) back to confirm the data receipt. If the Arizona site is excessively exceeding the CIR, the service provider flips a bit (known as the BECN bit) in the header of the ACK messages to notify the sender that it needs to slow down.

By default, your Cisco router ignores the BECN message (what audacity!). It does so because BECN response falls under a major configuration called Frame Relay Traffic Shaping, which you'll learn plenty about if you decide to continue on into the CCNP courses. It is to your advantage to drop your speed when you receive a BECN message because the service provider will soon thereafter liquidate the vast majority of your traffic in the Frame Relay cloud, causing drastic performance reductions.

Forwards Explicit Congestion Notification

This one is one of the most misunderstood of all Frame Relay terms. After you understand the concept of a BECN, it seems logical to assume a Forward Explicit Congestion Notification (FECN) tells the receiving side of the connection to slow down. This is not true at all. Why would a Frame Relay service provider tell the *receiver* to slow down? It is not sending any traffic, just receiving it. Instead, a FECN message is used to tell the receiver to generate traffic that the service provider can tag with a BECN to tell the sender to slow down. I'm sure you're thinking, "What?!?" Here's an example.

Again, you have a device in Arizona sending traffic to the California location. This time, they are sending an enormous video stream (which uses UDP communication). UDP requires no acknowledgments, so the service provider has no return traffic to mark as a BECN to tell the sender to slow down. Instead, it tags some of the traffic heading to the receiver. This is known as a FECN (it uses the same bit in the header as the BECN, but is interpreted as a FECN

because it is sent the other way). If the receiving router is configured to support FECNs, it generates some "junk" (called a Q.922 test frame), puts it in a frame, and sends it back to the sender. The junk in the packet is really junk. The sending router in Arizona drops it after it is received. All it's there for is to give the service provider something to tag to tell Arizona to slow down. So, a FECN message is just a method to generate some traffic so the service provider can send a BECN.

Discard Eligible

This term describes any traffic that you send above the CIR you have purchased. Because you are using bandwidth that you did not pay for, the service provider automatically tags your packets as Discard Eligible (written as D_e—that's *D* subscript *e*). Just because a packet is marked D_e doesn't mean it will be discarded. Most the time it make it across the Frame Relay network just fine. What the D_e marking means is if the service provider experiences congestion, guess which packets are the first to go—yep, the packets tagged as D_e.

When you get deeper into Frame Relay traffic shaping (later in your Cisco career), you'll discover that there's a way to mark your own traffic D_e. This enables you to be selective with what traffic is marked D_e rather than use the random selection of the service provider. This can keep your high-priority traffic from being sent above the CIR.

The Nature of NBMA Networks

Frame Relay networks fall under the umbrella of Non-Broadcast Multi-Access (NBMA) networks. As the name implies, these networks allow multiple devices to access the network, but do not allow broadcast between them. Although this is their default behavior, you can configure your Cisco router to treat the network however you'd like. Because NBMA networks allow traffic between only the sites for which you purchase PVCs, this leads to some very odd configurations. The hub and spoke topology can be very confusing to manage until you understand the problems associated with these network types.

One of the major problems that can be encountered is that of running distance vector routing protocols over a Frame Relay network. These routing protocols (which include RIP, IGRP, and even EIGRP) have a built-in loop prevention mechanism called *split-horizon*. This mechanism prevents a router from sending an update out the same interface as that on which it received an update. Figure 17.7 shows where the problems begin with the default Frame Relay configuration.

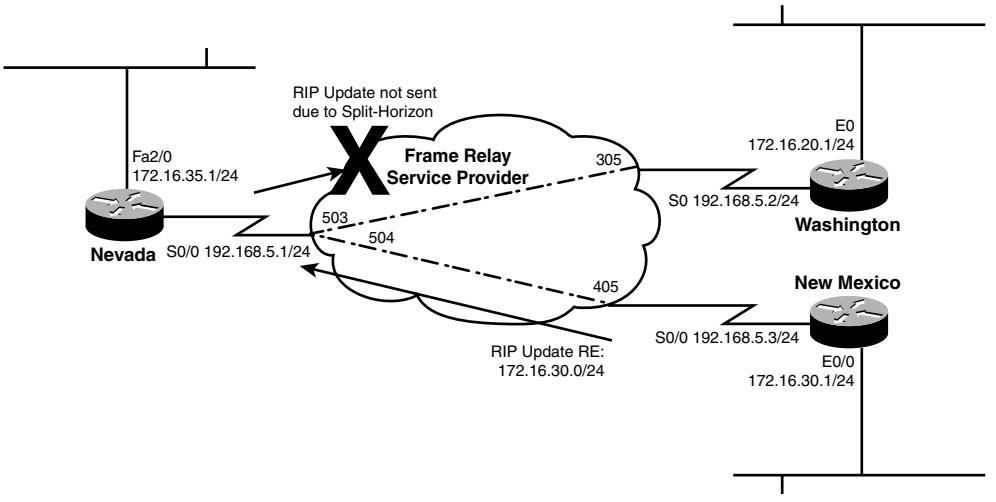


FIGURE 17.7 Split-horizon issues in Frame Relay networks.

This figure shows a typical hub and spoke configuration between Nevada, Washington, and New Mexico. Because this network is so simple, this company has decided to use the RIP routing protocol. Here's how the problem starts: New Mexico sends an RIP routing update to Nevada regarding its 172.16.30.0/24 network. Nevada receives the update coming in its S0 interface. Now the spilt-horizon rule steps in and tells the Nevada router not to send that routing update back out the interface on which it was received. Washington never hears about the 172.16.30.0 network through the RIP protocol and is unable to access any devices at that location. The same thing goes for the Washington network. The advertisement reaches the Nevada router, but is never sent to New Mexico because of the split-horizon rule.

Two methods are used to solve this problem. First, you can disable the split-horizon mechanism altogether. This is a risky move because you are then relying on the other loop prevention mechanisms to keep a loop from happening in the network. The second method is to use subinterfaces.

EXAM ALERT

Know the terminology behind Frame Relay. Especially ensure you understand the CIR and DLCI concepts.

Subinterfaces

Using subinterfaces to solve your split-horizon problem is the best way to go. Subinterfaces enable you to break your single, physical interface into multiple, logical interfaces. You still

have only a single physical connection to the Frame Relay service provider, however, your router sees it as multiple connections. There are two categories of Frame Relay subinterfaces: point-to-point and multipoint. Only the point-to-point interface type is designed to fix the split-horizon issue by creating a subinterface for each PVC connection. However, because we're talking about subinterfaces, it would be a good idea to talk about multipoint as well.

Multipoint Subinterfaces

Forgive me for allowing my opinion to get in the way of a neutral CCNA book, but multipoint interfaces are about as useful as a squirt gun for a scuba diver. This subinterface type enables you to have multiple PVCs terminating under a single, logical subinterface. This type of subinterface is how a physical interface behaves if no subinterfaces are created. It still encounters the same split-horizon issues, forcing you to disable split-horizon. You might wonder, "How is this type of subinterface helpful then?" Like I said…squirt gun for a scuba diver. Multipoint subinterfaces can be useful in other, non–Frame Relay deployments, but in Frame Relay they cause more trouble than anything.

Point-to-Point Subinterfaces

This subinterface type enables you to logically design your Frame Relay network as a series of point-to-point connections, no matter how complex your PVC configuration may be. Each PVC circuit is assigned to a single, point-to-point subinterface. This solves the split-horizon issue without much intervention from you because the Cisco router now sees each PVC as its own interface. For example, if a routing update is received on Serial 0, split-horizon blocks that update from being sent back out Serial 0. After you configure point-to-point subinterfaces correctly, the router sees an update come in on one of the subinterfaces, such as Serial 0.10. It has no problem sending that update out another subinterface, such as Serial 0.20, because it sees these interfaces as two, distinct ports.

Address Mapping in Frame Relay

Frame Relay functions at the Data Link layer of the OSI model. It provides services for the WAN just as ethernet provides services for the LAN. Because everything we do today typically relies on IP addresses, Frame Relay needs to have a way of mapping its Data Link layer address (a DLCI) to a Network layer address (typically an IP address). For example, your router may know that it can reach some location through DLCI 505, but DLCI 505 doesn't really mean anything to your router. Your router works with IP addresses, not DLCI numbers. So to allow DLCI 505 to mean something, your router needs to somehow map this to the IP address that DLCI 505 can reach. There are two methods you can use to accomplish this: Inverse ARP and static mappings.

Inverse ARP

Inverse ARP is the router's automated method to map DLCIs to IP addresses. It works as follows:

1. You connect your router to the Frame Relay service provider through a serial interface.
2. The service provider uses LMI to identify your router and send your router a list of DLCIs it can use to reach your remote sites.
3. Your router sends Inverse ARP messages to each one of these DLCI numbers. This Inverse ARP message carries the simple message, "Hello DLCI! Please send your IP address."
4. The remote router receives the message and responds with its IP address.
5. Your router maps the DLCI number to the IP address it received.

The router sends these Inverse ARP messages to each DLCI number it has received until it has a complete mapping table of DLCI numbers to IP addresses. All along, you as the administrator have done…nothing! This is a completely automated process that makes the Frame Relay setup seamless for small environments. The only drawback to this method is it does not work for subinterfaces. For Inverse ARP to function properly, you must leave all assigned DLCIs under the physical interface, which causes this interface to become a multipoint interface (if you have multiple DLCI numbers). As you have already seen, multipoint interfaces have problems with split-horizon.

Static Mappings

The alternative to allowing Inverse ARP to automatically configure your environment is to use static maps. This method is also specific to multipoint-style interfaces. Using this method, you can manually enter the DLCI to IP address mapping for each PVC. This gives you complete control over the mapping process and enables you to have more than one interface (unlike Inverse ARP). The specifics of this configuration, along with the considerations for point-to-point interfaces, are covered later in this chapter.

EXAM ALERT

Know what the differences are between Inverse ARP Frame Relay configuration and static mappings.

Configuring Frame Relay

Configuring Frame Relay can be very simple or slightly complex, depending on your network requirements and design. I'd like to walk you through three configuration scenarios, explaining step-by-step how each piece is configured. By time you're finished here, you'll be a Frame Relay expert. The three configuration scenarios are as follows:

- Configuring Frame Relay for a single neighbor
- Configuring Frame Relay that uses a multipoint interface
- Configuring Frame Relay that uses a point-to-point interface

Configuring Frame Relay for a Single Neighbor

This configuration is the simplest one to set up for Frame Relay. Because the router does most of the work for you in this configuration, many people call this a *Frame Relay auto-configuration*. It is helpful to walk through this configuration step-by-step, first looking at Figure 17.8.

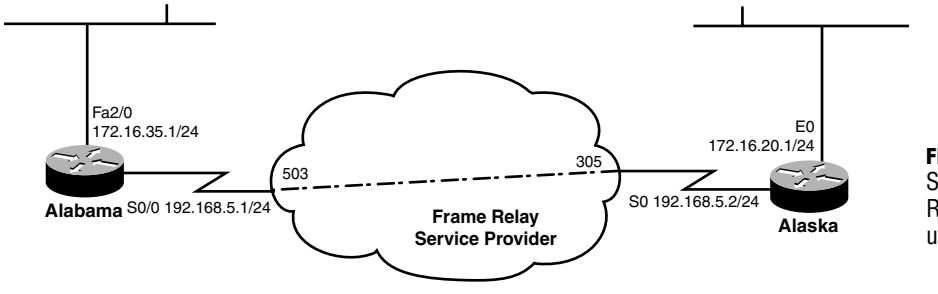


FIGURE 17.8 Simple Frame Relay configuration.

There are two locations in this scenario: Alabama and Alaska. This configuration is really a point-to-point style connection, we're just going through a Frame Relay cloud to accomplish it. Alabama uses DLCI 503 to reach Alaska, and Alaska uses DLCI 305 to reach Alabama. You've already configured the necessary IP addresses for the network requirements; all that's left to do is configure the Frame Relay connection. Let's have at it!

Step 1: Turn on Frame Relay Encapsulation

Start on the Alabama router to get familiar with your surroundings:

```
Alabama#show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
Serial0/0          192.168.5.1     YES manual administratively down down
Serial0/1          unassigned      YES unset  administratively down down
Serial0/2          unassigned      YES unset  administratively down down
```

```
Serial0/3          unassigned      YES unset  administratively down down
FastEthernet2/0    172.16.35.1     YES manual up                    up
```

It looks as though the Fast Ethernet interface is up and running, and the Serial 0/0 interface has an IP address, but needs a little work beyond. First turn on the Frame Relay encapsulation:

```
Alabama#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Alabama(config)#interface serial 0/0
Alabama(config-if)#encapsulation frame-relay ?
  ietf  Use RFC1490/RFC2427 encapsulation
  <cr>

Alabama(config-if)#encapsulation frame-relay
Alabama(config-if)#
```

Take a look at this. When you access the Serial interface and type **`encapsulation frame-relay ?`**, you are given the option of either hitting the Enter key or adding the `ietf` keyword after the command. If you just press the Enter key, the router uses Cisco proprietary Frame Relay encapsulation. The Cisco proprietary version of encapsulation came out before the industry standard (`ietf`) Frame Relay encapsulation and uses a slightly different method for identifying the Layer 3 protocol (IP, IPX, and so on) that is being encapsulated. This makes it incompatible with the industry standard Frame Relay encapsulation. What it boils down to is this: If you are connecting two Cisco routers over a Frame Relay network, use the command `encapsulation frame-relay` to configure each side. If you are connecting your Cisco router to a non-Cisco device, use the command `encapsulation frame-relay ietf` to use the industry standard Frame Relay encapsulation.

EXAM ALERT

Be sure to know how to configure Frame Relay encapsulation between Cisco and non-Cisco routers.

The example wants to connect two Cisco routers, so you can use the Cisco proprietary encapsulation. Watch what happens when the Serial 0/0 interface on the Alabama router is brought up:

```
Alabama(config-if)#no shutdown
Alabama(config-if)#
*Mar  1 00:23:40.571: %LINK-3-UPDOWN: Interface Serial0/0,
➥changed state to up
Alabama(config-if)#
*Mar  1 00:23:51.571: %LINEPROTO-5-UPDOWN: Line protocol on Interface
➥Serial0/0, changed state to up
```

It looks like the interface has come up, so now it's time get out to privileged mode and verify that everything is working as expected. The first command you can use to check the connection is `show frame-relay lmi`. Remember, LMI (the Local Management Interface) is the language of love between you and your service provider. The service provider uses this language to send status messages, DLCI information, and line statistics to your local router. This is the lowest level of Frame Relay communication. If it is not working, nothing will be working.

```
Alabama#show frame-relay lmi

LMI Statistics for interface Serial0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 36               Num Status msgs Rcvd 35
  Num Update Status Rcvd 0              Num Status Timeouts 1
```

Focus on the key information here, which has been conveniently bolded for you. You can see that you have sent 36 status messages and received 35 messages. This is good. These numbers should be relatively equal and increasing on a steady basis. If the connection is failing, you will see the `Num Status Timeouts` field increment steadily. You can think of these messages as keepalives for your Frame Relay connection. Your router is saying "Hello" to the service provider (`Num Status Enq. Sent`) and the service provider is saying "Hello back" (`Num Status msgs Rcvd`). Now let's move up to the next level.

```
Alabama#show frame-relay pvc

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

               Active      Inactive      Deleted       Static
  Local           0             0             0            0
  Switched        0             0             0            0
  Unused          0             1             0            0

DLCI = 503, DLCI USAGE = UNUSED, PVC STATUS = INACTIVE, INTERFACE =
➥Serial0/0

  input pkts 0              output pkts 0             in bytes 0
  out bytes 0               dropped pkts 0            in pkts dropped 0
  out pkts dropped 0                  out bytes dropped 0
  in FECN pkts 0            in BECN pkts 0            out FECN pkts 0
  out BECN pkts 0           in DE pkts 0              out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  switched pkts 0
```

```
Detailed packet drop counters:
no out intf 0            out intf down 0          no out PVC 0
in PVC down 0            out PVC down 0           pkt too big 0
shaping Q full 0         pkt above DE 0           policing drop 0
pvc create time 00:09:59, last time pvc status changed 00:09:34
```

By using the `show frame-relay pvc` command, you can see all your virtual circuit connections over the Frame Relay cloud. Notice that none of this has been configured. The service provider actually sent the usable DLCI information to you with the LMI signaling! Your router (Alabama) received DLCI 503 from the service provider. Referring back to the network diagram in Figure 17.8, you can see that this is exactly the DLCI information you want to receive. But there seems to be a problem: The DLCI is marked as `INACTIVE`. This is where understanding the four PVC states can come in very handy:

- **Active**—A PVC marked as ACTIVE is successfully connected through between the two endpoints (routers). This is the normal state if everything is working properly.
- **Inactive**—A PVC marked as INACTIVE is working properly on your end of the connection (the local side); however, the other side of the connection is either not configured or offline.
- **Deleted**—A PVC marked as DELETED is having problems at your side (local side) of the connection. Most likely, you are attempting to use a DLCI number that the service provider has not configured.
- **Static**—A PVC marked as STATIC has been manually entered by you (the administrator) rather than dynamically discovered from the service provider.

EXAM ALERT

Understanding the states of a PVC can be quite useful in both the real world and the testing environment.

Whew! Quite a bit of information there applies directly to what you are seeing right now. Because the PVC is marked as INACTIVE, it means that your side (Alabama) is working just fine; it's the remote side (Alaska) that is having the problem. This is where you suddenly realize that you are not just the administrator in Alabama, but also the administrator for Alaska as well. You need to jump on a plane (or use a telnet connection) to reach the Alaska router and configure that side of the connection.

```
Alaska#show ip interface brief
Interface         IP-Address      OK? Method Status                Protocol
Ethernet0         172.16.20.1     YES NVRAM  up                    up
Ethernet1         unassigned      YES unset  administratively down down
Serial0           192.168.5.2     YES NVRAM  administratively down down
Serial1           unassigned      YES unset  administratively down down
```

It looks as if Alaska is in the same state as Alabama was when you first got involved in the configuration. Turn on Frame Relay encapsulation and power on the interface:

```
Alaska#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Alaska(config)#interface serial 0
Alaska(config-if)#encapsulation frame-relay
Alaska(config-if)#no shutdown
Alaska(config-if)#
00:26:42: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:26:53: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
➥changed state to up
00:28:42: %FR-5-DLCICHANGE: Interface Serial0 - DLCI 305 state
➥changed to ACTIVE
```

Take a look at that—the Line Protocol (data link connectivity) on the Serial interface came up and the DLCI 305 went ACTIVE. Now do the same verification commands you did on Alabama to see what things look like:

```
Alaska(config-if)#^Z
Alaska#show frame lmi

LMI Statistics for interface Serial0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 53               Num Status msgs Rcvd 54
  Num Update Status Rcvd 0              Num Status Timeouts 0
Alaska#show frame pvc

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 305, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

  input pkts 1             output pkts 1            in bytes 30
  out bytes 30             dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 1          out bcast bytes 30
  pvc create time 00:00:59, last time pvc status changed 00:01:00
```

Right on! The PVC status is now viewed as ACTIVE from the perspective of Alaska, which implicitly implies that Alabama is working as well (because ACTIVE indicates both sides of the connection are working as they should). So, hold your breath—now it's time to do the final

test: to ping from Alaska to Alabama, which acts as an end-to-end test of Network layer (Layer 3) connectivity:

```
Alaska#ping 192.168.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/60/60 ms
```

YES!!! That's exactly what you want to see. Five exclamation points indicating five successful, round-trip ping messages over the Frame Relay network. Isn't this exciting?

So let me summarize what it took to get a point-to-point Frame Relay connection running:

1. Turn on Frame Relay encapsulation.

That's it! Of course, there are some prerequisite steps, such as assigning IP addresses and turning on the interface. It may have seemed like a bigger process because of the verification commands that were performed. However, if you have just a single connection over the Frame Relay cloud, the service provider sends both sides of the connection their DLCI information through LMI signaling. The router then uses Inverse ARP messages to discover the IP address on the remote end of the connection. After the remote IP address is discovered, the router makes the connection between the local DLCI and remote IP address. Look at one `more` show command:

```
Alaska#show frame-relay map
Serial0 (up): ip 192.168.5.1 dlci 305(0x131,0x4C10), dynamic,
              broadcast,, status defined, active
```

From the Alaska router's perspective, you can see from using the `show frame-relay map` command that the router has mapped the Alabama router's IP address (192.168.5.1) to the local DLCI the Alaska router uses to reach that IP address (305). You can also see that this map was dynamically defined, which means that the Cisco router made this link between IP and DLCI numbers with Inverse ARP.

So the key to allowing Cisco routers to configure the Frame Relay connection themselves is to ensure the LMI is working correctly between your router and the service provider, which brings us to the closing point of this section.

If you are using an extremely old version of the IOS (any version earlier than 11.2), the router is unable to auto-detect what LMI language the service provider is using. This means you must manually configure it with the following syntax:

```
Router(config-if)#frame-relay lmi-type ?
  cisco
  ansi
  q933a
```

To determine which LMI signaling you should use, you need to contact your service provider.

EXAM ALERT

Be sure to know the LMI types and be able to pick them out of a line-up. It is also key to remember that "ietf" is a Frame Relay encapsulation type. IETF is *not* an LMI type.

Configuring Frame Relay That Uses a Multipoint Interface

Now, the scenario has expanded with the addition of another office to the mix. This change is reflected in Figure 17.9.

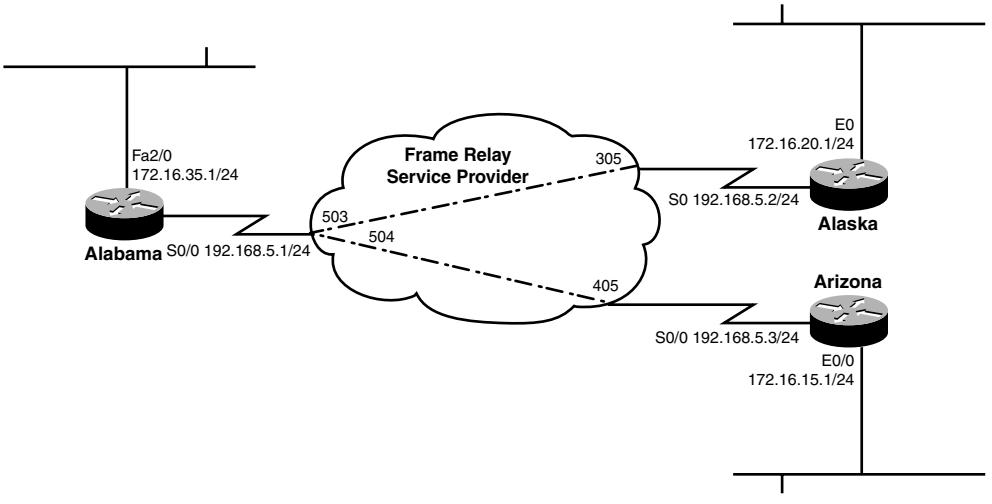


FIGURE 17.9 Frame Relay configuration with multiple locations.

The Arizona office has entered the picture and moved this story to a hub and spoke design. Alabama is the hub of the network, having PVC connections to both Alaska and Arizona. To save on cost, Alaska and Arizona are not directly connected and must use their PVC to Alabama anytime they would like to reach each other. Notice the IP addressing in this figure as well: All routers are configured on the same subnet (192.168.5.0/24) for their WAN connections. This IP addressing tells you that you are using a point-to-multipoint design. The routers think the WAN operates just like an ethernet network where all points connected to the network are able to reach all other points in the network. If you were using a point-to-point design (a much better design, in my humble opinion), each PVC would be on its own subnet, just as if you had point-to-point WAN links through the Frame Relay cloud. The point-to-point design is discussed a little bit later; for now, it's time to focus on making the point-to-multipoint design work successfully.

Configuring a multipoint interface can be done in two ways: You can either place the configuration under the physical interface itself or use a subinterface. Let me demonstrate. You've already done plenty of configuration on the physical interface, just by placing commands directly under the Serial interface. If you want to configure a subinterface, this is how the process looks:

```
Alaska#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Alaska(config)#interface serial 0.?
  <0-4294967295>  Serial interface number

Alaska(config)#interface serial 0.10 ?
  multipoint      Treat as a multipoint link
  point-to-point  Treat as a point-to-point link

Alaska(config)#interface serial 0.10 multipoint
Alaska(config-subif)#
```

In this case, the multipoint subinterface Serial 0.10 has been created. The subinterface number you choose is completely up to you. As you can see, you can use numbers from zero up to slightly more than 4 billion (Cisco is all about flexibility). In this case, I chose 10. If you were using this for your Frame Relay configuration, you could remove all commands from the physical interface (Serial 0) except for the `encapsulation frame-relay` command and place them under the subinterface. At this point, there's no real advantage to configuring Frame Relay with subinterfaces because you are using a multipoint configuration. After you get to point-to-point, you'll see the many advantages of this configuration. For now, you can save a little complexity and just configure everything under the physical interface.

If you had a full mesh Frame Relay design where every location had a PVC to every other location, this setup would take care of itself just like the previous configuration you saw. Each location would send an Inverse ARP message out on its PVCs and figure out how to connect to everyone else. However, if you look at the figure, you can see that there is no full mesh of virtual circuits. Alabama will work just fine in this design because it has PVCs to each location. Alaska and Arizona are going to have some problems if you just leave everything in its default configuration. The Inverse ARP message will be able to discover Alabama because it is directly at the end of the PVC; however, the Inverse ARP message does not "bounce through." Alaska does not discover Arizona and vice versa. This is where Frame Relay maps come in handy. You can manually configure each site by defining static maps dictating which DLCIs connect to each remote IP address. Even though it is not necessary to manually configure Alabama, it is a good practice not to mix dynamic and static configurations. If you want to use dynamic, it should be in use everywhere. Likewise, if you want to use static, use it everywhere. So the first thing to do is to configure the hub of the network, Alabama:

```
Alabama#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Alabama(config)#interface serial 0/0
Alabama(config-if)#frame-relay map ?
  bridge  Bridging
  ip      IP
  llc2    llc2

Alabama(config-if)#frame-relay map ip ?
  A.B.C.D  Protocol specific address

Alabama(config-if)#frame-relay map ip 192.168.5.2 ?
  <16-1007>  DLCI

Alabama(config-if)#frame-relay map ip 192.168.5.2 503 ?
  broadcast            Broadcasts should be forwarded to this address
  cisco                Use CISCO Encapsulation
  compress             Enable TCP/IP and RTP/IP header compression
  ietf                 Use RFC1490/RFC2427 Encapsulation
  nocompress           Do not compress TCP/IP headers
  payload-compression  Use payload compression
  rtp                  RTP header compression parameters
  tcp                  TCP header compression parameters
  <cr>

Alabama(config-if)#frame-relay map ip 192.168.5.2 503 broadcast
Alabama(config-if)#frame-relay map ip 192.168.5.3 504 broadcast
```

You've now statically mapped the DLCI numbers to the remote IP addresses. Remember, after you do this, you've overruled the Inverse ARP process; you are now taking the role of Inverse ARP under your belt. Look at the first static map: It tells the router, "If you would like to reach the *remote* IP address 192.168.5.2, use the *local* DLCI number 503." Likewise, the second line says, "To reach the *remote* IP address 192.168.5.3, use the *local* DLCI number 504."

It's also important to talk about the last option added to the syntax, `broadcast`. By default, your router treats the Frame Relay cloud just like the type of network it is: NBMA. Therefore, your routing protocols (which use multicast and broadcast traffic) will not work over a Frame Relay network. If you would like the router to forward broadcasts over the Frame Relay cloud, attach the `broadcast` keyword onto the end of the Frame Relay map.

You can also see from the context-sensitive help that you have many other options in addition to the `broadcast` keyword that you can add to the end of the Frame Relay map. Most of these options deal with the various flavors of compression that you can enable over the Frame Relay network if you wish. However, the other two highlighted options are of key importance. The keywords `cisco` and `ietf` define whether the remote router is a Cisco router or some other brand that uses the IETF industry-standard Frame Relay encapsulation. You might have noticed that neither command was entered under the `map` statement. The Cisco router uses the Cisco Frame Relay encapsulation by default. If you are connecting to non-Cisco routers, be sure to add the `ietf` keyword to the each map.

Now you can move on to the Alaska and Arizona routers:

```
Alaska#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Alaska(config)#interface serial 0
Alaska(config-if)#frame map ip 192.168.5.1 305 broadcast
Alaska(config-if)#frame map ip 192.168.5.3 305 broadcast

Arizona#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Arizona(config)#interface serial 0/0
Arizona(config-if)#frame map ip 192.168.5.1 405 broadcast
Arizona(config-if)#frame map ip 192.168.5.2 405 broadcast
```

Take a look at this: On the Arizona and Alaska routers, both remote IP addresses have been mapped to the same DLCI number. This is why you could not use Inverse ARP to solve this whole scenario: It would have detected only the directly connected neighbor—Alabama, in this case. Because I'm still sitting on the Arizona router, I perform the verification from there:

```
Arizona#show frame-relay lmi

LMI Statistics for interface Serial0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 1336             Num Status msgs Rcvd 1337
  Num Update Status Rcvd 0              Num Status Timeouts 2
  Last Full Status Req 00:00:23         Last Full Status Rcvd 00:00:23
```

It looks like the LMI information is being received successfully. Now examine the PVC status and mappings:

```
Arizona#show frame-relay pvc

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

               Active     Inactive      Deleted       Static
  Local           1            0            0            0
  Switched        0            0            0            0
  Unused          0            0            0            0

DLCI = 405, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
```

```
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:15:57, last time pvc status changed 00:00:20

Arizona#show frame-relay map
Serial0/0 (up): ip 192.168.5.1 dlci 405(0x195,0x6450), static,
              broadcast,
              CISCO, status defined, active
Serial0/0 (up): ip 192.168.5.2 dlci 405(0x195,0x6450), static,
              broadcast,
              CISCO, status defined, active
```

Based on the output from the `show frame-relay pvc` and `show frame-relay map` commands, it looks like DLCI 405 is ACTIVE and statically mapped to both the remote IP addresses it is able to reach. Because it tests round-trip connectivity, the final ping test verifies that the rest of the locations are configured correctly as well:

```
Arizona#ping 192.168.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms

Arizona#ping 192.168.5.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/117/124 ms
```

Take a look at that—successful pings everywhere! However, things are not as peachy as they may seem initially. Compare those round trip times for the two destinations. When the first ping was performed from Arizona to Alabama, the average round-trip response time was 58ms. The second ping went from Arizona to Alaska, and the round-trip response time effectively *doubled*, moving up to 117ms! Although the hub and spoke topologies are very cost effective, they can have devastating effects on delay-sensitive traffic, such as Citrix, Voice over IP, or Video over IP.

Now that the Frame Relay network is working correctly, it may be tempting to walk away cheering and feeling quite fantastic about the general state of your life. However, one more thing needs to be checked. Take a look again at Figure 17.8. Each location has a LAN connection, representing the offices in those locations. Although the Frame Relay network may be humming along, you still need to check the routing tables to ensure each one of these locations is able to reach the other. Behind the scenes, I've configured EIGRP for Autonomous

System 100 on each router, sending and receiving advertisements on all interfaces. Look at the routing table on Alabama first:

```
Alabama#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.35.0 is directly connected, FastEthernet2/0
D       172.16.20.0 [90/20537600] via 192.168.5.2, 00:00:35, Serial0/0
D       172.16.15.0 [90/20537600] via 192.168.5.3, 00:00:03, Serial0/0
C    192.168.5.0/24 is directly connected, Serial0/0
```

Whew! Everything looks good. As you can see, the highlighted output shows the Alabama router has learned about the networks in Alaska and Arizona just fine. Just to be certain of things, jump over to Arizona and verify the routing table over there.

```
Arizona#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 2 subnets
D       172.16.35.0 [90/2172416] via 192.168.5.1, 00:02:12, Serial0/0
C       172.16.15.0 is directly connected, Ethernet0/0
C    192.168.5.0/24 is directly connected, Serial0/0
```

Uh-oh. That warm, fuzzy feeling is slipping away. It appears that Arizona has learned about only the Alabama network, and is not showing Alaska in the routing table. It's a good idea to verify the Alaska routing table as well.

```
Alaska#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - default
       U - per-user static route, o - ODR
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 2 subnets
```

```
D       172.16.35.0 [90/2172416] via 192.168.5.1, 00:03:22, Serial0
C       172.16.20.0 is directly connected, Ethernet0
C    192.168.5.0/24 is directly connected, Serial0
```

Sure enough, Alaska is not learning about the Arizona network either. You have just experienced the split-horizon routing rule taking effect. The Alabama router is acting as the hub of the network. As it receives incoming routing updates on its Serial 0 interface from the Alaska and Arizona routers, the split-horizon rule jumps in and restricts the Alabama router's capability to send those updates back out of the interface on which it was received. There are two ways to solve this problem. First, you could move from a multipoint configuration to a point-to-point configuration (the safer, more preferred method), or disable the split-horizon routing rule completely (opening yourself up to the potential of routing loops). Remember, these routing rules have been put in place for a reason. Disabling them is like skydiving without a backup parachute. Most of the time, you should be fine, but just wait until that unusual situation. There may be very little chance of a safe landing.

Because this is a multipoint configuration, you can go ahead and disable the split-horizon features for now. The point-to-point solution is explained in just a moment. You need to be careful to disable split-horizon only at the key points of a network. If you disable it everywhere, you will most certainly end up with routing loops. In this case, you need to disable it at the network hub: Alabama. If you turn it off on this router, the routing updates will be received on the Serial 0 interface and sent right back out the same interface, allowing Arizona and Alaska to hear about each other. Here's how it's done:

```
Alabama#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Alabama(config)#interface serial 0/0
Alabama(config-if)#no ip split-horizon ?
  eigrp  Enhanced Interior Gateway Routing Protocol (EIGRP)
  <cr>
Alabama(config-if)#no ip split-horizon eigrp ?
  <1-65535>  Autonomous system number
Alabama(config-if)#no ip split-horizon eigrp 100
*Mar  1 00:45:29.507: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor
➥192.168.5.3 (Serial0/0) is down: split horizon changed
*Mar  1 00:45:29.507: destroy peer: 192.168.5.3
*Mar  1 00:45:29.507: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor
➥192.168.5.2 (Serial0/0) is down: split horizon changed
*Mar  1 00:45:29.507: destroy peer: 192.168.5.2
Alabama(config-if)#
*Mar  1 00:46:19.647: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor
➥192.168.5.2 (Serial0/0) is up: new adjacency
*Mar  1 00:46:38.111: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor
➥192.168.5.3 (Serial0/0) is up: new adjacency
```

You can see that turning off split-horizon for the EIGRP routing system caused the neighbors to reset themselves because of the configuration change. Now that they've come back up, you can verify the Alaska and Arizona routing tables:

```
Alaska#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - default
       U - per-user static route, o - ODR
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 3 subnets
D       172.16.35.0 [90/2172416] via 192.168.5.1, 00:02:12, Serial0
C       172.16.20.0 is directly connected, Ethernet0
D       172.16.15.0 [90/21049600] via 192.168.5.1, 00:02:12, Serial0
C    192.168.5.0/24 is directly connected, Serial0

Arizona#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 3 subnets
D       172.16.35.0 [90/2172416] via 192.168.5.1, 00:02:57, Serial0/0
D       172.16.20.0 [90/21049600] via 192.168.5.1, 00:02:33, Serial0/0
C       172.16.15.0 is directly connected, Ethernet0/0
C    192.168.5.0/24 is directly connected, Serial0/0
```

Excellent! The remote sites are now seeing each other's LAN connections in the routing table. The multipoint Frame Relay configuration is complete.

Configuring Frame Relay That Uses Point-to-Point Interfaces

I'm so excited! All this configuration has led up to this point: my highly suggested and preferred Frame Relay configuration, point-to-point subinterfaces. As you just saw, configuring Frame Relay using multipoint connections can be confusing because you have multiple, non–directly connected sites tied together through a single physical interface. In addition, it can cause some technical problems, primarily with routing protocols. Now, enter point-to-point subinterfaces into the configuration and these problems slowly melt away.

The configuration of point-to-point subinterfaces does require a little more work than multipoint because it requires you to create a logical subinterface for each PVC coming out of your locations. To explain this, let me introduce the next scenario to be configured. It involves setting up a network very similar to the previous, multipoint configuration. This time, a router known as Salmon will be the hub. BlueGill and Trout will act as the spokes. Take a look at the logical diagram in Figure 17.10.

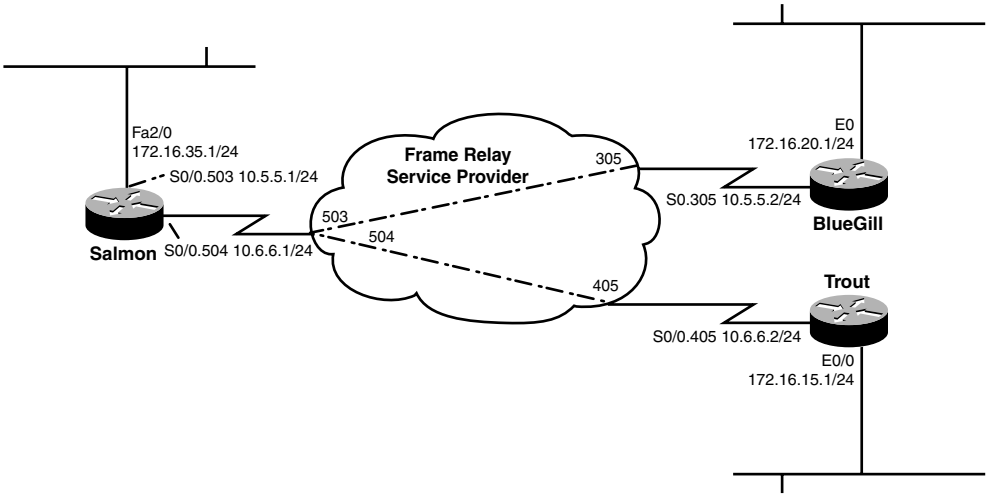


FIGURE 17.10 Point-to-point Frame Relay configuration.

Can you see the difference between the point-to-point and multipoint configurations at the hub router? Instead of having a single IP address and interface connected to the Frame Relay cloud, you now have two *logical subinterfaces* connected to the Frame Relay cloud: Serial0/0.503 and Serial0/0.504. Each one of these subinterfaces is on its own subnet. Now, the split-horizon problems from before are automatically solved through the creation of these subinterfaces. When the router receives a routing update on Serial0/0.503, it has no problem sending it out Serial0/0.504, and vice versa. Now you may argue that it is still sending it out the same physical interface, which is true. However, the router doesn't see it this way. After you create the two subinterfaces, the router sees them as two completely independent connections. The only disadvantage of a point-to-point configuration is that you must configure a separate subnet for each PVC, whereas the multipoint allowed all routers to share a common subnet.

With that foundation in place, let's jump straight into the configuration and fill in the gaps as you go. I'm going to begin with the hub of the network: the great Salmon router. First, familiarize yourself with the surroundings:

```
Salmon#show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
```

```
Serial0/0          unassigned      YES manual up                    up
Serial0/1          unassigned      YES NVRAM  administratively down down
Serial0/2          unassigned      YES NVRAM  administratively down down
Serial0/3          unassigned      YES NVRAM  administratively down down
Ethernet1/0        unassigned      YES NVRAM  administratively down down
FastEthernet2/0    172.16.35.1     YES NVRAM  up                    up
```

Good—the Serial0/0 interface has no IP configuration. Let's begin:

```
Salmon#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Salmon(config)#interface serial 0/0
Salmon(config-if)#encapsulation frame-relay
Salmon(config-if)#exit
Salmon(config)#
*Mar  1 02:06:37.787: %LINEPROTO-5-UPDOWN: Line protocol on
➥Interface Serial0/0, changed state to up
```

The first move is to enable Frame Relay encapsulation on the physical interface. Notice that the line protocol immediately comes online. At this point, you are finished with the physical interface configuration. Now you can move to the subinterfaces.

```
Salmon(config)#interface serial 0/0.?
  <0-4294967295>  Serial interface number

Salmon(config)#interface serial 0/0.503 ?
  multipoint      Treat as a multipoint link
  point-to-point  Treat as a point-to-point link

Salmon(config)#interface serial 0/0.503 point-to-point
Salmon(config-subif)#
```

We've just created the subinterface Serial0/0.503 in a point-to-point configuration, as shown in Figure 17.9. The fact that the subinterface number matches the local DLCI used for the connection holds no functional significance whatsoever. It is just a common practice to have your subinterface number match the DLCI number for administrative identification purposes. Now that you are in the subinterface configuration mode, you can set up the logical parameters. This will take just two settings:

```
Salmon(config-subif)#ip address 10.5.5.1 255.255.255.0
Salmon(config-subif)#frame-relay interface-dlci 503
Salmon(config-fr-dlci)#exit
Salmon(config-subif)#exit
Salmon(config)#
```

The two commands necessary assigned the IP address and the local DLCI number to the subinterface. No complex mappings. No broadcast keywords. Just an IP address and DLCI

number. Simple is good. Now add the second subinterface to the configuration and verify how everything looks:

```
Salmon(config)#interface serial 0/0.504 point-to-point
Salmon(config-subif)#ip address 10.6.6.1 255.255.255.0
Salmon(config-subif)#frame-relay interface-dlci 504
Salmon(config-fr-dlci)#end
Salmon#
*Mar  1 02:14:31.287: %SYS-5-CONFIG_I: Configured from console by console
Salmon#show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
Serial0/0          unassigned      YES manual up                    up
Serial0/0.503      10.5.5.1        YES manual up                    up
Serial0/0.504      10.6.6.1        YES manual up                    up
Serial0/1          unassigned      YES NVRAM  administratively down down
Serial0/2          unassigned      YES NVRAM  administratively down down
Serial0/3          unassigned      YES NVRAM  administratively down down
Ethernet1/0        unassigned      YES NVRAM  administratively down down
FastEthernet2/0    172.16.35.1     YES NVRAM  up                    up
```

Have you ever had a fresh chocolate chip cookie, pulled right out of the oven, cooked to a golden crisp that literally melts in your mouth? That's the only thing that *might* be better than a configuration like this. Look at that!!! You have two logical subinterfaces configured perfectly on their own subnets. The router also knows what DLCI number it is able to use to reach the other side of the connection. One quick note: Have you been noticing how the router moves you into a DLCI configuration mode after you enter the `frame-relay interface-dlci` command? When you get into the advanced Frame Relay configurations, you will be able to assign certain traffic shaping parameters to each one of those connections that tell the router how fast it should send to each site, among many other things. That's for the CCNP certification. For now, go ahead and bring up the two spoke routers:

```
BlueGill#show ip interface brief
Interface      IP-Address      OK? Method Status                Protocol
Ethernet0      172.16.20.1     YES NVRAM  up                    up
Ethernet1      unassigned      YES unset  administratively down down
Serial0        unassigned      YES NVRAM  up                    down
Serial1        unassigned      YES unset  administratively down down
BlueGill#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BlueGill(config)#interface serial 0
BlueGill(config-if)#encapsulation frame-relay
*Mar  1 02:19:32.011: %LINEPROTO-5-UPDOWN: Line protocol on
➥Interface Serial0, changed state to up
BlueGill(config-if)#exit
BlueGill(config)#interface serial 0.305 point-to-point
BlueGill(config-subif)#ip address 10.5.5.2 255.255.255.0
BlueGill(config-subif)#frame-relay interface-dlci 305
02:20:18: %FR-5-DLCICHANGE: Interface Serial0 - DLCI 305 state
```

```
➥changed to ACTIVE
BlueGill(config-fr-dlci)#^Z
BlueGill#

Trout#show ip interface brief
Interface              IP-Address      OK? Method Status        Protocol
Ethernet0/0            172.16.15.1     YES NVRAM  up            up
Serial0/0              unassigned      YES NVRAM  up            down
Trout#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Trout(config)#interface serial 0/0
Trout(config-if)#encapsulation frame-relay
*Mar  1 02:29:36.081: %LINEPROTO-5-UPDOWN: Line protocol on Interface
➥Serial0/0, changed state to up
Trout(config-if)#exit
Trout(config)#interface serial 0/0.405 point-to-point
Trout(config-subif)#ip address 10.6.6.2 255.255.255.0
Trout(config-subif)#frame-relay interface-dlci 405
02:33:18: %FR-5-DLCICHANGE: Interface Serial0/0 - DLCI 405 state
➥changed to ACTIVE
Trout(config-fr-dlci)#^Z
Trout#
```

Did you see those DLCIs go ACTIVE? That's a really good sign that things are working just fine. Behind the scenes, I also configured the EIGRP process on all three routers to include all attached interfaces. Because I'm currently connected to the Trout router, I'll verify everything is working okay from here:

```
Trout#ping 10.6.6.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms

Trout#ping 10.5.5.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.5.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/116/117 ms
Trout#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 3 subnets
D       172.16.35.0 [90/2172416] via 10.6.6.1, 00:05:21, Serial0/0.405
D       172.16.20.0 [90/21049600] via 10.6.6.1, 00:05:21, Serial0/0.405
C       172.16.15.0 is directly connected, Ethernet0/0
     10.0.0.0/24 is subnetted, 2 subnets
C       10.6.6.0 is directly connected, Serial0/0.405
D       10.5.5.0 [90/21024000] via 10.6.6.1, 00:05:21, Serial0/0.405
```

Sweet! The first ping tested connectivity from the Trout router to the Salmon router. The second ping tested connectivity from the Trout router to the BlueGill router. Finally, by examining the routing table, you can see that the Trout router has already learned about the LANs behind Trout and BlueGill, and has even learned about the PVC between Salmon and BlueGill (this is the last bolded entry in the routing table). This is a key feature of the point-to-point configuration. Because every PVC is seen as its own subnet, routing protocols enable your routers to learn about those connections without requiring the messy maps of multipoint configurations. Just like that, you have a point-to-point Frame Relay configuration.

Verifying Frame Relay

As you have gone through the three different configurations of Frame Relay, you have really seen the Frame Relay verification commands in action. However, it's time for a formal introduction of the three major commands you use when ensuring all is well with your Frame Relay configuration.

show frame-relay lmi

This command enables you to verify your communication with the Frame Relay service provider.

```
Lilo#show frame-relay lmi
LMI Statistics for interface Serial0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 258              Num Status msgs Rcvd 259
  Num Update Status Rcvd 0              Num Status Timeouts 0
  Last Full Status Req 00:00:07         Last Full Status Rcvd 00:00:07
```

Notice that the `Num Status Enq. Sent` and `Num Status msgs Rcvd` fields are relatively the same. This indicates that your communication with the service provider is excellent.

show frame-relay pvc

This command enables you to see, in detail, all the PVC connections your router has established through the cloud.

```
Stitch#show frame-relay pvc
PVC Statistics for interface Serial0/0 (Frame Relay DTE)
               Active     Inactive      Deleted       Static
  Local           1            0            0            0
  Switched        0            0            0            0
  Unused          0            0            0            0
DLCI = 405, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
➥Serial0/0.405
  input pkts 643           output pkts 638          in bytes 54196
  out bytes 51074          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0               out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 624       out bcast bytes 49746
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:45:12, last time pvc status changed 00:45:12
```

The main information you'll grab from this output is the status of the circuit (shown here as ACTIVE) and the DLCI number (shown here as 405). It's sometimes nice to see the packet statistics for the PVCs as well to ensure traffic is passing between your locations.

show frame-relay map

This command is my favorite command to verify my Frame Relay circuits.

```
Stitch#show frame-relay map
Serial0/0.405 (up): point-to-point dlci, dlci 405(0x195,0x6450), broadcast
          status defined, active
```

This is the most concise way of finding out your DLCI number and the state of the circuit, without being overwhelmed with all the statistics for the line.

Troubleshooting Frame Relay

Alas, when all is not well with your Frame Relay connections, the `debug` commands come to the rescue. Thankfully, for most troubleshooting scenarios, there is just one `debug` command that can expose the problem. Before you get into the debug, though, you'll quickly see that the

standard `show` commands from the verification section can give quite a bit of useful information. Take a look:

```
Stitch#show frame-relay map
Serial0/0.407 (down): point-to-point dlci, dlci 407(0x197,0x6470), broadcast
          status deleted
Serial0/0.405 (up): point-to-point dlci, dlci 405(0x195,0x6450), broadcast
          status defined, active
Serial0/0.406 (down): point-to-point dlci, dlci 406(0x196,0x6460), broadcast
          status defined, inactive
```

Just a simple `show frame-relay map` command can point you in the initial direction for troubleshooting the circuit. As you can see from the output, there are three different DLCI numbers in three different activity states. First up is DLCI 407, which is in a status of DELETED. This means that the router is attempting to communicate with the service provider through DLCI 407, but the service provider has no idea what the router is talking about. They have no DLCI 407 defined. In this case, the configuration problem is most likely on your own router. Typing the DLCI number incorrectly is one likely cause. Otherwise, the service provider dropped the ball and did not accurately set up the connections. The second DLCI in the list is DLCI 405, which is in a status of ACTIVE. This is a good circuit, going through to the other end of the connection. The final DLCI in the list is DLCI 406, which is in a status of INACTIVE. This means that the end of the connection is configured, and the service provider recognizes the DLCI you are attempting to use. The other end of the connection is where the problem lies. They have either configured an incorrect DLCI or have not configured the interface at all.

Just from this initial output, you can figure out a direction or a location to begin your troubleshooting efforts. Now comes the lower-level debug troubleshooting.

```
Salmon#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
*Mar  1 00:05:07.215: Serial0/0(out): StEnq, myseq 1, yourseen 0, DTE down
*Mar  1 00:05:07.215: datagramstart = 0x1DA2F74, datagramsize = 14
*Mar  1 00:05:07.215: FR encap = 0x00010308
*Mar  1 00:05:07.215: 00 75 95 01 01 01 03 02 01 00
*Mar  1 00:05:17.215: Serial0/0(out): StEnq, myseq 2, yourseen 0, DTE down
*Mar  1 00:05:17.215: datagramstart = 0x1C01254, datagramsize = 14
*Mar  1 00:05:17.215: FR encap = 0x00010308
*Mar  1 00:05:17.215: 00 75 95 01 01 00 03 02 02 00
*Mar  1 00:05:27.215: Serial0/0(out): StEnq, myseq 3, yourseen 0, DTE down
*Mar  1 00:05:27.215: datagramstart = 0x1DA21B4, datagramsize = 14
*Mar  1 00:05:27.215: FR encap = 0x00010308
*Mar  1 00:05:27.215: 00 75 95 01 01 00 03 02 03 00
*Mar  1 00:05:37.215: Serial0/0(out): StEnq, myseq 4, yourseen 0, DTE down
*Mar  1 00:05:37.215: datagramstart = 0x1C00494, datagramsize = 14
*Mar  1 00:05:37.215: FR encap = 0x00010308
*Mar  1 00:05:37.215: 00 75 95 01 01 00 03 02 04 00
```

The most useful debug is typically the `debug frame-relay lmi` because this focuses on your direct communication with the service provider. At first, this output looks quite cryptic, but take a look at the highlighted information. You can see the sequence numbers increasing on your end (that's the `myseq` field), but the service provider doesn't see this. This most likely indicates that the Frame Relay LMI language is mismatched between you and the service provider. Here's how to fix the problem:

```
Salmon#show frame-relay lmi

LMI Statistics for interface Serial0/0 (Frame Relay DTE) LMI TYPE = ANSI
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 49               Num Status msgs Rcvd 14
  Num Update Status Rcvd 0              Num Status Timeouts 34
Salmon#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Salmon(config)#interface serial 0/0
Salmon(config-if)#
*Mar  1 00:08:47.215: Serial0/0(out): StEnq, myseq 23, yourseen 0, DTE down
*Mar  1 00:08:47.215: datagramstart = 0x1C019D4, datagramsize = 14
*Mar  1 00:08:47.215: FR encap = 0x00010308
*Mar  1 00:08:47.215: 00 75 95 01 01 00 03 02 17 00
*Mar  1 00:08:47.215:
Salmon(config-if)#frame lmi-type cisco
*Mar  1 00:08:57.215: Serial0/0(out): StEnq, myseq 1, yourseen 0, DTE down
*Mar  1 00:08:57.215: datagramstart = 0x1DA2BB4, datagramsize = 13
*Mar  1 00:08:57.215: FR encap = 0xFCF10309
*Mar  1 00:08:57.215: 00 75 01 01 00 03 02 01 00
*Mar  1 00:08:57.227: Serial0/0(in): Status, myseq 1
*Mar  1 00:08:57.227: RT IE 1, length 1, type 0
*Mar  1 00:08:57.227: KA IE 3, length 2, yourseq 1 , myseq 1
*Mar  1 00:08:57.227: PVC IE 0x7 , length 0x6 , dlci 503, status 0x0 , bw 0
*Mar  1 00:08:57.227: PVC IE 0x7 , length 0x6 , dlci 504, status 0x0 , bw 0
*Mar  1 00:09:07.215: Serial0/0(out): StEnq, myseq 2, yourseen 1, DTE down
*Mar  1 00:09:07.215: datagramstart = 0x1DA22F4, datagramsize = 13
*Mar  1 00:09:07.215: FR encap = 0xFCF10309
*Mar  1 00:09:07.215: 00 75 01 01 01 03 02 02 01
*Mar  1 00:09:07.235: Serial0/0(in): Status, myseq 2
*Mar  1 00:09:07.235: RT IE 1, length 1, type 0
*Mar  1 00:09:07.235: KA IE 3, length 2, yourseq 2 , myseq 2
*Mar  1 00:09:07.235: PVC IE 0x7 , length 0x6 , dlci 503, status 0x0 , bw 0
*Mar  1 00:09:07.235: PVC IE 0x7 , length 0x6 , dlci 504, status 0x0 , bw 0
```

Sure enough, you saw that the LMI type was hard-coded as ANSI. After it was changed over to Cisco, the debug showed the sequence numbers matching up between your router and the

service provider. Right after the sequence number synchronization, the service provider's router delivers the DLCI information to your router. This is where it pays to know the status codes. These are not covered on the CCNA exam, but are tested on when you get into the CCNP level exams:

Status 0x0 = INACTIVE

Status 0x2 = ACTIVE

Status 0x4 = DELETED

In this case, you can see that both DLCI 503 and 504 are marked as INACTIVE.

Most of the Frame Relay troubleshooting comes from a misconfiguration of the Frame Relay DLCI. It's very easy to map the wrong DLCI to the wrong IP address because Frame Relay uses a very different addressing perspective than most other networking technologies. Understanding the Frame Relay circuit states can really help in isolating the problem quickly.

Chapter Summary

This chapter has taken you from the basics of Frame Relay into a fairly complex configuration using subinterfaces. The steepest part of the learning curve in the Frame Relay world is in trying to understand the terminology. Frame Relay uses a new set of Layer 2 addresses known as DLCIs. These are your logical addresses, which enable you to communicate with remote devices over the Frame Relay cloud. Unlike typical addressing, DLCIs work through a localized system—that is, you leave on a local DLCI to reach a remote destination over a PVC. This PVC is established for you by a service provider (after you have paid an excessive amount of money) and is one of the primary criteria that determine your monthly cost for the line. The other cost-affecting criterion is the CIR you purchase for each circuit. This is the speed that the service provider commits to give you for each PVC you purchase. Many times, you will be able to burst above this speed if extra bandwidth is available.

After you understand the terminology of Frame Relay, you have three different configuration options. For simple network designs, you can let the Inverse ARP system take care of the Frame Relay setup for you. If you just enable Frame Relay encapsulation on your Serial interface, the router can configure itself. It does this by using LMI signaling to receive all its DLCI information from the service provider. The router can then use Inverse ARP to discover the remote devices. As your network becomes more advanced and uses multiple virtual circuits, you can rely on a multipoint or point-to-point configuration. The advantage of multipoint is that all the routers connected to the Frame Relay cloud can share a common subnet. The major problem with this configuration comes from the routing loop prevention mechanism split-horizon. This prevents a router from sending a routing update out the same interface as that over which it was received. Coming to the rescue are point-to-point subinterfaces. These enable you to statically assign a DLCI number to a dedicated subinterface. Because each PVC has its own subinterface, there are no problems with split-horizon.

Key Terms

- virtual circuit
- permanent virtual circuit (PVC)
- switched virtual circuit (SVC)
- hub and spoke design
- partial mesh design
- full mesh design
- Local Management Interface (LMI)
- Data Link Connection Identifier (DLCI)
- local access rate/line speed
- Committed Information Rate (CIR)
- Backwards Explicit Congestion Notification (BECN)
- Forwards Explicit Congestion Notification (FECN)
- Discard Eligible (D_e)
- Non-Broadcast Multi-Access (NBMA)
- split-horizon

- point-to-point subinterfaces
- point-to-multipoint/multipoint subinterfaces
- Frame Relay map
- inverse ARP
- static mappings
- Cisco Frame Relay encapsulation
- IETF Frame Relay encapsulation
- ACTIVE, INACTIVE, and DELETED PVC status
- Cisco, ANSI, and Q933A LMI signaling

Apply Your Knowledge

Exercises

17.1 Configuring Frame Relay in a Partial Mesh Environment

Trees Unlimited Inc., a well-to-do lumber company, has offered you an exorbitant amount of money to convert their point-to-point T1 infrastructure into a partial mesh Frame Relay environment. They have four locations with a variety of connectivity requirements. The circuits have been installed and provisioned at each of their four locations, shown in Figure 17.11.

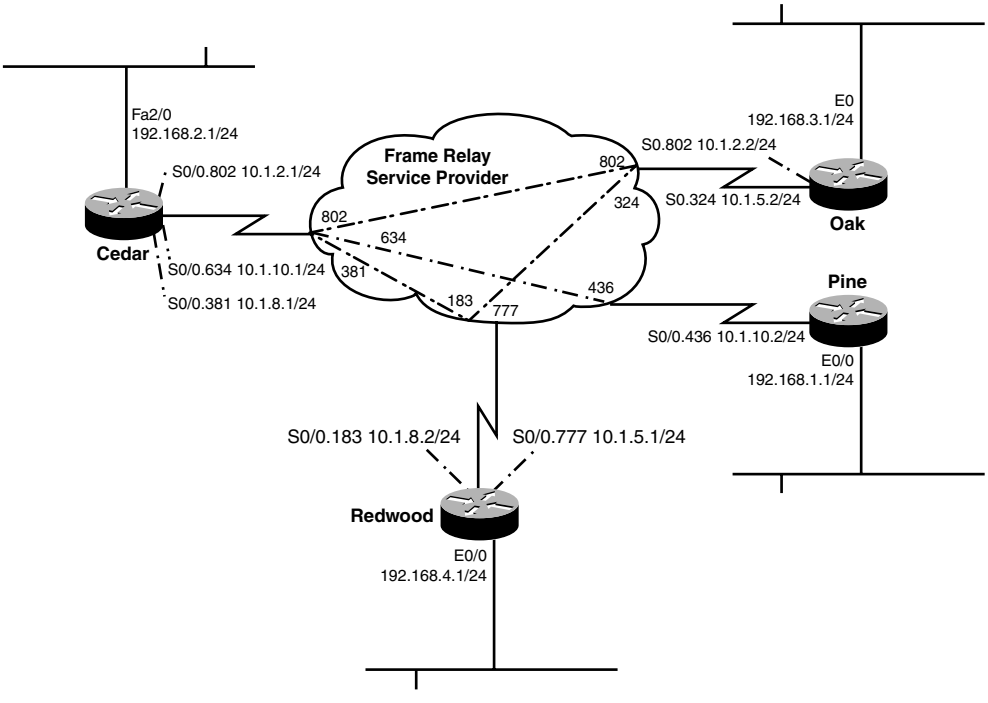


FIGURE 17.11 Trees Unlimited Inc. Frame Relay network.

Your goal is to configure the Frame Relay network as shown in the network diagram. You also need to enable EIGRP routing for autonomous system 50 for all networks to ensure routes are accurately advertised around the network.

Estimated Time: 15–20 minutes

Wow! What a scenario! It looks overwhelming at first. Take this one router at a time, starting with the hub of the network: Cedar. As shown in this diagram, it's clear that the network designer decided to go with a point-to-point setup because every PVC is assigned its own subnet. Also, take a look at the PVC between the Cedar and Oak routers. That's not a misprint! It is a common practice for Frame Relay service providers to use the same DLCI number on both sides of the connection. Because DLCIs are locally significant, accessing DLCI 802 at the Cedar location means something completely different than accessing DLCI 802 at the Oak location. With those prerequisites in place, you can jump right into the configuration:

```
Cedar#show ip interface brief
Interface        IP-Address   OK? Method Status                Protocol
Serial0/0        unassigned   YES NVRAM  up                    down
Serial0/1        unassigned   YES NVRAM  administratively down down
Serial0/2        unassigned   YES NVRAM  administratively down down
Serial0/3        unassigned   YES NVRAM  administratively down down
Ethernet1/0      unassigned   YES NVRAM  administratively down down
FastEthernet2/0  192.168.2.1  YES manual up                    up
Cedar#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cedar(config)#interface serial 0/0
Cedar(config-if)#encapsulation frame-relay
Cedar(config-if)#exit
*Mar  1 00:03:40.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface
➥Serial0/0, changed state to up
Cedar(config)#interface serial 0/0.802 point-to-point
Cedar(config-subif)#ip address 10.1.2.1 255.255.255.0
Cedar(config-subif)#frame-relay interface-dlci 802
Cedar(config-fr-dlci)#exit
Cedar(config-subif)#exit
Cedar(config)#interface serial 0/0.634 point-to-point
Cedar(config-subif)#ip address 10.1.10.1 255.255.255.0
Cedar(config-subif)#frame-relay interface-dlci 634
Cedar(config-fr-dlci)#exit
Cedar(config-subif)#exit
Cedar(config)#interface serial 0/0.381 point-to-point
Cedar(config-subif)#ip address 10.1.8.1 255.255.255.0
Cedar(config-subif)#frame-relay interface-dlci 381
Cedar(config-fr-dlci)#exit
Cedar(config-subif)#exit
Cedar(config)#router eigrp 50
Cedar(config-router)#network 10.0.0.0
Cedar(config-router)#network 192.168.2.0
Cedar(config-router)#no auto-summary
Cedar(config-router)#exit
```

```
Cedar(config)#exit
*Mar  1 00:05:17.535: %SYS-5-CONFIG_I: Configured from console by
➥console
Cedar#show ip interface brief
Interface        IP-Address   OK? Method Status                Protocol
Serial0/0        unassigned   YES NVRAM  up                    up
Serial0/0.381    10.1.8.1     YES manual down                  down
Serial0/0.634    10.1.10.1    YES manual up                    up
Serial0/0.802    10.1.2.1     YES manual down                  down
Serial0/1        unassigned   YES NVRAM  administratively down down
Serial0/2        unassigned   YES NVRAM  administratively down down
Serial0/3        unassigned   YES NVRAM  administratively down down
Ethernet1/0      unassigned   YES NVRAM  administratively down down
FastEthernet2/0  192.168.2.1  YES manual up                    up
```

Initially, it may look like there is a problem here. Only one of the subinterfaces has come up, but when you look back at the network diagram (in Figure 17.10), you can see that subinterface Serial0/0.634 on the Cedar router connects down to the Pine router. Pine happens to be the only router that does not have multiple PVC connections. In this case, Inverse ARP took care of the mapping on that side of the connection, which brings the interface up. The rest of them require the remote router be configured before the operational status goes active. Before you leave the Cedar router, you need to do one more verification command:

```
Cedar#show frame-relay pvc

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

               Active     Inactive      Deleted       Static
  Local           0            3            0            0
  Switched        0            0            0            0
  Unused          0            0            0            0

DLCI = 381, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE =
➥Serial0/0.381

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:06:56, last time pvc status changed 00:06:56

DLCI = 634, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE =
➥Serial0/0.634
```

```
  input pkts 0             output pkts 86           in bytes 0
  out bytes 14864          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0               out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 86        out bcast bytes 14864
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:06:58, last time pvc status changed 00:00:08

DLCI = 802, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE =
➥Serial0/0.802

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in pkts dropped 0
  out pkts dropped 0               out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:06:59, last time pvc status changed 00:06:59
```

Just as expected: Every DLCI is marked as INACTIVE. This is actually good news: It says that the remote side is not configured correctly; however, your side is configured just fine (otherwise the PVC status would be set to DELETED). Now move on to the Oak location.

```
Oak#show ip interface brief
Interface      IP-Address   OK? Method Status                Protocol
Ethernet0      192.168.3.1  YES manual up                    up
Ethernet1      unassigned   YES unset  administratively down down
Serial0        unassigned   YES unset  up                    down
Serial1        unassigned   YES unset  administratively down down
Oak#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Oak(config)#interface serial 0
Oak(config-if)#encapsulation frame-relay
Oak(config-if)#exit
00:20:01: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
➥changed state to up
00:20:02: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:20:02: %FR-5-DLCICHANGE: Interface Serial0 - DLCI 802 state
➥changed to ACTIVE
Oak(config)#interface serial 0.802 point-to-point
Oak(config-subif)#ip address 10.1.2.2 255.255.255.0
Oak(config-subif)#frame-relay interface-dlci 802
Oak(config-fr-dlci)#exit
Oak(config-subif)#exit
Oak(config)#interface serial 0.324 point-to-point
```

```
Oak(config-subif)#ip address 10.1.5.2 255.255.255.0
Oak(config-subif)#frame-relay interface-dlci 324
00:20:57: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0.324,
➥changed state to down
Oak(config-fr-dlci)#exit
Oak(config-subif)#exit
Oak(config)#router eigrp 50
Oak(config-router)#network 10.0.0.0
Oak(config-router)#network 192.168.3.0
Oak(config-router)#no auto-summary
Oak(config-router)#exit
Oak(config)#exit
00:21:19: %SYS-5-CONFIG_I: Configured from console by console
Oak#show ip interface brief
Interface    IP-Address   OK? Method Status                Protocol
Ethernet0    192.168.3.1  YES manual up                    up
Ethernet1    unassigned   YES unset  administratively down down
Serial0      unassigned   YES unset  up                    up
Serial0.324  10.1.5.2     YES manual down                  down
Serial0.802  10.1.2.2     YES manual up                    up
Serial1      unassigned   YES unset  administratively down down
Oak#ping 10.1.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/60/60 ms
```

Nice. Now you can ping successfully between the Oak and Cedar locations because you have configured both sides of the connection. Did you notice that DLCI 802 went ACTIVE as soon as you turned on Frame Relay encapsulation? The Oak router used Inverse ARP to detect that the Cedar router had been configured on the other end of the connection. Now you can continue around the network diagram in a clockwise fashion and set up the Pine router.

```
Pine#show ip interface brief
Interface        IP-Address   OK? Method Status                Protocol
Ethernet0/0      192.168.1.1  YES manual up                    up
Serial0/0        unassigned   YES NVRAM  up                    down
Pine#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Pine(config)#interface serial 0/0
Pine(config-if)#encapsulation frame-relay
Pine(config-if)#exit
*Mar  1 00:22:51.147: %LINEPROTO-5-UPDOWN: Line protocol on Interface
➥Serial0/0, changed state to up
Pine(config)#interface serial 0/0.436 point-to-point
Pine(config-subif)#ip address 10.1.10.2 255.255.255.0
Pine(config-subif)#frame-relay interface-dlci 436
Pine(config-fr-dlci)#exit
```

```
Pine(config-subif)#exit
Pine(config)#router eigrp 50
Pine(config-router)#network 10.0.0.0
Pine(config-router)#network 192.168.1.0
Pine(config-router)#no auto-summary
Pine(config-router)#exit
Pine(config)#
Pine(config)#exit
*Mar  1 00:23:45.504: %SYS-5-CONFIG_I: Configured from console by
➥console
Pine#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
Ethernet0/0        192.168.1.1     YES manual up            up
Serial0/0          unassigned      YES NVRAM  up            up
Serial0/0.436      10.1.10.2       YES manual up            up
Pine#ping 10.1.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
```

Excellent. You can ping to the Cedar router. You now have three routers configured in this story; take a moment to check the routing table and see whether EIGRP is doing its job:

```
Pine#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.10.0 is directly connected, Serial0/0.436
D       10.1.2.0 [90/21024000] via 10.1.10.1, 00:02:02, Serial0/0.436
C    192.168.1.0/24 is directly connected, Ethernet0/0
D    192.168.2.0/24 [90/2172416] via 10.1.10.1, 00:02:02, Serial0/0.436
D    192.168.3.0/24 [90/21049600] via 10.1.10.1, 00:02:02, Serial0/0.436
Pine#ping 192.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/116/117 ms
```

Everything looks good here! Just for fun, I sent a ping from the Pine router over to the LAN interface of Oak and it looks as sweet as…well, a chocolate chip cookie. Now take on the final router configuration:

```
Redwood#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
Ethernet0/0        192.168.4.1     YES manual up            up
Serial0/0          unassigned      YES unset  up            down
Redwood#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Redwood(config)#interface serial 0/0
Redwood(config-if)#encapsulation frame-relay
Redwood(config-if)#exit
*Mar  1 00:35:28.484: %LINEPROTO-5-UPDOWN: Line protocol on Interface
➥Serial0/0, changed state to up
Redwood(config)#interface serial 0/0.183 point-to-point
Redwood(config-subif)#ip address 10.1.8.2 255.255.255.0
Redwood(config-subif)#frame-relay interface-dlci 183
Redwood(config-fr-dlci)#exit
Redwood(config-subif)#exit
Redwood(config)#interface serial 0/0.777 point-to-point
Redwood(config-subif)#ip address 10.1.5.1 255.255.255.0
Redwood(config-subif)#frame-relay interface-dlci 777
Redwood(config-fr-dlci)#exit
Redwood(config-subif)#exit
Redwood(config)#router eigrp 50
Redwood(config-router)#network 10.0.0.0
*Mar  1 00:37:12.411: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 50: Neighbor 10.1.8.1
(Serial0/0.183) is up: new adjacency
*Mar  1 00:37:14.714: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 50: Neighbor 10.1.5.2
(Serial0/0.777) is up: new adjacency
Redwood(config-router)#network 192.168.4.0
Redwood(config-router)#no auto-summary
Redwood(config-router)#^Z
Redwood#
*Mar  1 00:37:30.316: %SYS-5-CONFIG_I: Configured from console by console
Redwood#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
Ethernet0/0        192.168.4.1     YES manual up            up
Serial0/0          unassigned      YES unset  up            up
Serial0/0.183      10.1.8.2        YES manual up            up
Serial0/0.777      10.1.5.1        YES manual up            up
Redwood#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
```

```
C    192.168.4.0/24 is directly connected, Ethernet0/0
     10.0.0.0/24 is subnetted, 4 subnets
D       10.1.10.0 [90/21024000] via 10.1.8.1, 00:00:12, Serial0/0.183
C       10.1.8.0 is directly connected, Serial0/0.183
D       10.1.2.0 [90/2681856] via 10.1.5.2, 00:00:12, Serial0/0.777
C       10.1.5.0 is directly connected, Serial0/0.777
D    192.168.1.0/24 [90/21049600] via 10.1.8.1, 00:00:12, Serial0/0.183
D    192.168.2.0/24 [90/2172416] via 10.1.8.1, 00:00:12, Serial0/0.183
D    192.168.3.0/24 [90/2195456] via 10.1.5.2, 00:00:13, Serial0/0.777
```

Well, it looks like your work here is done. All that's left to do is to collect that exorbitant check from the wealthy tree company!

Review Questions

1. There are three virtual circuit design strategies for a Frame Relay cloud. Explain what these are and the advantages and disadvantages associated with each.
2. Write a brief definition for the following terms:
   - Local Management Interface
   - Data Link Connection Identifier
   - Local Access Rate
   - Committed Information Rate
3. When you connect a router to a Frame Relay network, the service provider transmits DLCI information to your router via LMI. How does the router then find the Layer 3 address to associate with the circuit?
4. When connecting a router to a Frame Relay network with multiple destinations, split-horizon issues can occur. Explain why this is and the two methods you could use to fix these issues.
5. You are troubleshooting a Frame Relay network. It appears that your router is not receiving any DLCI information. What command(s) would you use to begin troubleshooting this problem and why?

Exam Questions

1. Into what categories of network does Frame Relay fit? (Choose 2.)
   - ❍ **A.** Circuit-switched
   - ❍ **B.** Packet-switched
   - ❍ **C.** Broadcast multi-access
   - ❍ **D.** NBMA

2. Which of the following connections describe an on-demand circuit through the Frame Relay cloud that is created when needed and then destroyed after data has been transmitted?

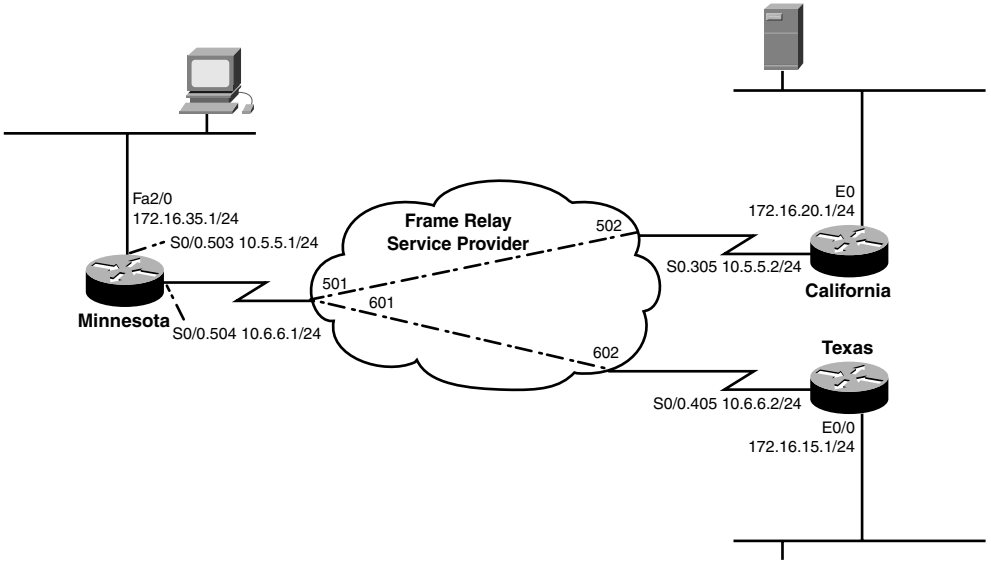
- ❍ **A.** PVC
- ❍ **B.** SVC
- ❍ **C.** DID
- ❍ **D.** DOD

3. Which of the following are valid LMI signaling types? (Choose 3.)

- ❍ **A.** Cisco
- ❍ **B.** IETF
- ❍ **C.** ANSI
- ❍ **D.** Q.933a

4. According to Figure 17.12, what DLCI would be used if a client in Minnesota wanted to send information to a server in California?

- ❍ **A.** 501
- ❍ **B.** 502
- ❍ **C.** 601
- ❍ **D.** 602



5. A router connected to a Frame Relay service provider can occasionally send faster than the subscribed _____, but never faster than the _____.

- ❍ **A.** Local Access Rate, CIR
- ❍ **B.** Virtual Circuit Speed, CIR
- ❍ **C.** CIR, Virtual Circuit Speed
- ❍ **D.** CIR, Local Access Rate

6. If your router is sending too much information into the Frame Relay cloud, the service provider tags any return traffic with a _____ to notify your router to reduce its transmission rate.

- ❍ **A.** D_e
- ❍ **B.** BECN
- ❍ **C.** FECN
- ❍ **D.** Burst

7. By default, Cisco routers receive LMI messages from the service provider that provide all usable DLCI numbers for the local circuit. How does your router find out the remote devices it is able to reach?

- ❍ **A.** The router sends Hello messages down each virtual circuit.
- ❍ **B.** The router uses CDP to discover its directly connected neighbors.
- ❍ **C.** The router uses Inverse ARP messages.
- ❍ **D.** The router does not need to do anything; LMI signaling from the service provider autoconfigures the router.

8. You have two routers connected over a Frame Relay network. The router in Arizona has the IP address 10.1.1.1/24 and uses a local DLCI of 512. The router in Michigan has the IP address 10.1.1.2/24 and uses a local DLCI of 598. Which syntax among the following choices correctly creates a static map that enables Arizona to reach Michigan and allows routing protocol functionality?

- ❍ **A.** `frame-relay map ip 10.1.1.2 512 broadcast`
- ❍ **B.** `frame-relay map ip 10.1.1.1 512 broadcast`
- ❍ **C.** `frame-relay map ip 10.1.1.2 598 broadcast`
- ❍ **D.** `frame-relay map ip 10.1.1.1 598 broadcast`

9. You are configuring your router's Serial 0 interface to communicate across the Frame Relay cloud with a non-Cisco router. You would like to use the Inverse ARP feature of the router to avoid configuring static maps; what command would you use to enable this feature?

   - ❍ **A.** `encapsulation frame-relay`
   - ❍ **B.** `inverse-arp frame-relay`
   - ❍ **C.** `ietf inverse-arp`
   - ❍ **D.** `encapsulation frame-relay ietf`

10. You are troubleshooting your Frame Relay connections. After typing in the `show frame-relay pvc` command, one of your PVCs shows up as DELETED. What causes this?

    - ❍ **A.** Your router is incorrectly configured. You need to add the right DLCI information and the circuit should come up.
    - ❍ **B.** The remote router is incorrectly configured.
    - ❍ **C.** You are physically disconnected from the service provider.
    - ❍ **D.** You need to switch from a multipoint configuration to a point-to-point configuration and create a subinterface for each PVC you plan on using.

Answers to Review Questions

1. The three Frame Relay virtual circuit design strategies are hub and spoke, partial mesh, and full mesh. Hub and spoke is the cheapest design; however, it also offers the least amount of redundancy. If the hub location fails, the entire WAN mesh goes down. In addition, the hub and spoke design increases the amount of delay for packets traveling between the spoke locations. This can be devastating for VoIP traffic. Partial mesh designs connect key sites with multiple virtual circuits. This offers redundancy for those key locations, but can become a more costly design. Full mesh offers the ultimate level of redundancy and delay guarantees, but requires a huge monthly cost to support the large number of circuits.

2. Local Management Interface (LMI): This is the language spoken between your Frame Relay router and the service provider that is used to provide DLCI status and traffic statistics.

   Data Link Connection Identifier (DLCI): This is the Data Link address used to identify virtual circuits in the Frame Relay cloud.

   Local Access Rate: This is the maximum physical speed your interface connected to the Frame Relay cloud can use.

   Committed Information Rate: This is the level of bandwidth the service provider commits to give you on a regular basis.

3. After your router receives DLCI information, it sends Inverse ARP messages to each DLCI number requesting the Layer 3 address of the remote router.

4. Split-horizon is a loop-prevention mechanism that prevents a router from advertising a route out the same interface that received the original route advertisement. It can cause problems with Frame Relay because a hub router could have multiple destinations connected to a single physical interface. When those destinations send advertisements to the hub router, split horizon prevents the router from propagating the advertisements to other remote offices. The two methods you can use to resolve this issue are disabling the split-horizon mechanism or using point-to-point subinterfaces.

5. The command you would be most likely to use to troubleshoot the failed DLCI communication is the `show frame-relay lmi` command. It enables you to focus on the communication with the Frame Relay service provider. If necessary, you may also use the `debug frame-relay lmi` command to probe deeper into the messages exchanged between your router and the service provider.

Answers to Exam Questions

1. **B, D.** Frame Relay is considered a packet-switched network and operates in much the same way as X.25 and ATM. Rather than have users connected directly together over leased lines, virtual circuits are established through the service provider network. Frame Relay also falls under the NBMA category. This means that, by default, multiple devices can access the network, but broadcast messages are not forwarded. Answer A is incorrect because circuit-switched networks encompass connections that use the telephone company as a backbone. Answer C is incorrect because it describes ethernet connectivity, not Frame Relay.

2. **B, A.** SVC is an on-demand circuit through the Frame Relay cloud that is created when needed and then destroyed after data has been transmitted. This circuit type is not commonly used and has been widely replaced by PVCs, which is Answer A. Answers C and D are incorrect because these acronyms have nothing to do with Frame Relay.

3. **A, C, D.** The valid LMI signaling methods are Cisco, ANSI, and Q.933a. Answer B is incorrect because IETF represents the industry standard Frame Relay encapsulation that allows non-Cisco devices to interoperate with Cisco devices over a Frame Relay cloud.

4. **A.** DLCI addressing works exactly opposite of how most folks think it should work. Rather than send to a *destination* DLCI number, you *leave* on a *local* DLCI number. In this case, the Minnesota router would leave on DLCI 501 to reach the California office. Answer B is incorrect because California would leave on DLCI 502 to get to Arizona. Answers C and D are incorrect because they reference the connection between Minnesota and Texas.

5. **D.** A router connected to a Frame Relay service provider can often send faster than the Committed Information Rate (CIR), but never faster than the Local Access Rate. The CIR describes the minimum amount of bandwidth that the service provider contractually guarantees the client. The Local Access Rate references the fastest physical speed the line can handle. Answers B and C are incorrect because there is no such thing as a Virtual Circuit Speed. Answer A is incorrect because the terms are reversed.

6. **B.** The service provider tags any return traffic with a Backwards Explicit Congestion Notification (BECN) marking. By default, your router ignores these notifications. Answer A is incorrect because Discard Eligible (D_e) describes markings placed on any traffic sent above the CIR. Answer C is incorrect because Forward Explicit Congestion Notification (FECN) markings are placed on packets if there is no return traffic that can be marked with BECNs to tell the sender to slow down. Answer D is what happens to a balloon if you poke it with a needle.

7. **C.** After the routers receive the DLCI information through LMI signaling, they send Inverse ARP messages through to the other side of the connection. This enables them to discover the remote IP addresses they are able to reach. Answer A is incorrect because Hello messages are specific to routing protocols such as OSPF and EIGRP. Answer B is incorrect because Cisco Discovery Protocol enables you to see information just about directly connected Cisco devices. Answer D is incorrect because LMI can only give your routers the DLCI numbers it can use to reach remote devices, but cannot tell the router how the remote devices are configured.

8. **A.** The correct syntax of the Frame Relay map command is `frame-relay map ip <remote_ip_address> <local_dlci> broadcast`. The `broadcast` keyword enables routing protocol updates to function. In this case, Arizona is trying to reach the remote IP address in Michigan of 10.1.1.2, and uses the local DLCI of 512 to get there. All other answers use either the wrong DLCI or IP address.

9. **D.** To use the industry standard Frame Relay encapsulation, you need to type in **`encapsulation frame-relay ietf`**. This enables Inverse ARP to map your Frame Relay circuits for you. Answer A is incorrect because this uses the Cisco proprietary Frame Relay encapsulation that does not work with any non-Cisco gear. The other two answers use invalid syntax and commands.

10. **A.** Three primary PVC states indicate the status of the line. ACTIVE means there are no problems. INACTIVE means that there is a problem with the remote router, which rules out Answer B. DELETED means that there is a problem with your local router. Typically, this is caused by using the incorrect DLCI information. Answer D is eliminated because multipoint and point-to-point designs use DLCI information in the same way. If the DLCI shows up as DELETED under a multipoint configuration, it shows up as DELETED under a point-to-point configuration. Finally, if you were physically disconnected from the service provider, you would not see DLCI information (because LMI is used to send the DLCI status to your router), making answer C incorrect.

Suggested Reading and Resources

1. Cisco TAC Configuring Frame Relay, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/wan_c/wcdfrely.htm.

2. Ward, Chris and Cioara, Jeremy. *Exam Cram 2 CCNA Practice Questions*. Que Publishing, 2004.

3. Chin, Jonathan. *Cisco Frame Relay Solutions Guide*. Cisco Press, 2004.

PART II

Final Review

Fast Facts

Practice Exam

Fast Facts

CCNA

OSI Model in Review

Table FF.1 lists the seven layers of the OSI model and significant aspects of each layer.

TABLE FF.1 The OSI Model

OSI Layer	Important Functions
Application	Provides an interface between a host's communication software and any necessary external applications.
	Evaluates what resources are necessary and available resources for communication between two devices.
	Synchronizes client/server applications.
	Provides error control and data integrity between applications.
	Provides system-independent processes to a host.
Presentation	Presents data to the application layer.
	Acts as a data format translator.
	Handles the structuring of data and negotiating data transfer syntax to Layer 7.
	Processes involved include data encryption, decryption, compression, and decompression.
Session	Handles dialog control among devices.
	Determines the beginning, middle, and end of a session or conversation that occurs between applications (intermediary).
Transport	Manages end-to-end connections and data delivery between two hosts.
	Segments and reassembles data.
	Provides transparent data transfer by hiding details of the transmission from the upper layers.

(continues)

TABLE FF.1 *Continued*

OSI Layer	Important Functions
Network	Determines best path for packet delivery across the network.
	Determines logical addressing, which can identify the destination of a packet or datagram.
	Uses data packets (IP, IPX) and route update packets (RIP, EIGRP, and so on).
	Uses routed protocols IP, IPX, and AppleTalk DDP.
	Devices include routers and Layer 3 switches.
Data Link	Ensures reliable data transfer from the Network layer to the Physical layer.
	Oversees physical or hardware addressing.
	Formats packets into a frame.
	Provides error notification.
	Devices include bridges and Layer 2 switches.
Physical	Moves bits between nodes.
	Assists with the activation, maintenance, and deactivation of physical connectivity between devices.
	Devices include hubs and repeaters.

Application Protocols Supported by the Application Layer

TABLE FF.2 Application Layer Protocols

Application Protocols	Function
Telnet	A TCP/IP protocol that provides terminal emulation to a remote host by creating a virtual terminal. TeraTerm is one program that can be installed on a user computer to create telnet sessions. This protocol requires authentication via a username and password.
Hypertext Transfer Protocol (HTTP)	Enables web browsing with the transmission of Hypertext Markup Language (HTML) documents on the Internet.
Secure Hypertext Transfer Protocol (HTTPS)	Enables secure web browsing. A secure connection is indicated when the URL begins with https:// or when there is a lock symbol at the lower right corner of the web page that is being viewed.
File Transfer Protocol (FTP)	Allows a user to transfer files. Provides access to files and directories.

TABLE FF.2 *Continued*

OSI Layer	Important Functions
Trivial File Transfer Protocol (TFTP)	A bare bones version of FTP that does not provide access to directories. With TFTP you can simply send and receive files. Unlike FTP, TFTP is not secure and sends smaller blocks of data.
Domain Name System (DNS)	Resolves hostnames such as cisco.com into IP addresses.
Simple Mail Transfer Protocol (SMTP)	Sends electronic mail across the network.
Post Office Protocol 3 (POP3)	Receives electronic mail by accessing a network server.
Network File System (NFS)	Allows users with different operating systems (that is, NT and Unix workstations) to share files through a network. Remote files appear as though they reside on a local machine even though the local machine might be "diskless."
Network News Transfer Protocol (NNTP)	Offers access to Usenet newsgroup postings.
Simple Network Management Protocol (SNMP)	Monitors the network and manages configurations. Collects statistics to analyze network performance and ensure network security.
Network Time Protocol (NTP)	Synchronizes clocks on the Internet to provide accurate local time on the user system.
Dynamic Host Configuration Protocol (DHCP)	Works dynamically to provide an IP address, subnet mask, domain name, and a default gateway for routers. Works with DNS and WINS (used for NetBIOS addressing).

TABLE FF.3 Control Information for Each Layer

OSI Layer	Control Information Name
Application	Data
Presentation	
Session	
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit

TABLE FF.4 OSI Layers and Related TCP/IP Layers

OSI Layer	TCP/IP Layer
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data Link	Network Access
Physical	

TCP uses Positive Acknowledgment and Retransmission (PAR):

Step 1 The source device begins a timer when a segment is sent and retransmits if the timer runs out before an acknowledgment is received.

Step 2 The source device keeps track of segments that are sent and requires an acknowledgment for each segment.

Step 3 The destination device acknowledges when a segment is received by sending a packet to the source that iterates the next sequence number it is looking for from the source.

TABLE FF.5 The TCP Segment Header Format

Source Port	Destination Port
	Sequence Number
	Acknowledgment Number
Miscellaneous Flags	Window (Flow Control)
Checksum	Urgent
	Options

TABLE FF.6 Applications Using TCP and Related Ports

Application	Port #(s)
FTP	20, 21
Telnet	23
SMTP	25
DNS (zone transfers)	53
HTTP	80
POP3	110
NNTP	119
HTTPS	443

TABLE FF.7 The UDP Header

Source Port	Destination Port
Length	Checksum

TABLE FF.8 Applications Using UDP and Related Ports

Application	Port #(s)
DHCP	67, 68
DNS (name resolution)	53
TFTP	69
NTP	123
SNMP	161

Network Domains

Two domains determine data transport reliability:

Broadcast Domain—A group of nodes that can receive each other's broadcast messages and are segmented by routers.

Collision Domain—A group of nodes that share the same media and are segmented by switches. A collision occurs if two nodes attempt a simultaneous transmission. **Carrier Sense Multiple Access Collision Detection (CSMA/CD)** sends a jam signal to notify the devices that there has been a collision. The devices will then halt transmission for a random back off time.

Cabling, Lines, and Services

Bandwidth—The total amount of information that can traverse a communications medium measured in millions of bits per second. Bandwidth is helpful for network performance analysis. Also, availability is increasing but limited.

Crosstalk—An electrical or magnetic field that is a result of one communications signal that can affect the signal in a nearby circuit.

Near-end Crosstalk (NEXT)—Crosstalk measured at the transmitting end of a cable.

Far-end Crosstalk (FEXT)—Crosstalk measured at the far end of the cable from where the transmission was sent.

Unshielded twisted-pair (UTP) cables are vulnerable to Electromagnetic Interference (EMI) and use an RJ-45 connector. Fiber-optic cables are not susceptible to EMI.

Use a straight-through cable to connect the following devices:

- Terminated directly into a dedicated hub or switch port
- From a PC to a switch or a hub
- From a router to a switch or a hub

Use a cross-over cable to connect the following devices:

- From switch to switch
- From router to router
- From PC to PC
- From a PC to a router
- From a hub to a hub
- From a hub to a switch

Spread Spectrum Wireless LANs allow for high-speed transmissions over short distances.

Wireless Fidelity (Wi-Fi) is defined by IEEE 802.11.

TABLE FF.9 Summary of Ethernet 802.3 Characteristics

Standard	Speed	Media Type	Connector Used
10BASE-2	10Mbps	RG-58 coaxial	BNC
10BASE-5	10Mbps	RG-58 coaxial	BNC
10BASE-T	10Mbps	Category 3, 4, or 5 UTP or STP	RJ-45
10BASE-FL	10Mbps	Fiber-optic	SC or ST

TABLE FF.10 Comparison of Fast Ethernet 802.3u Characteristics

Standard	Speed	Media Type	Connector Used
100BASE-T4	100Mbps	Category 3, 4, or 5 UTP or STP	RJ-45
100BASE-TX	100Mbps	Category 5 UTP or STP	RJ-45
100BASE-FX	100Mbps	Fiber-optic	SC or ST

TABLE FF.11 Summary of Gigabit Ethernet 802.3ab Characteristics

Standard	Speed	Media Type	Connector Used
1000BASE-T or 1000BASE-TX	1000Mbps or 1Gbps	Category 5 UTP or higher	RJ-45

TABLE FF.12 Comparison of Gigabit Ethernet 802.3z Characteristics

Standard	Speed	Media Type	Connector Used
1000BASE-CX	1000Mbps or 1Gbps	Shielded copper wire	9-pin shielded connector
1000BASE-SX	1000Mbps or 1Gbps	MM fiber-optic	SC or ST
1000BASE-LX	1000Mbps or 1Gbps	MM or SM fiber-optic	SC or ST

MAC Addressing

A MAC address is hard-coded (burnt-in) on the network interface controller (NIC) of the Physical layer device attached to the network. Each MAC address must be unique and use the following format:

- Consist of 48 bits (or 6 bytes).
- Displayed by 12 hexadecimal digits (0–9, A–F).
- First six hexadecimal digits in the address are a vendor code or organizationally unique identifier (OUI) assigned to that NIC manufacturer.
- Last six hexadecimal digits are assigned by the NIC manufacturer and must be different from any other number assigned by that manufacturer.

Example of a MAC address: 00:00:07:A9:B2:EB

The OUI in this example is 00:00:07.

The broadcast address value is FFFF.FFFF.FFFF.

Framing and Duplex Types

802.3 frame information and parameters are as follows:

- The data-link header portion of the frame contains the Destination MAC address (6B), Source MAC address (6B), and Length (2B).

- The Logical Link Control portion of the frame contains Destination Service Access Point (DSAP), Source Service Access Point (SSAP), and Control information. All three are 1B long. The Service Access Point (SAP) identifies an upper-layer protocol such as IP (06) or IPX (E0).
- The Data and cyclical redundancy check (CRC) portion of the frame is also called the data-link trailer. The Data field can be anywhere from 43 to 1497B long. The frame check sequence (FCS) field is 4B long. FCS or CRC provides error detection.

Bridges and switches examine the source MAC address of each inbound frame to learn MAC addresses.

Switches are multi-port bridges that use ASIC hardware chips for frame forwarding. Dedicated bandwidth enables the switch port to guarantee the speed assigned to that port. For example, 100Mbps port connections will get 100Mbps transmission rates.

Hubs use half-duplex technology. Switches can be set up for full-duplex.

WAN Interfaces

WAN interfaces are used to provide a point of interconnection between Cisco routers and other network devices. Types of WAN interfaces include

- Basic Rate Interface (BRI)
- Synchronous Serial
- Asynchronous Serial
- High-Speed Serial Interface (HSSI)
- T1 Controller Card

BRI is an Integrated Services Digital Network (ISDN) line that consists of two 64Kbps bearer (B) channels and one 16Kbps data (D) channel.

DCE equipment might consist of a

- Modem
- Channel Service Unit/Data Service Unit (CSU/DSU)
- BRI NT-1

DTE equipment might consist of a

- Router
- PC
- Server

Memory Types

Four memory components are used by Cisco devices. Those components include ROM, Flash, RAM, and NVRAM.

RAM contains the running IOS, with the exception of Run-From-Flash (RFF) routers. RAM also contains the running configuration or the active configuration that is used after a machine is booted.

IOS File Naming Conventions

Given the example filename c2600-ipbase-1.122-1.T.bin, from left to right, each portion of the filename represents the following:

c2600—Hardware Platform (Cisco 2600 router)

ipbase—Feature Set

1—File Format (compressed re-locatable)

122—IOS Version number

l—Maintenance Release Number

T—Train Identifier

Utilities Using ICMP

Internet Control Messaging Protocol (ICMP) is used by ping and traceroute utilities. Packet Internet Groper (ping) allows you to validate that an IP address exists and can accept requests.

- ping is an echo and the response is an echo response.
- Routers send Destination Unreachable messages when they can't reach the destination network and they are forced to drop the packet. The router that drops the packet sends the ICMP DU message.

A traceroute traces the route or path taken from a client to a remote host. Traceroute also reports the IP addresses of the routers at each next hop on the way to the destination. This is

especially useful when you suspect that a router on the route to an unreachable network is responsible for dropping the packet.

IP Addressing

IPv4 addresses

- Consist of 32-bits.
- Broken down into four octets (eight bits each).
- Use dotted decimal format: example is 172.16.122.204.
- Minimum value (per octet) is 0, and the maximum value is 255.
- 0.0.0.0 is a Network ID.
- 255.255.255.255 is a Broadcast IP.

TABLE FF.13 IPv4 Address Classes

	1st Octet	2nd Octet	3rd Octet	4th Octet
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host

TCP/IP defines two additional address classes:

- Class D—used for Multicast addresses
- Class E—used for Research purposes

TABLE FF.14 Address Class Ranges

Class	1st Octet Decimal Range
A	1–126
B	128–191
C	192–223
D	224–239
E	240–255

The 127.*x.x.x* address range is reserved for loopback addresses.

Default subnet masks:

- Class A—255.0.0.0
- Class B—255.255.0.0
- Class C—255.255.255.0

Classless Addressing

Classless Interdomain Routing (CIDR) notation might also be used to identify the subnet mask. The CIDR notation for each network class can be determined by counting the 1s in binary or the amount of bits that make up the *network* portion of the address.

The mask is written in slash notation as follows:

- Class A—/8
- Class B—/16
- Class C—/24

Private Ranges

IANA Private Address Space Allocations:

Class A = 10.0.0.0–10.255.255.255

Class B = 172.16.0.0–172.31.255.255

Class C = 192.168.0.0–192.168.255.255

Subnetting

TABLE FF.15 Decimal to Binary Conversions

Decimal	Binary
0	00000000
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

To calculate the hosts in a subnet, we can use the formula $2^H - 2$. The exponent *H* represents the number of host bits in a network.

To calculate the networks in a subnet, we can use the formula $2^N - 2$. The exponent *N* represents the number of subnet bits in a network.

The range of valid IP addresses in a subnet is the first IP address after the Network ID and the last IP address before the broadcast IP address.

The following represents IP subnetting:

IP Address = 100.15.209.0

Subnet Mask = 255.255.254.0

Network ID = 100.15.208.0

Broadcast IP = 100.15.209.255

Valid IP range = 100.15.208.1–100.15.209.254

Layer 3 Functions

Routers and Layer 3 switches perform the following functions:

- Do not forward broadcasts or multicasts by default.
- Make best path decisions.
- Filter packets with access lists.
- Remove and add Layer 2 frames.
- Quality of service (QoS) rules for traffic types.

Routers decide which interface to forward a packet through by examining the network portion of each IP address.

IOS Terminal Access Methodologies

To gain access to an EXEC session to an IOS for configuration and administration, you can use the following methods:

- Console—Out-of-band CLI access via a rollover cable connected to the COM port of your terminal PC.
- Auxiliary—Out-of-band CLI access via rollover cable connected to external modem for remote access.
- Telnet—In-band CLI access to an active IP address on the device's vty lines using the telnet protocol. Requires configuration.

- SSH—Secure encrypted in-band CLI access to an active IP address using the SSH protocol. Requires configuration.
- HTTP—In-band GUI access to an active IP address using the HTTP protocol. Requires configuration.

IOS Boot Processes

To solidify the startup process, the following is a recap of the stages of the bootup, any fallback procedures, and the memory locations involved:

1. POST located in ROM tests hardware.
2. Bootstrap located in ROM looks at boot field in configuration register to locate IOS. 0x2100 will boot to ROMmon located in ROM. 0x2101 will boot to RxBoot located in ROM.
3. 0x2102-0x210F will prompt bootstrap to parse startup-config in NVRAM for any boot system commands. If there are any commands, do what they say.
4. If no boot system commands, load first file in Flash. If no file in Flash, TFTP boot. If no IOS file found from TFTP, go to RxBoot in ROM. If no RxBoot, go to ROMmon mode.
5. After IOS is loaded, check configuration register. If 0x2142, ignore startup-config in NVRAM. If 0x2102, load startup-config in NVRAM. If no startup-config, TFTP autoinstall. If no TFTP autoinstall configuration found, enter Setup Mode.

IOS Navigation

TABLE FF.16 IOS Navigation Modes

Mode	Prompt	Description
User EXEC	Router>	Basic troubleshooting and verification
Privileged EXEC	Router#	All available commands including `delete`, `clear`, `erase`, `configure`, `copy`, and `reload`
Global Configuration	Router(config)#	Configurations that apply to the entire device
Line Configuration	Router(config-line)#	Configurations that apply to the terminal lines into a device
Interface Configuration	Router(config-if)#	Configurations that apply to interfaces
Subinterface Configuration	Router(config-subif)#	Configurations that apply to logical extensions of the physical interface
Router Configuration	Router(config-router)#	Configurations that apply to routing protocols

Context-Sensitive Help

The question mark will show all the available commands at that particular prompt. To see all the available commands that start with a letter or letter(s), type the letter(s) immediately followed by the question mark. To see the list of commands that follows a keyword, type the keyword followed by the question mark separated by a space. Commands can be abbreviated as long as there are enough characters to recognize what command you are typing.

Terminal Editing Keys

TABLE FF.17 Cisco IOS Terminal Editing Keystrokes

Keystroke	Function
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+B	Moves the cursor back one character.
Ctrl+F	Moves the cursor forward one character.
Esc+B	Moves cursor back one word.
Esc+F	Moves cursor forward one word.

Syntax Errors

- Ambiguous Command—This error is displayed when you have not typed enough characters for the IOS to distinguish which command you want to use. In other words, several commands start with those same characters, so you must type more letters of the command for the IOS to recognize your particular command.
- Incomplete Command—The IOS has recognized your keyword syntax with this error message; however, you need to add more keywords to tell the IOS what you want to do with this command.
- Invalid Input—Also known as the "fat finger" error, this console error message is displayed when you mistype a command. The IOS will display a carrot mark (^) up to the point where the IOS could understand your command.

Global Configuration Commands

TABLE FF.18 Global Configuration Commands

Command	Description
`config-register` *register*	Alters the configuration register.
`boot system` *location*	Specifies location to load IOS.
`hostname` *hostname*	Changes the name of the Cisco router or switch.
`banner motd` *char banner char*	Creates a message of the day login banner.
`Ip host` *name ipaddress*	Configures a static mapping of a hostname to an IP address.
`Ip name-server` *ip*	Specifies a DNS server IP address for dynamic name resolution.
`Ip domain-lookup`	Enables automatic name resolution.

Securing the IOS

To secure User EXEC to your console port

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password password
```

To secure User EXEC to your aux port

```
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password password
```

To secure User EXEC to all five telnet lines

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password password
```

To secure access to Privileged EXEC

```
Router(config)#enable secret password
Router(config)#enable password password
```

The `enable secret` global configuration command encrypts the password using a MD5 hash. If the `enable secret` and the `enable password` commands are used at the same time, the `enable secret` password is used.

To encrypt the enable password and the line passwords, use the `service password-encryption` command.

Interface Configuration Commands

TABLE FF.19 Interface Configuration Commands

Command	Description
`ip address ip subnetmask`	Assigns an IP address to an interface.
`no shutdown`	Administratively enables an interface.
`full-duplex`	Changes the duplex setting to full-duplex.
`clock rate` *`speed`*	Sets the timing speed of the network on a DCE interface in bps.
`bandwidth` *`speed`*	Sets the logical bandwidth setting for routing protocols in Kbps.

Switch Commands

TABLE FF.20 Switch Configuration Commands

Command	Description
`interface range` *`media range`*	Configures several interfaces with the same parameters.
`ip address` *`ipaddress`*	Assigns an IP address to a VLAN interface.
`ip default-gateway` *`ip`*	Sets the gateway of last resort for a Layer 2 switch.
`speed` *`speed`*	Changes the speed of an autosensing link in Mbps.
`duplex` *`duplex`*	Sets the duplex of a switchport.

The `copy` Command

The `copy` command is used to copy files from one location to another. For example, to save the current configuration, we copy the running-config in RAM to the startup-config in NVRAM using the `copy running-config startup-config` command.

The `copy` command is used to copy files between our device and a TFTP server. For instance, `copy flash tftp` will back up the IOS in flash to a TFTP server. `Copy flash tftp` can be used to upgrade, downgrade, or restore an IOS back onto our device. Before copying to a TFTP server, the following preparation steps are in order:

1. The TFTP server must have the TFTP service running.
2. Your device must be cabled correctly. If a switch, plug the TFTP server into the switch with a straight-through ethernet cable. If going directly between a router and the TFTP server, use a cross-over cable.

3. You must have IP connectivity to the server.
4. There must be enough room on the TFTP server and your device's memory to store these files.

The `show` Command

Table F.21 General `show` Commands

Command	Mode	Output
`show running-config`	Privileged	Current active configuration in RAM.
`show startup-config`	Privileged	Configuration stored in NVRAM that will be loaded on reboot.
`show interfaces`	User and Privileged	Status of the interfaces as well as physical and logical address, encapsulation, bandwidth, reliability, load, MTU, duplex, broadcasts, collisions, and frame errors.
`show ip interface brief`	User and Privileged	Status of the interfaces and their logical addresses.
`show controller`	User and Privileged	Microcode of the interface including DCE/DTE cable connection.
`show flash`	User and Privileged	Filenames and sizes of IOS files stored in Flash memory.
`show version`	User and Privileged	IOS version, system uptime, amount of RAM, NVRAM, Flash memory, and configuration register.

Interface Status

TABLE FF.22 Interface Status Values

Layer 1	Layer 2 (line protocol)	Possible Symptoms
Up	Up	None. Interface is functional.
Up	Down	Encapsulation mismatch, lack of clocking on serial interfaces.
Down	Down	Cable is disconnected or attached to a shutdown interface on the far-end device.
Administratively Down	Down	Local interface was not enabled with the `no shutdown` command.

Cisco Discovery Protocol

- Proprietary Cisco Layer 2 protocol that uses multicast to gather hardware and protocol information about directly connected devices.
- Network layer protocol and media independent.
- Enabled by default on all Cisco devices, but can be disabled globally:

```
Router(config)#no cdp run
```

  or can be disabled on interface-by-interface basis:

```
Router(config-if)#no cdp enable
```

- To learn the remote device's Layer 3 address and IOS version

```
Router>show cdp neighbor detail
```

  or

```
Router>show cdp entry *
```

Telnet

Telnet enables a virtual terminal connection to a remote device's IP address using the Application layer protocol, telnet (TCP port 23 at Transport layer).

To telnet from IOS, type the keyword **`telnet`** followed by the IP address or hostname. If you only type an IP address or hostname in User or Privileged EXEC, IOS automatically assumes that you are telnetting. To telnet to a Cisco device, the vty passwords must be set or you will receive the "Password required, but none set" error. To access Privileged EXEC in a telnet session, you must have enable password set or you will receive the "% No password set" error.

- To suspend the telnet session use the Ctrl+Shift+6, x keystroke.
- To see a list of the active sessions in the originating router, use the `show sessions` command.
- To resume a suspended session, press the Enter key from User EXEC or Privileged EXEC, or type **`resume`** followed by the session number.
- To close a telnet session from the device we are telnetted into, type **`exit`** or **`logout`** from User EXEC or Privileged EXEC.
- To close a telnet session from the originating device, type **`disconnect`** followed by the session number.

- To see log messages in your telnet session, use the Privileged EXEC command, `terminal monitor`, in the device that you are telnetted into.

Bridges and Switches

Bridges and switches have the following functions:

- Segment LANs into multiple collision domains.
- Learn MAC addresses by examining the source MAC address of each frame received and store them in a CAM table.
- Base their forwarding decisions based on the destination MAC address of an ethernet frame.
- Flood broadcast, multicast, and unknown unicast frames out all ports except the one it was received.

Switches differ from bridges due to the following:

- Faster hardware-based frame transmissions using ASIC technology
- Greater port density
- VLAN support

A switch has three methods of forwarding frames:

- Store and Forward—Latency varying transmission method that buffers the entire frame and calculates the CRC before forwarding the frame.
- Cut Through—Only looks at the destination MAC address in an ethernet frame and forwards it.
- Fragment Free—Checks the first 64 bytes for frame fragments (due to collisions) before forwarding the fame.

Duplex Connections

- Half-duplex interfaces have one-way communications with sub-optimal throughput because they operate in a collision domain in which CSMA/CD must be enabled. When connected to a hub, they must run half-duplex.

- Full-duplex interfaces simultaneously send and receive, allowing higher throughput because CSMA/CD is disabled. Connections to other switches or devices can be full-duplex.

Spanning Tree Protocol IEEE 802.1d

STP is a Layer 2 protocol that is used to prevent switching loops in networks with redundant switched paths.

TABLE FF.23 STP Port States

State	Function	Transition Time
Disabled	The interface is administratively shut down or disabled from port violation.	NA
Blocking	Does not forward any user data. All ports start out in this state. Does not send, but still can receive BPDUs to react to topology changes.	0–20 seconds
Listening	Begins to transition to a forwarding state by listening and sending BPDUs. No user data sent.	15 seconds
Learning	Begins to build MAC addresses learned on the interface. No user data sent.	15 seconds
Forwarding	User data forwarded.	

STP elects root bridge/switch by determining which switch has the lowest Bridge ID in the topology learned from sending and receiving BPDUs. Bridge ID is a combination of Priority + MAC address.

All non-root switches determine root port based on the fastest (lowest cumulative cost) path back to root switch. If a tie occurs, the Bridge ID followed by port priority and port number are the tie breakers.

On each segment, the switch advertising the fastest way back to the root switch is the designated port for that segment.

If port is not a root or a designated port, it is blocking.

TABLE FF.24 Port Cost Values

Interface	Cost
10Gbps	2
1Gbps	4
100Mbps	19
10Mbps	100

STP Topology Changes and Enhancements

In the event of a topology change, formerly blocked ports might transition to a forwarding state. It might take up to 50 seconds to transition from a blocking state to a forwarding state.

An exception to these 50 seconds is if the following Cisco enhancements are in place to speed up convergence:

- PortFast—Skips listening and learning states on end-devices such as servers, PCs, and printers. PortFast can cause switching loops if a hub or switch is connected. BPDU Guard will add protection by disabling a port if the interface receives a BPDU.
- UplinkFast—Skips the listening and learning transitions when a direct failure occurs on its root port on a switch with redundant uplinks to a distribution switch.
- BackboneFast—Speeds up convergence by skipping the max age time when switches learn of a failure indirectly.

EtherChannel was created for Cisco switches to enable multiple parallel links between two switches to use all the bandwidth by treating them as a logical bundle in which STP will not block the individual links.

STP Configuration

STP is enabled by default for all VLANs in a switch. To change the priority to a lower value for root switch elections, use one of the following commands:

```
Switch(config)#spanning-tree vlan 1 priority 4096
```

or

```
Switch(config)#spanning-tree vlan 1 root
```

Port Security

Configuration that limits the amount of MAC addresses that can be dynamically learned on a switch port:

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
```

If violation occurs, the default response of a Catalyst switch will be to shut down the port.

Virtual LANs (VLANs)

VLANs logically divide a switch into multiple broadcast domains at Layer 2.

Each VLAN can represent a logical grouping of users by function or department. As users in these VLANs move, we simply need to change the VLAN assigned to their switch port. VLANs also enhance security because users in one VLAN cannot communicate to users in another VLAN without the use of a Layer 3 device providing inter-VLAN routing.

VLAN Configuration

VLANs can be statically assigned to switch access ports or dynamically by using a VMPS. By default, all interfaces are assigned to the management VLAN, VLAN 1.

To configure a VLAN

1. The VLAN must be created in the VLAN database.
2. The VLAN must be named.

```
Switch#vlan database
Switch(vlan)#vlan 2 name ExamPrep
VLAN 2 added:
    Name: ExamPrep
Switch(vlan)#exit
APPLY completed
```

3. The desired ports must be added to the new VLAN.

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport access vlan 2
```

Trunks

VLANS can span multiple switches using trunks. Trunks multiplex traffic from all VLANs over a single connection. The VLAN identifier is tagged over trunk using one of the following tagging methods:

- ISL—Cisco proprietary trunk that encapsulates the original Ethernet frame with a 26-byte header and a 4-byte CRC.
- IEEE 802.1q—Standard-based VLAN tagging that inserts a 4-byte tag in the original ethernet frame. Traffic originating from the native VLAN (VLAN 1 by default) will not be tagged over trunk. If native VLAN configuration does not match on both sides, it could cause VLAN leakage.

Trunk Configuration

```
Switch(config)#interface FastEthernet 0/24
Switch(config-if)#switchport trunk encapsulation [isl|dot1q]
Switch(config-if)#switchport mode trunk
```

VLAN Trunking Protocol

Cisco created VTP to minimize the amount of VLAN administration in switches by enabling a VTP server to multicast VTP advertisements to other switches in the same VTP domain. Switches receiving these advertisements will synchronize their VLAN database with the VLAN information advertised from the server, assuming that the revision number is higher.

TABLE FF.25 VTP Modes

Mode	Function
Server	Default VTP mode that enables you to create, modify, and delete VLANS. These VLANs are advertised to other switches and saved in the VLAN database.
Client	Cannot create, modify, or delete VLANs. Will forward advertisements received from server, but does not save VLAN configuration into VLAN database.
Transparent	Creates, modifies, and deletes VLANs only on the local switch. Transparent switches do not participate in VTP, but forwards VTP advertisements received from servers. Also saves VLAN configuration in the VLAN database.

VTP Configuration

```
Switch#vlan database
Switch(vlan)#vtp domain ExamPrep
Changing VTP domain name from null to ExamPrep
Switch(vlan)#vtp password examcram
Setting device VLAN database password to examcram
Switch(vlan)#vtp transparent
Setting device to VTP TRANSPARENY mode.
Switch(vlan)#exit
APPLY completed
```

InterVLAN Routing

InterVLAN routing requires a Layer 3 device such as router or a Layer 3 switch:

- Router on a stick—Connection between router and switch must be at least Fast Ethernet speeds and must be a trunk. Router interface consists of subinterfaces to

assign IP gateway for each VLAN. VLAN is associated with subinterface using the `encapsulation` command.

```
Router(config)#interface FastEthernet 0/1.2
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 2
Router(config)#interface FastEthernet 0/1.3
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 3
```

- Switched Virtual Interfaces—VLAN interfaces configured in Layer 3 switch that enables inter-VLAN routing using ASIC technology.

```
Router(config)#interface Vlan 2
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config)#interface Vlan 3
Router(config-if)#ip address 192.168.3.1 255.255.255.0
```

Routing Characteristics

Packets originating from a non-routing device destined for another network are sent to their default gateway (Layer 3 device on segment). The router consults its routing table to determine if the destination network can be reached. If not, the ICMP Destination Unreachable message is sent to the source. If so, packet is forwarded out interface associated with the destination network in routing table.

Routing Sources

- Connected Interfaces—As soon as we assign an IP address to a working (up/line protocol up) interface, the router associates the entire subnet of the interface's IP address in the routing table.
- Static Routes—These are manual entries that an administrator enters into the configuration that describes the destination network and the next hop (router along the destination path).
- Routing Protocols—Protocols exchanged between routing devices to dynamically advertise networks.

When multiple routing sources are advertising the same IP subnet, the router will use the source with the lowest administrative distance.

TABLE FF.26 Default Administrative Distances

Routed Source	Default Distance
Connected	0
Static Route	1
EIGRP (internal)	90
IGRP	100
OSPF	110
ISIS	115
RIPv1 and v2	120
EIGRP (external)	170

Static and Default Routes

Static routes are useful in stub networks in which we want to control the routing behavior by manually configuring destination networks into the routing table.

```
Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.2.5
```

A floating static route can be configured when redundant connections exist and you want to use the redundant link if the primary fails. This is configured by adding a higher administrative distance at the end of a static route.

```
Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.2.9 2
```

A default route is a gateway of last resort for a router when there isn't a specific match for an IP destination network in the routing table (such as packets destined for the Internet).

```
Router(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0
```

With routing protocols, you can specify a default network, which is a network in the routing table that routing devices will consider as the gateway of last resort. Using their routing protocols, they will determine the best path to the default network.

```
Router(config)#ip default-network 192.168.1.0
```

Dynamic Routing Protocols

In complex networks with multiple pathways to destinations, dynamic routing protocols enable routers to advertise their networks to each other and dynamically react to topology changes.

Routing protocols determine the best path based on the lowest metric.

Routing Metrics

Because one of the core responsibilities of routing protocols is to build routing tables to determine optimal routing paths, we need to have some means of measuring which routes are preferred when there are multiple pathways to a destination. Routing protocols use some measure of metrics to identify which routes are optimal to reach a destination network. The lowest cumulative metric to a destination is the preferred path and the one that ultimately enters the routing table. Different routing protocols use one or several of the following metrics to calculate the best path.

TABLE FF.27 Routing Metrics

Metric	Description
Hop count	The number of routing devices that the packet must travel to reach a destination network
Bandwidth	The cumulative bandwidth of the links to the destination in kilobits per second
Delay	The length of time (measured in microseconds) a packet takes from source to destination
Reliability	The consistency of the links and paths toward the destination based on error rates of the interfaces
Load	The cumulative amount of congestion or saturation of the links toward the destination
MTU	The maximum frame size that is allowed to traverse the links to the destination
Cost	An arbitrary number typically based on the bandwidth of the link

Interior and Exterior Gateway Routing Protocols

- Interior Gateway Routing Protocols—IG routing protocols advertise networks and metrics within an autonomous system.
- Exterior Gateway Routing Protocols—EG routing protocols advertise networks in between autonomous systems.

Classful and Classless Routing Updates

- Classful Routing—The routing updates only contain the classful networks without any subnet mask. Summarization is automatically done when a router advertises a network out an interface that is not within the same major subnet. Classful routing protocols must have a FLSM design and will not operate correctly with discontiguous networks.
- Classless Routing—The routing updates can contain subnetted networks since the subnet mask is advertised in the updates. Route summarization can be manually configured at any bit boundary. Classless routing protocols support VLSM designs and discontiguous networks.

Routing Protocol Classes

- Distance Vector—The entire routing table is periodically sent to directly connected neighbors regardless of a topology change. These routing protocols manipulate the routing table updates before sending that information to their neighbors and are slow to converge when a topology change occurs.
- Link State—All possible link states are stored in an independent topology table in which the best routes are calculated and put into the routing table. The topology table is initially synchronized with discovered neighbors followed by frequent hello messages. These routing protocols are faster to converge than distance vector routing protocols.
- Hybrid—By using the best characteristics from link-state and routing protocols, these advanced routing protocols efficiently and quickly build their routing information and converge when topology changes occur.

Redistribution

Redistribution is the method of configuring routing protocols to advertise networks from other routing protocols:

- One-way redistribution—Networks from an edge protocol are injected into a more robust core routing protocol, but not the other way around. This method is the safest way to perform redistribution.
- Two-way redistribution—Networks from each routing protocol are injected into the other. This is the least preferred method because it is possible that suboptimal routing or routing loops might occur because of the network design or the difference in convergence times when a topology change occurs.

Distance Vector Routing Loop Mitigation

Distance vector routing protocols contain several measures to prevent routing loops:

- Maximum Hop Counts—To ensure that routing metrics do not increment until infinity in a routing loop, distance vector routing protocols have a maximum hop count.

TABLE FF.28 Maximum Hop Counts

Protocol	Distance Vector/Link State/Hybrid	Maximum Hop Count
RIPv1	Distance Vector	15
RIPv2	Distance Vector	15
IGRP	Distance Vector	100/255
EIGRP	Hybrid	224
OSPF	Link State	Infinite

- Split Horizon—Subnets learned from neighbor routers should not be sent back out the same interface from which the original update came.
- Route Poisoning with Poison Reverse—When a route to a subnet fails, the subnet is advertised with an infinite metric. Routers receiving the poisoned route will override the split horizon rule and send a poison reverse back to source.
- Hold-Down Timers—The amount of time a router will ignore any information about an alternative route with a higher metric to a poisoned subnet.
- Flash Updates/Triggered Updates—When a route fails, the router will immediately shoot out an update as opposed to waiting for a normal update interval.

RIP and RIPv2

TABLE FF.29 RIP and RIPv2 Comparison

	RIPv1	RIPv2
Classful/Classless	Classful	Both
Algorithm	Bellman-Ford	Bellman-Ford
Metric	Hops	Hops
Maximum Hop Count	15	15
Infinite Metric	16	16
Hello/Dead Time	30/180	30/180
Updates	Broadcast	Multicast (224.0.0.9)
Update Authentication	No	Yes
Load Balancing	Equal Paths	Equal Paths

RIP Configuration

The configuration for RIP is seamless as long as you remember these two simple rules:

1. Only advertise your directly connected networks.
2. Only advertise the classful network.

```
Router(config)#router rip
Router(config-router)#network 192.168.7.0
Router(config-router)#network 172.17.0.0
```

RIPv2 Configuration

```
Router(config)#router rip
Router(config-router)#network 192.168.7.0
Router(config-router)#network 172.17.0.0
Router(config-router)#version 2
Router(config-router)#no auto-summary
```

Verifying and Troubleshooting RIP

TABLE FF.30 Verifying and Troubleshooting RIP Commands

Command	Output
`show ip route`	The routing table with RIP entries represented as "R"
`show ip protocols`	RIP timers, advertised networks
`debug ip rip`	Real-time display of RIP routing updates being sent and received

Before using any `debug` commands, verify the processor utilization using the `show processes` command.

IGRP

TABLE FF.31 IGRP Characteristics

	IGRP
Classful/Classless	Classful
Algorithm	Bellman-Ford
Metric	Composite (Bandwidth+Delay) by default. Can support Load, Reliability, and MTU.
Maximum Hop Count	100/255
Infinite Metric	4,294,967,295
Hello/Dead Time	90/270

TABLE FF.31 *Continued*

	IGRP
Updates	Broadcast
Cisco or Standard	Cisco
Load Balancing	Unequal Paths

IGRP Configuration

IGRP uses the concept of autonomous system numbers in the configuration. These autonomous system numbers must match in all configured Cisco routing devices.

```
Router(config)#router igrp 100
Router(config-router)#network 192.168.7.0
Router(config-router)#network 172.17.0.0
```

IGRP is capable of routing over unequal paths using the `variance` command. This enables the router to load balance over any path that has a metric of the multiplier multiplied by the lowest cumulative metric to a subnet.

```
Router(config-router)#variance 10
```

Verifying and Troubleshooting IGRP

TABLE FF.32 Verifying and Troubleshooting IGRP Commands

Command	Output
`show ip route`	The routing table with IGRP entries represented as "I"
`show ip protocols`	IGRP timers, autonomous system, advertised networks
`debug ip igrp transactions`	Real-time display of IGRP routing updates being sent and received
`debug ip events`	Real-time summary display of IGRP of the updates that are being sent and received

OSPF Characteristics

TABLE FF.33 OSPF Characteristics

	OSPF
Classful/Classless	Classless
Algorithm	Dijkstra SPF

TABLE FF.33 *Continued*

	OSPF
Metric	Cost (10^8/Bandwidth bps)
Maximum Hop Count	None
Areas or Autonomous System Configuration	Areas
Hello/Dead Time	10/40, 30/120
Cisco or IETF	IETF
Updates	Multicast (224.0.0.5, 224.0.0.6)
Load Balancing	Equal Paths
Routed Protocols	IP

OSPF is a link-state routing protocol that automatically discovers its neighbors by sending hello messages to 224.0.0.5. After the neighbors are discovered, they form an adjacency by synchronizing their databases. This database lists all possible routes that the neighbor is aware of in the topology. Each subnet learned has a cost associated with it which is calculated by taking 10^8/bandwidth. The paths with the lowest cost to a destination are put in the routing table.

TABLE FF.34 Cost Values Based on Bandwidth

Bandwidth	OSPF Cost
56Kbps	1785
64Kbps	1562
T1 (1.544 Mbps)	64
Ethernet (10 Mbps)	10
Fast Ethernet (100 Mbps)	1
Gigabit Ethernet (1000 Mbps)	1

OSPF uses areas to limit the size of the topology table for devices inside that area, which allows for smaller updates and faster convergence. ABRs that sit on the border of these areas have a hierarchically function over other routers because they manually summarize networks to the rest of the OSPF autonomous system. The result of this summarization is a smaller topology and routing table because the individual subnets are not being advertised. In addition, topology changes are confined inside the area where the change occurred because other areas are not aware of the individual subnets.

Areas can be numbered from 0–65535. Area 0 is known as the backbone area in which all other areas must connect. An area can be configured as a stub area in which ABRs will advertise default routes instead of summarized networks into an area to minimize the topology and route tables.

In broadcast and non-broadcast multi-access topologies, OSPF decreases the amount of update overhead by electing a DR and BDR. The DR and BDR are determined by the router that has the highest priority. In the case of a tie, the highest Router ID is a tiebreaker.

The Router ID is determined by the highest active loopback IP address that is configured when the OSPF process starts. The loopback interface is a virtual interface that does not go down unless the router is turned off. In the absence of any loopback interfaces, the highest active physical IP address is used. It is common to use a host mask (255.255.255.255) on a loopback interface.

When a topology change occurs, the update is sent to the DR and BDR to the 224.0.0.6 multicast address. The DR is responsible for sending that update to the rest of the OSPF routers by multicasting the update to 224.00.5. When a device receives an update, it immediately floods it to its neighbors before calculating the topology change.

OSPF Configuration

The first step should be to configure the loopback interface to establish the Router ID.

```
Router(config)#interface loopback 0
Router(config-if)#ip address 10.1.42.1 255.255.255.255
```

You must specify an OSPF process ID between 1 and 65535. The OSPF process ID identifies a unique instance of an OSPF process and is locally significant (does not have to match in all routers in the OSPF autonomous system).

```
Router(config)#router ospf 1
```

To associate the networks to OSPF areas, you must specify the network followed by the wildcard mask and the area.

```
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

The area can be designated as a stub area as long as there is only one pathway in and out of the area.

```
Router(config-router)#area 1 stub
```

To change the cost of a link on an interface, you must navigate to the interface and use the following command:

```
Router(config-if)#ip ospf cost 30
```

On broadcast and non-broadcast multi-access topologies, you should configure force the election by changing the default OSPF priority on the interface:

```
Router(config-if)#ip ospf priority 5
```

Verifying and Troubleshooting OSPF

TABLE FF.35 Verifying and Troubleshooting OSPF Commands

Command	Output
`show ip route`	The routing table with OSPF entries represented as "O." Routes learned from other areas will also have an inter-area indicator ("IA").
`show ip protocols`	OSPF process ID and advertised networks.
`show ip ospf interface`	Local router's Router ID, interface topology type, link cost and priority, Router ID for the DR and BDR on the segment, hello/dead intervals, and a count of how many neighbors and adjacencies.
`show ip ospf neighbor`	Neighbor table to verify neighbor IDs and if neighbor is DR or BDR.
`show ip ospf database`	OSPF subnets and advertising routers in topology table.
`debug ip ospf events`	Real-time display of LSAs and LSUs being sent and received.

EIGRP Characteristics

TABLE FF.36 EIGRP Characteristics

	EIGRP
Classful/Classless	Both
Algorithm	DUAL
Metric	32-bit Composite (Bandwidth+ Delay)
Maximum Hop Count	224
Areas or Autonomous System Configuration	Autonomous Systems
Hello/Dead Time	5/15, 60/180
Cisco or IETF	Cisco
Load Balancing	Unequal Paths
Routed Protocols	IP, IPX, AppleTalk
Redistribution	Automatic with matching IGRP autonomous system number
Administrative Distance	90 for internally learned networks
	170 for externally learned networks
Updates	Multicast (224.0.0.10)

In the EIGRP topology table, it maintains the advertised distance and the feasible distance to every subnet. The subnet(s) with the lowest feasible distance is the route that is placed in the routing table known as the successor route. If the advertised distance of an alternate route is lower than the feasible distance of the successor route, it is a feasible successor, which will be

used if the successor route fails. This is why EIGRP's DUAL algorithm makes it the fastest converging routing protocol.

In cases in which there isn't a feasible successor, the route will go from a passive state to an active state. The state is active because the router is actively querying its neighbor for alternate paths to the destination. If a reply indicates an alternate path, that link will be used.

EIGRP Configuration

Similar to IGRP, EIGRP uses the concept of autonomous system numbers in the configuration. These autonomous system numbers must match in all configured Cisco routing devices.

```
Router(config)#router eigrp 100
Router(config-router)#network 192.168.7.0
Router(config-router)#network 172.17.0.0
```

EIGRP can also load balance over unequal paths using the `variance` command:

```
Router(config-router)#variance 10
```

Similar to RIPv2, EIGRP can be configured as classless supporting VLSM, discontiguous networks, and manual route summarization:

```
Router(config-router)#no auto-summary
```

Verifying and Troubleshooting EIGRP

TABLE FF.37 Verifying and Troubleshooting EIGRP Commands

Command	Output
`show ip route`	The routing table with OSPF entries represented as "D." External route entries learned from redistribution also have an "EX" indicator.
`show ip protocols`	EIGRP autonomous system and advertised networks.
`show ip eigrp neighbors`	Neighbor table to verify neighbors in neighbor table.
`show ip eigrp topology`	EIGRP-learned subnets and the calculated successors for each subnet based on lowest composite metric.
`debug ip eigrp`	Real-time display of hellos and updates being sent and received.

Cisco Access Lists

Access lists are a Cisco configuration paramount to enabling your router to do any major task. The following facts are relevant to access lists:

A Cisco access list is nothing more than an ordered list of permit and deny statements.

They are read by the router in a top-down format; as soon as a match condition is reached, the access list stops processing.

If you reach the end of an access list and have not been explicitly permitted, you will be implicitly denied.

Numbered and named access lists do not allow you to reorder statements; however, named access lists allow you to delete individual access list lines.

Access lists have a number of functions on the Cisco router. The primary access lists uses are

- Packet Filtering
- Quality of Service (QoS)
- Dial on Demand Routing
- Network Address Translation (NAT)
- Route filtering

There are two types of IP-based access lists:

- Standard access lists are capable of filtering traffic based only on the source IP address.
- Extended access lists are capable of filtering traffic based on protocol, source address, source port number, destination address, and destination port number.

IP Standard access lists use numbers <1–99> and IP Extended access lists use numbers <100–199>.

The configuration of a standard access list uses the following syntax:

```
Router(config)#access-list <1-99> <permit/deny> <source_IP_address> <wildcard_mask>
```

The following configuration creates access list 25, which permits a single host (10.1.1.5) and the 192.168.1.0/24 subnet:

```
Router(config)#access-list 25 permit 10.1.1.5 0.0.0.0
Router(config)#access-list 25 permit 192.168.1.0 0.0.0.255
```

As a shortcut, you can use the `host` keyword instead of a wildcard mask of 0.0.0.0 and the `any` keyword instead of a wildcard mask of 255.255.255.255. The following example shows these keywords in action:

```
Router(config)#access-list 25 permit host 10.1.1.5
Router(config)#access-list 25 deny any
```

When looking to apply an access list to an interface, remember the mantra:

One access list

- per protocol
- per interface
- per direction

When trying to find what direction to apply an access list, picture yourself as a router. Hold out an arm to represent an interface. If the traffic is moving away from your body, it should be applied `out` (outbound) on the interface. If the traffic is coming into your body, it should be applied `in` (inbound) on the interface. Standard access lists are always applied closest to the destination. Extended access lists are always applied closest to the source.

The following is the generic syntax used to apply access lists to an interface:

```
Router(config-if)#ip access-group <access-list_number> <in/out>
```

The following configuration applies access list 25 in the inbound direction:

```
Router(config-if)#ip access-group 25 in
```

Access lists can also be applied to VTY ports to restrict telnet access to your router. The following configuration applies access list 25 to the VTY ports of a router.

```
Router(config)#line vty 0 4
Router(config-line)#access-class 25 in
```

Extended access list configuration gets slightly more complex than a standard access list. The following is the generic syntax used to create an extended access list:

```
Router(config)#access-list <100-199> <permit/deny> <protocol> <source_IP_address>
<wildcard_mask> <source_port_number> <destination_IP_address> <wildcard_mask>
<destination_port_number>
```

There are many IP-based protocols that extended access lists can permit or deny. The following is a list of the protocols you should be familiar with:

- **IP**: Permits or denies source/destination addresses using the entire TCP/IP protocol suite. Using this keyword permits or denies *all* access from a source to a destination.
- **TCP**: Permits or denies source/destination addresses using TCP-based applications. The most common applications include FTP, Telnet, SMTP, and HTTP.
- **UDP**: Permits or denies source/destination addresses using UDP-based applications. The most common applications include DNS and TFTP.
- **ICMP**: Permits or denies source/destination addresses using ICMP-based applications. The most common applications include Echo, Echo-Reply, and Unreachables.

When configuring extended access lists, you will rarely, if ever, know a network device's source port number information. This number is randomly generated by the host's operating system. You should leave it blank for any CCNA-level configuration you perform.

You will need to know these commonly used port numbers for the CCNA exam:

TCP Ports:

- Port 21: FTP
- Port 23: Telnet
- Port 25: SMTP
- Port 80: HTTP
- Port 443: HTTPS

UDP Ports:

- Port 53: DNS
- Port 69: TFTP

The following access list permits a single host (10.1.1.5) to access any destination using port 80 (HTTP):

```
Router(config)#access-list 150 permit tcp host 10.1.1.5 any eq 80
```

The following access list denies a network subnet (172.16.70.0/24) from accessing a single host (172.16.50.100) using port 21 (FTP):

```
Router(config)#access-list 125 deny tcp 172.16.70.0 0.0.0.255 host 172.16.50.100 eq 21
```

Often, you will need to end an access list with a "permit all" statement. The following examples show how to accomplish this:

```
Router(config)#access-list 12 permit any   (standard access list example)
Router(config)#access-list 125 permit ip any any    (extended access list example)
```

Often, a router connected to the Internet will deny all incoming traffic to secure the internal network. However, this prevents internal users from receiving responses to their common web browsing requests. The following extended access list entry permits any return traffic that is a response to a request originated from the internal network:

```
Router(config)#access-list 150 permit tcp any any established
```

You can verify access lists using a few show commands:

- **show running-config**: Shows the full access-list configuration and the interfaces where you have applied them.
- **show ip interface**: Shows the inbound and outbound access lists applied to each interface.
- **show access-lists**: Shows all access lists created on the router and the number of times each entry has been matched.
- **show ip access-lists**: Shows just the IP-based access lists on the router and the number of times each entry has been matched.

Network Address Translation (NAT)

NAT is in use on virtually every Internet-connected router in the world today. This technology acts as a security boundary and Internet address sharing system. The following facts are relevant to NAT.

NAT operates by typically translating private IP addresses to public Internet addresses. The following are the private address ranges as defined by RFC 1918:

- Class A: 10.*X.X.X*
- Class B: 172.16.*X.X*–172.31.*X.X*
- Class C: 192.168.*X.X*

The three primary forms of NAT are as follows:

- **Static NAT**: Allows you to manually map one IP address to another in a one-to-one relationship.
- **Dynamic NAT**: Allows you to define a pool of addresses to be translated along with a pool of addresses they will be translated to.
- **NAT Overload/PAT**: Allows a single Internet IP address to support many internal clients.

The standards bodies have developed many terms to describe the location of an IP address in the world of NAT:

- **Inside Local Addresses**: Refers to everything inside of your network.
- **Inside Global Addresses**: The Internet valid IP address assigned to your router that is directly connected to the Internet.

- **Outside Global Addresses**: A standard, Internet IP address accessible from any host connected to the Internet.
- **Outside Local Addresses**: How an Internet host is seen by the internal network as it is translated through the NAT router into your local network.

The following shows a Static NAT configuration fully translating 192.168.1.50 (on the internal network) to 5.1.1.10 (on the Internet). It then shows a single Static NAT port translation mapping 192.168.1.150 port 53 (DNS) on the internal network to 5.1.1.11 port 53 on the Internet:

```
NAT_Router(config)#interface fastethernet0
NAT_Router(config-if)#ip nat inside
NAT_Router(config)#interface serial0
NAT_Router(config-if)#ip nat outside
NAT_Router(config)#ip nat inside source static 192.168.1.50 5.1.1.10
NAT_Router(config)#ip nat inside source static udp 192.168.1.150 53 5.1.1.11 53
```

The following shows a NAT Overload/PAT configuration translating the entire internal network (192.168.1.0/24) to a single Internet address assigned to the Serial0 interface:

```
NAT_Router(config)#interface fastethernet0
NAT_Router(config-if)#ip nat inside
NAT_Router(config)#interface serial0
NAT_Router(config-if)#ip nat outside
NAT_Router(config)#access-list 50 permit 192.168.1.0 0.0.0.255
NAT_Router(config)#ip nat inside source list 50 interface serial0 overload
```

Wide Area Networks

Wide area network (WAN) connections tie together geographically distant locations, enabling them to communicate as if directly connected. The following facts are relevant to WANs.

WAN technologies only encompass the Physical and Data Link layers of the OSI model. The three major categories of WAN technology used to connect networks today are as follows:

- **Leased Lines**: Provides a dedicated, point-to-point link between two locations.
- **Circuit Switched Networks**: Establishes a dedicated channel (or circuit) for the duration of the transmission, and then tears down the channel when the transmission is complete.
- **Packet Switched Networks**: Enables the service provider to create a large pool of bandwidth for its clients who establish connections through the shared bandwidth using virtual circuits.

Cisco routers connect to most WAN connections through their serial ports. The Cisco side of the connection will use either a DB-60 or Smart Serial port. The CSU/DSU that the Cisco router connects to will have one of five standard connectors: V.35, X.21, EIA/TIA-232, EIA/TIA-449, and EIA/TIA-530.

At the Data Link layer, Cisco routers will primarily use one of two WAN encapsulations for leased line and circuit switched networks:

- **Point-to-Point Protocol (PPP)**: The most popular, industry standard, feature packed protocol for connecting routers
- **Cisco High-level Data Link Control (HDLC)**: A Cisco proprietary, low overhead protocol that makes your WAN connections very efficient between Cisco devices

HDLC is the default encapsulation on all Cisco serial interfaces. However, PPP is used to gain more features and industry standard capabilities when connecting over the WAN. It is made up of three sub-layers:

- **ISO HDLC**: Responsible for enabling PPP to be supported by multiple devices.
- **Link Control Protocol (LCP)**: Feature negotiation layer that performs the following functions:
  - **Authentication**: Requires a username and password for the connecting device.
  - **Call Back**: Enables a dial-up server (or router) running PPP to call back the person who initially dialed into the location using a predefined number.
  - **Compression**: Makes WAN connections more efficient by minimizing the amount of data sent.
  - **Multilink**: Bundles multiple WAN connections (or WAN channels in the case of ISDN) into a single, logical connection.
- **Network Control Protocol (NCP)**: Gives PPP the functionality to enable multiple Network layer protocols to run across a single WAN link at any given time.

When configuring PPP authentication, you can choose between two authentication protocols:

- **Password Authentication Protocol (PAP)**: Sends username and password once in clear-text format when authenticating.
- **Challenge Handshake Authentication Protocol (CHAP)**: Sends a username and hashed password when demanded by the CHAP server.

When configuring PPP compression, you can choose between three compression types:

- **Stacker**: A flat compression algorithm that is notoriously heavy on CPU resources and has less effect on the router's memory resources. Useful for WAN links with many traffic patterns.
- **Predictor**: A dictionary-based compression algorithm that is notoriously heavy on memory resources and has less effect on the router's CPU resources. Useful for WAN links with similar traffic patterns.
- **Microsoft Point-to-Point Compression (MPPC)**: Used for Microsoft Windows dial-up clients wanting to use compression.

To activate PPP encapsulation on an interface, use the following syntax:

```
Router(config)#interface serial 0
Router(config-if)#encapsulation ppp
```

When adding CHAP authentication to your configuration, you need to ensure that you create a user account that matches the hostname of the other side of the connection. In addition, the passwords must be the same on both sides. Here is a PPP CHAP authentication configuration between the Kirk and Spock routers:

```
Kirk(config)#username Spock password cisco
Kirk(config)#interface serial 0
Kirk(config-if)#encapsulation ppp
Kirk(config-if)#ppp authentication chap

Spock(config)#username Kirk password cisco
Spock(config)#interface serial 0
Spock(config-if)#encapsulation ppp
Spock(config-if)#ppp authentication chap
```

In order to enable PPP compression on an interface, you can use the following syntax:

```
Router(config-if)#compress  ?
  mppc       MPPC compression type
  predictor  predictor compression type
  stac       stac compression algorithm
```

The `show interface` command is one of the most useful when verifying the PPP configuration. The connection is active when the LCP Open tag is seen as shown here:

```
Router#show interface serial 0
Serial0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.2.2.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP Open
  Open: IPCP, CCP, CDPCP
```

When troubleshooting PPP authentication issues, use the `debug ppp authentication` command to observe the authentication process as it occurs.

Integrated Services Digital Network (ISDN)

ISDN has been slowly declining in popularity in the United States. Because of this, Cisco has limited the amount of ISDN content on its certification exams. Here are the relevant facts regarding ISDN.

ISDN was originally designed to *integrate* multiple services (voice and data) through a single medium. ISDN connections are built using a combination of Bearer (B)-channels and a Delta (D)-channel. B-channels (always 64Kbps) can be used to send or receive data. D-channels (64Kbps or 16Kbps) are used to send signaling data.

ISDN connections come in two primary flavors: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI is composed of two 64Kbps B-channels and one 16Kbps D-channel. PRI is composed of 23 64Kbps B-channels and one 64Kbps D-channel.

ISDN uses two signaling protocols over the D-channel:

- **Q.921**: Used to send Data Link (Layer 2) messages between the customer premise equipment (CPE) and the service provider
- **Q.931**: Used to send Network (Layer 3) messages between the two customer-connected routers

When architecting an ISDN connection, it is key to understand the different pieces of an ISDN network:

Equipment:

- **Network Termination, Type 1 (NT-1)**: Converts from the two-wire ISDN line the service provider installs in your location to a four-wire connection that your internal devices can use.

- **Network Termination, Type 2 (NT-2)**: This optional device allows you to either split the ISDN signal or aggregate multiple ISDN connections into a single stream.
- **Terminal Endpoint, Type 1 (TE1)**: This is an ISDN compatible endpoint, such as a router with an ISDN S/T or U interface.
- **Terminal Endpoint, Type 2 (TE2)**: This is an non-ISDN compatible endpoint, such as a router with no ISDN interfaces or an end-user PC, requiring a Terminal Adapter (TA) to understand the ISDN signal, such as a router with no ISDN interfaces or an end-user PC.
- **Terminal Adapter (TA)**: This device converts an ISDN signal into some other type of signaling.

Reference Points:

- **U**: Identifies the connection leading up to the NT-1 device.
- **T**: Identifies the connection between the NT-1 and NT-2 devices.
- **S**: Identifies the connection between the NT-2 and TE1 devices.
- **R**: Identifies the connection between the TA and TE2 devices.

The first step in configuring an ISDN interface is to set the ISDN switch type of your router to that of your service provider. This can be done from either global configuration mode or interface configuration mode using the following syntax:

```
Router(config)#isdn switch-type ?
  basic-1tr6    1TR6 switch type for Germany
  basic-5ess    AT&T 5ESS switch type for the U.S.
  basic-dms100  Northern DMS-100 switch type
  basic-net3    NET3 switch type for UK and Europe
  basic-ni      National ISDN switch type
  basic-ts013   TS013 switch type for Australia
  ntt           NTT switch type for Japan
  vn3           VN3 and VN4 switch types for France
  <cr>
```

Most ISDN service providers will require SPID information to be added to the dialup syntax for billing purposes. Use the following syntax to configure SPIDs on your router:

```
Router(config-if)#isdn spid1 <number>
Router(config-if)#isdn spid2 <number>
```

Because ISDN must dial in order to make a connection to another location, Dial on Demand Routing (DDR) is frequently used to initiate the connection. Here is a complete DDR configuration example between the GreenEggs and Ham routers:

```
GreenEggs(config)#interface BRI0
GreenEggs(config-if)#ip address 10.1.1.1 255.255.255.0
GreenEggs(config-if)#encapsulation ppp
GreenEggs(config-if)#dialer map ip 10.1.1.2 broadcast 48022222222
GreenEggs(config-if)#dialer-group 1
GreenEggs(config-if)#isdn spid1 111
GreenEggs(config-if)#isdn switch-type basic-5ess
GreenEggs(config)#dialer-list 1 protocol ip permit

Ham(config)#interface BRI0
Ham(config-if)#ip address 10.1.1.2 255.255.255.0
Ham(config-if)#encapsulation ppp
Ham(config-if)#dialer map ip 10.1.1.1 broadcast 4801111111
Ham(config-if)#dialer-group 1
Ham(config-if)#isdn spid1 222
Ham(config-if)#isdn switch-type basic-5ess
Ham(config)#dialer-list 1 protocol ip permit
```

The two best show commands for ISDN are `show dialer` and `show isdn status`. The `show dialer` command displays the DDR information, and the `show isdn status` command shows the status of the bottom three layers of the OSI model for the ISDN connection.

Dialer profiles enhance the traditional DDR configuration by applying alternate interface settings for each location dialed. The following is a sample dialer profile configuration for two locations on a router equipped with two BRI interfaces:

```
Router(config)#interface dialer 1
Router(config-if)#description CONNECTION TO R1
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#encapsulation ppp
Router(config-if)#dialer pool 50
Router(config-if)#dialer string 4802222222
Router(config-if)#dialer-group 1
Router(config)#interface dialer 2
Router(config-if)#description CONNECTION TO R2
Router(config-if)#ip address 172.16.1.2 255.255.255.0
Router(config-if)#encapsulation ppp
Router(config-if)#dialer pool 50
Router(config-if)#dialer string 4803333333
Router(config-if)#dialer-group 1
Router(config)#interface bri 0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication chap
Router(config-if)#dialer pool-member 50
Router(config-if)#exit
```

```
Router(config)#interface bri 1
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication chap
Router(config-if)#dialer pool-member 50
```

The ISDN interface will remain connected as long as it sees interesting traffic passing along the connection. The `dialer idle-timeout` command can be used to tell the router how long it should wait without seeing interesting traffic before disconnecting the DDR connection.

Frame Relay

Frame Relay is the only packet switched network tested on the CCNA exam. It is one of the more popular connections in businesses today. The following facts are relevant to Frame Relay.

Frame Relay offers the high-speeds demanded by the networks of today at cut-rate prices. Rather than connecting sites together through individual physical interfaces, Frame Relay connects sites together using Virtual Circuits. Virtual Circuits are logical links through service provider networks that give routers the impression that they are linked directly together. The more Virtual Circuits purchased to connect network locations, the more redundant the network connections will be; at the same time, the monthly cost will rise significantly. Because of this, there are three design strategies to provisioning Virtual Circuits:

- **Hub and Spoke**: A centralized location (most likely, your largest, most connected office) acts as the "hub" of the network. All other locations will be considered "spokes" and will have a single Virtual Circuit connection back to the hub.
- **Partial Mesh**: Key network sites will have redundant Virtual Circuit connections through the Frame Relay cloud. Other non-critical sites might only have a single Virtual Circuit.
- **Full Mesh**: Every site has a direct Virtual Circuit to every other site in the network.

Frame Relay also introduces another set of terminology CCNA candidates should be familiar with:

- **Permanent Virtual Circuit (PVC)**: A permanently "nailed-up" circuit through the Frame Relay service provider network
- **Switched Virtual Circuit (SVC)**: An "on-demand" connection through the Frame Relay cloud
- **Local Management Interface (LMI)**: Signaling between your router and the Frame Relay service provider

- **Data Link Connection Identifier (DLCI)**: The Data Link layer addressing used by Frame Relay to identify endpoints connected to the Frame Relay service provider
- **Local Access Rate**: The maximum physical speed that a Frame Relay connection can attain
- **Committed Information Rate (CIR)**: Minimum speed the service provider commits to give you for a Virtual Circuit at all times
- **Backward Explicit Congestion Notification (BECN)**: A message sent by the service provider notifying a router sending at an excessive data rate to reduce its speed
- **Forward Explicit Congestion Notification (FECN)**: A message sent by the service provider notifying a receiving router to send information that can be tagged as a BECN to tell a router sending at an excessive data rate to reduce its speed
- **Discard Eligible (De)**: Describes any traffic that you send above the CIR you have purchased

In order to provide more logical configurations, Cisco routers can create multiple subinterfaces that can connect to any number of virtual circuits. The two types of subinterfaces that can be created are as follows:

- **Point-to-Point Subinterfaces**: Assigned to a single Virtual Circuit. Only one DLCI number assigned per point-to-point subinterface.
- **Multipoint Subinterfaces**: Assigned to one or more Virtual Circuits. Numerous DLCI numbers can be mapped under a multipoint subinterface.

Using multipoint interfaces or the physical Serial interface for multiple Virtual Circuits causes known problems with the Distance Vector routing protocol loop prevention mechanism, Split Horizon.

Cisco routers will initially receive a list of DLCIs they can reach from the Frame Relay service provider. There are two ways it can map the DLCI number to the remote IP address it can reach at the other end of the connection:

- **Inverse ARP**: Enables the router to send messages down each one of the DLCI numbers to discover the router's IP address on the remote end.
- **Static Mappings**: Allows the Cisco administrator to manually map each DLCI number to the router's IP address on the remote end.

Understanding the states of a Frame Relay PVC can be quite useful in both the real world and the testing environment:

- **Active**: PVC is successfully connected through between the two endpoints (routers). This is the normal state if everything is working properly.
- **Inactive**: PVC is working properly on your end of the connection (the local side); however, the other side of the connection is either not configured or offline.
- **Deleted**: PVC is having problems at your side (local side) of the connection. Most likely, you are attempting to use a DLCI number that the service provider has not configured.
- **Static**: PVC has been manually entered by you (the administrator) rather than being dynamically discovered from the service provider.

Configuring a Frame Relay interface for a single Virtual Circuit requires the following minimal configuration:

```
Router(config)#interface serial 0
Router(config-if)#encapsulation frame-relay
```

If you are connecting to a non-Cisco router through the Frame Relay cloud, use the command `encapsulation frame-relay ietf` to enable your interface with the industry standard Frame Relay encapsulation.

If you are using an extremely old version of the IOS (any version earlier than 11.2), the router is unable to auto-detect what LMI language the service provider is using. This means that you must manually configure it using the following syntax:

```
Router(config-if)#frame-relay lmi-type ?
  cisco
  ansi
  q933a
```

The following is a sample configuration of a multipoint interface using static Frame Relay maps. In this case, 192.168.5.1 is the remote end IP address and DLCI 405 is used to get there. Likewise, 192.168.5.2 is another remote end router that can be reached through DLCI 406:

```
Router(config)#interface serial 0/0.10 multipoint
Router(config-if)#frame map ip 192.168.5.1 405 broadcast
Router(config-if)#frame map ip 192.168.5.2 406 broadcast
```

The following is a sample configuration using the same setup as the previous example, but using point-to-point interfaces:

```
Router(config)#interface serial 0/0.405 point-to-point
Router(config-if)#frame-relay interface-dlci 405
Router(config)#interface serial 0/0.406 point-to-point
Router(config-if)#frame-relay interface-dlci 406
```

When troubleshooting Frame Relay connections, start with the `show frame-relay lmi` command to check connectivity to the service provider. From there, use `show frame-relay pvc` to check the status of the Virtual Circuits.

Practice Exam

CCNA

Exam Questions

1. You are trying to enter a command in the IOS, and you receive the following console message: "Invalid input detected at ^." What should you do to correct this?

   - ❍ **A.** Enter more characters for the IOS to understand the command.
   - ❍ **B.** Enter more keywords so that the IOS understands what you want to do with the command.
   - ❍ **C.** Check your typing syntax.
   - ❍ **D.** Check your console connection.

2. According to the following access list, what would happen to a packet coming from the source address 192.168.5.67?

```
access-list 50 permit 192.168.5.16 0.0.0.15
access-list 50 permit 192.168.5.32 0.0.0.15
access-list 50 permit 192.168.5.48 0.0.0.7
access-list 50 permit 192.168.5.0 0.0.0.0
```

   - ❍ **A.** The packet would be denied because of the implicit deny statement.
   - ❍ **B.** The packet would be permitted because of the `permit 192.168.5.32 0.0.0.15` statement.
   - ❍ **C.** The packet would be permitted because of the `permit 192.168.5.48 0.0.0.7` statement.
   - ❍ **D.** The packet would be permitted because of the `permit 192.168.5.0 0.0.0.0` statement.

3. Which of the following are Application layer protocols? (Choose the 3 best answers.)

- ❍ **A.** Telnet
- ❍ **B.** JPEG
- ❍ **C.** HTTP
- ❍ **D.** FTP

4. Which of the following commands will enable you to specify the datagram size in a ping to 10.1.1.1?

- ❍ **A.** Router>**ping -l**
- ❍ **B.** Router#**ping**
- ❍ **C.** Router#**ping 10.1.1.1**
- ❍ **D.** Router>**ping 10.1.1.1**

5. You have an internal web server that must be accessed from the corporate Internet connection. This internal web server has the IP address 172.16.55.10. The router accesses the Internet through the FastEthernet0/1 interface. What NAT syntax is necessary to forward HTTP requests to the internal web server?

- ❍ **A.** ip nat outside destination tcp 80 fastEthernet0/1 172.16.55.10 80
- ❍ **B.** ip nat inside source static tcp 172.16.55.10 80 interface fastEthernet 0/1 80
- ❍ **C.** ip nat outside source tcp 80 172.16.55.10 80 interface fastEthernet0/1 80
- ❍ **D.** ip nat inside destination static tcp 172.16.55.10 80 interface fastEthernet 0/1 80

6. This Application layer protocol resolves hostnames or fully qualified domain names (FQDNs) such as www.cisco.com into IP addresses.

- ❍ **A.** SMTP
- ❍ **B.** NFS
- ❍ **C.** NNTP
- ❍ **D.** DNS

7. Which of the following configuration registers will cause the IOS to boot from Flash if no `boot system` commands are present?

- ❍ **A.** 0x2100
- ❍ **B.** 0x2106
- ❍ **C.** 0x2140
- ❍ **D.** 0x2101

8. When connecting a serial cable from the CSU/DSU to your Cisco router, what two standards are supported on the Cisco end of the connection? (Choose 2.)

- ❍ **A.** EIA/TIA-449
- ❍ **B.** Smart Serial
- ❍ **C.** DB-60
- ❍ **D.** RJ-45

9. Which layer of the OSI model handles dialog control among devices?

- ❍ **A.** Application
- ❍ **B.** Presentation
- ❍ **C.** Session
- ❍ **D.** Transport

10. Which of the following STP 802.11d port states actively learns MAC addresses? (Choose all that apply.)

- ❍ **A.** Blocking
- ❍ **B.** Learning
- ❍ **C.** Listening
- ❍ **D.** Forwarding

11. You are reviewing your device's current configuration. You notice that you have configured different switch type settings for your switch in both Global Configuration mode and Interface Configuration mode. What is the effective switch type?

- ❍ **A.** The global setting overrides all settings.
- ❍ **B.** The interface setting overrides the global setting for that interface.
- ❍ **C.** Neither setting takes effect.
- ❍ **D.** This configuration cannot be created.

12. SNMP uses which port number?

- ❍ **A.** 67
- ❍ **B.** 68
- ❍ **C.** 69
- ❍ **D.** 161

13. At the end of your Setup Mode dialog, you are prompted if you want to keep the configuration that you created. This configuration will be present even if you reboot the device. Where is this configuration stored?

- ❍ **A.** NVRAM
- ❍ **B.** RAM
- ❍ **C.** ROM
- ❍ **D.** Flash

14. Which of the following are valid LMI signaling types? (Choose 3.)

- ❍ **A.** Cisco
- ❍ **B.** ANSI
- ❍ **C.** ITU-T
- ❍ **D.** Q.933a
- ❍ **E.** IETF

15. _____ is an electrical or magnetic field that is a result of one communications signal that can affect the signal in a nearby circuit.

- ❍ **A.** EMI
- ❍ **B.** Attenuation
- ❍ **C.** Crosstalk
- ❍ **D.** Bandwidth

16. Which of the following is not an advantage of areas in OSPF?

- ❍ **A.** ABRs perform automatic summarization.
- ❍ **B.** Smaller topology tables.
- ❍ **C.** Confinement of topology changes.
- ❍ **D.** Speed up convergence.

17. You would like to deny Network 1 (shown in the following figure) from accessing the Internet. Where would be the most efficient location to apply the access list ?

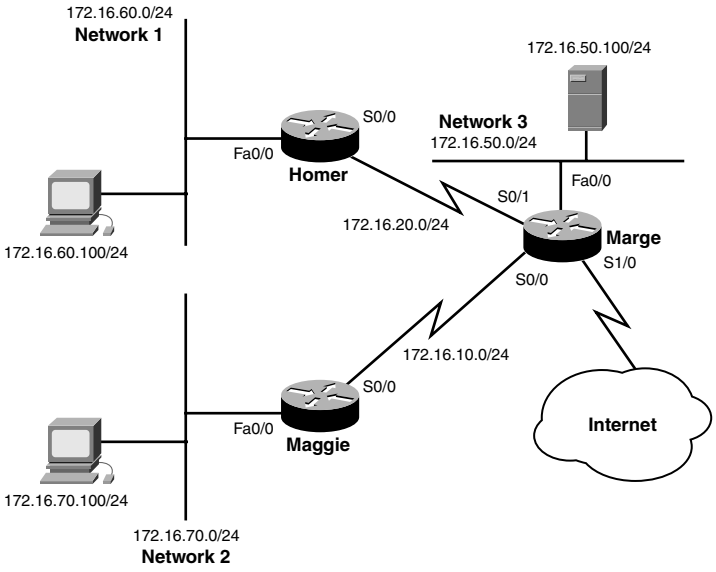


FIGURE PE.1
Applying an access list.

```
access-list 75 deny 172.16.60.0 0.0.0.255
access-list 75 permit any
```

- ❍ **A.** On the Homer router, Fa0/0 inbound
- ❍ **B.** On the Homer router, Fa0/0 outbound
- ❍ **C.** On the Homer router, S0/0 inbound
- ❍ **D.** On the Homer router, S0/0 outbound
- ❍ **E.** On the Marge router, S0/1 inbound
- ❍ **F.** On the Marge router, S0/1 outbound
- ❍ **G.** On the Marge router, S1/0 inbound
- ❍ **H.** On the Marge router, S1/0 outbound

18. What type of UTP cable would you use to connect a switch to a PC?

- ❍ **A.** Coaxial cable
- ❍ **B.** Straight-through cable
- ❍ **C.** Cross-over cable
- ❍ **D.** Thin coax

19. Given the following output, which of the statements is false?

```
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 2 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    Ethernet0        2     2      examprep
    Serial0          2     2
  Routing for Networks:
    172.19.0.0
    10.2.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance:          80
```

- ❍ **A.** The administrative distance has been changed.
- ❍ **B.** This is version 2 of RIP.
- ❍ **C.** Update authentication is configured.
- ❍ **D.** The router configuration looks like the following:

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.2.0.0
Router(config-router)#network 172.19.0.0
```

20. Which of the following forms of NAT allows you to translate one group of IP addresses to another in a 1:1 relationship with minimal configuration?

- ❍ **A.** Port Address Translation
- ❍ **B.** Static NAT
- ❍ **C.** NAT Overload
- ❍ **D.** Dynamic NAT

21. The Ethernet IEEE 802.3 specification defines which of the following LAN standards? (Choose the 3 best answers.)

- ❍ **A.** 10BASE-2
- ❍ **B.** 10BASE-5
- ❍ **C.** 10BASE-T
- ❍ **D.** Wi-Fi

22. Which of the following networks are contained in the summarized CIDR route of 192.168.64.0 /19? (Choose all that apply.)

- ❍ **A.** 192.168.96.0 /24
- ❍ **B.** 192.168.60.0 /24
- ❍ **C.** 192.168.80.0 /24
- ❍ **D.** 192.168.101.0 /24

23. Which of the following encapsulation types can be used on leased line connections? (Choose 2.)

- ❍ **A.** HDLC
- ❍ **B.** Frame Relay
- ❍ **C.** ISDN
- ❍ **D.** PPP

24. Which devices are implemented at the Physical layer of the OSI model? (Choose the 2 best answers.)

- ❍ **A.** Switch
- ❍ **B.** Bridge
- ❍ **C.** Hub
- ❍ **D.** Repeater

25. Which of the following are 802.3 MAC sublayer ethernet addresses? (Choose the 3 best answers.)

- ❍ **A.** IP address
- ❍ **B.** Unicast address
- ❍ **C.** Multicast address
- ❍ **D.** Broadcast address

26. You just added a switch to your VTP domain, and all of your VLANs in the domain vanished. What is a likely cause of this behavior?

- ❍ **A.** The new switch has a higher revision number in client mode.
- ❍ **B.** The new switch has a higher revision number in server mode.
- ❍ **C.** The existing switches have a higher revision number than the new switch.
- ❍ **D.** Someone went to each switch and deleted the VLANs without your knowing.

27. You need to configure the line to disconnect if there have been two minutes of idle activity. What command should you use?

- ❍ **A.** dialer timeout 120
- ❍ **B.** dialer idle-timeout 120
- ❍ **C.** dialer idle 120
- ❍ **D.** dialer line idle 120

28. Which Ethernet MAC 802.3 sublayer address type always starts with the hexadecimal characters 0100.5E?

- ❍ **A.** Unicast address
- ❍ **B.** Multicast address
- ❍ **C.** Broadcast address
- ❍ **D.** IP address

29. You no longer have IP connectivity to a remote router at a customer's site. From your location, what terminal option can you use to gain access to an EXEC session on the remote router?

- ❍ **A.** Console port
- ❍ **B.** Telnet
- ❍ **C.** SSH
- ❍ **D.** Auxiliary port

30. Your manager would like you to convert the company's leased line connections to a Frame Relay topology. He would like to use the lowest cost solution available. What topology should you design?

- ❍ **A.** Full mesh
- ❍ **B.** Partial mesh
- ❍ **C.** Hub and spoke
- ❍ **D.** NBMA

31. _____ occurs when a switch creates a dedicated path for sending and receiving transmissions with each connected host.

- ❍ **A.** Microsegmentation
- ❍ **B.** Half-duplex
- ❍ **C.** Full-duplex
- ❍ **D.** CSMA/CD

32. You want to speed up convergence on switch ports connected to hosts, but you are afraid of someone plugging in a switch or hub and causing a loop. Which two features will address both requirements? (Choose 2.)

- ❍ **A.** BackboneFast
- ❍ **B.** PortFast
- ❍ **C.** UplinkFast
- ❍ **D.** BPDU guard

33. In DDR operation, what is "interesting traffic"?

- ❍ **A.** Traffic signaling a possible attack
- ❍ **B.** Traffic that should be blocked
- ❍ **C.** Traffic that should initiate the connection
- ❍ **D.** Traffic that initiates from the router

34. Which devices are implemented at the Data Link layer of the OSI model? (Choose the 2 best answers.)

- ❍ **A.** Hub
- ❍ **B.** Repeater
- ❍ **C.** Switch
- ❍ **D.** Bridge

35. What range represents the first octet value of a Class A address?

- ❍ **A.** 0–126
- ❍ **B.** 1–126
- ❍ **C.** 128–191
- ❍ **D.** 192–223

36. IGRP routing protocol is advertising the 172.16.0.0 network. In the same autonomous system, RIP is advertising the 10.0.0.0 network. What will the contents of the routing table look like in a router running both routing protocols?

- ❍ **A.** The 10.0.0.0 and the 172.16.0.0 will be learned through IGRP because it has a lower administrative distance.
- ❍ **B.** The 10.0.0.0 and the 172.16.0.0 will be learned through RIP because it has a higher administrative distance.
- ❍ **C.** 10.0.0.0 will be learned through IGRP, and 172.16.0.0 will be learned through RIP.
- ❍ **D.** 10.0.0.0 will be learned through RIP, and 172.16.0.0 will be learned through IGRP.

37. You are configuring the Internet connection for the network pictured in the following figure. The initial NAT Overload configuration has been set up; you must now publish the internal FTP and web server to the Internet. What commands will accomplish this? (Choose 2.)

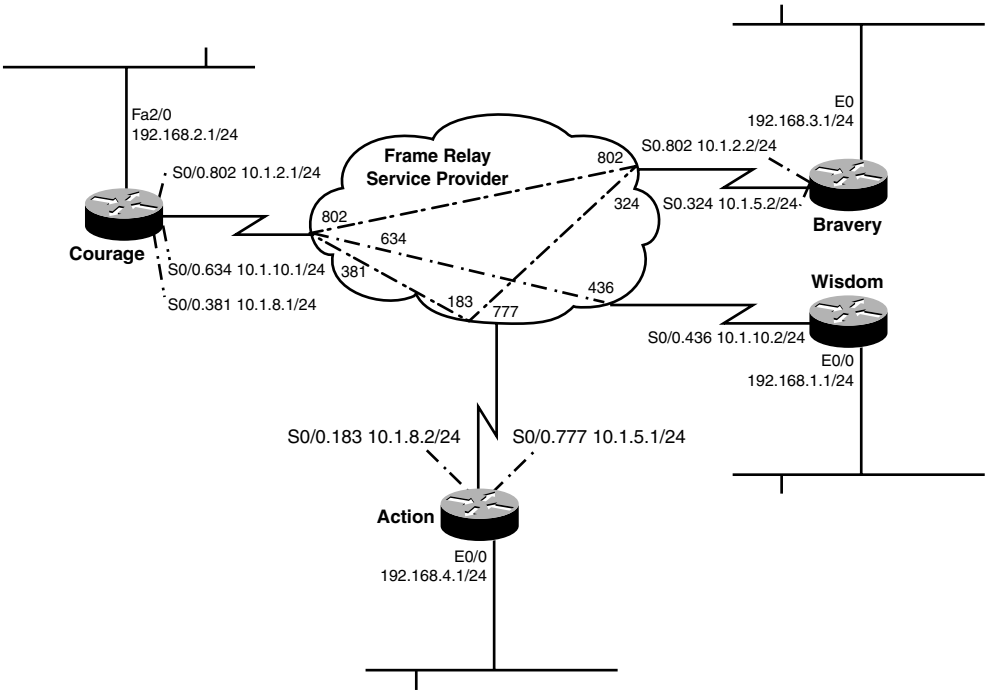


FIGURE PE.2 Publishing NAT Overload addresses.

- ❍ **A.** ip nat inside source static tcp 80 192.168.254.100 80 24.15.240.9
- ❍ **B.** ip nat inside source static tcp 192.168.254.50 20 24.15.240.9 20
- ❍ **C.** ip nat inside source static tcp 192.168.254.50 21 24.15.240.9 21
- ❍ **D.** ip nat inside source static tcp 192.168.254.100 80 24.15.240.9 80
- ❍ **E.** ip nat inside source static tcp 21 192.168.254.50 21 24.15.240.9

38. A _____ can be installed in a router's T1 slot to communicate with and control the 24 DS0 channels.

- ❍ **A.** GBIC
- ❍ **B.** T1 controller card
- ❍ **C.** BRI – NT1
- ❍ **D.** HSSI

39. What is the end result of the 192.168.2.0 network based on the following output?

```
RouterA#debug ip rip
RIP protocol debugging is on
RouterA#
00:26:27: RIP: received v1 update from 192.168.1.6 on Serial0/0
00:26:27:      192.168.2.0 in 12 hops
00:26:37: RIP: received v1 update from 192.168.1.12 on Serial0/1
00:26:37:      192.168.2.0 in 12 hops
```

- ❍ **A.** The router will forward packets to 192.168.1.6 because it received that update first.
- ❍ **B.** The router will forward packets to 192.168.1.12 because it received that update last.
- ❍ **C.** The router will ignore the updates because the maximum hop count is reached.
- ❍ **D.** Both entries will be put in the router, and it will load balance over both links.

40. You need to block a host from Internet access by using an access list. When creating the access list, you use the syntax `access-list 99` to start the command. What type of access list is this?

- ❍ **A.** An IP standard access list
- ❍ **B.** An IP extended access list
- ❍ **C.** An IP standard expanded-range access list
- ❍ **D.** An IP extended expanded-range access list

41. What is 00111000 10110011 01010111 11011010 converted into decimal format?

- ❍ **A.** 56.179.87.217
- ❍ **B.** 56.179.87.218
- ❍ **C.** 56.179.87.219
- ❍ **D.** 56.179.87.220

42. Which of the following is not a difference between IGRP and EIGRP?

- ❍ **A.** EIGRP can only load balance of equal paths.
- ❍ **B.** EIGRP has a 32-bit metric.
- ❍ **C.** EIGRP supports IP, IPX, and AppleTalk.
- ❍ **D.** EIGRP can distinguish between internal and external networks.

43. You are configuring your Cisco 2500 router to connect across the WAN to a Cisco 2600 router. You would like to use the default WAN encapsulation; will this work?

- ❍ **A.** Yes, Cisco routers all support the same WAN encapsulation standards.
- ❍ **B.** Yes, newer Cisco routers support different WAN encapsulation standards, but they are backward compatible with older WAN encapsulation types.
- ❍ **C.** No, newer Cisco routers use PPP as their WAN encapsulation types, while older Cisco routers use HDLC.
- ❍ **D.** No, newer Cisco routers use the industry standard HDLC, while older Cisco routers use a proprietary version.

44. What is the Broadcast IP of 212.84.5.66/26?

- ❍ **A.** 212.84.5.125
- ❍ **B.** 212.84.5.126
- ❍ **C.** 212.84.5.127
- ❍ **D.** 212.84.5.128

45. Which of the statements is true regarding the 10.1.100.0 network based on the following output?

```
CstmrARtr#show ip route
…output omitted…

Gateway of last resort is 192.168.1.9 to network 0.0.0.0

I    10.1.100.0 /24 [100/16] via 192.168.1.9, 00:00:11, Serial0
C    172.17.0.0/16 is directly connected, Ethernet0
I    172.16.0.0/16 [100/2340] via 172.17.0.2, 00:00:02, Ethernet0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.8 is directly connected, Serial0
```

- ❍ **A.** The 10.1.100.0 network is 11 hops away.
- ❍ **B.** Network 10.1.100.0 is configured in a FLSM design.
- ❍ **C.** Serial 0 has an IP address of 192.168.1.9.
- ❍ **D.** The maximum hop count has been reached.

46. Which of the following commands would you type to see the output shown here?

```
PVC Statistics for interface Serial0 (Frame Relay DCE)
       Active   Inactive   Deleted    Static
       Local       1      0      0      0
       Switched    0      0      0      0
    Unused     0      0      0      0

DLCI = 101, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

 input pkts 207      output pkts 239     in bytes 15223
 out bytes 14062     dropped pkts 0      in FECN pkts 0
 in BECN pkts 0      out FECN pkts 0     out BECN pkts 0
 in DE pkts 0       out DE pkts 0
 out bcast pkts 17    out bcast bytes 3264
 PVC create time 00:11:32, last time PVC status changed 00:11:32
Router1#
```

- ❍ **A.** `show frame relay lmi`
- ❍ **B.** `show frame relay pvc`
- ❍ **C.** `show frame relay virtual circuit`
- ❍ **D.** `show frame relay all`

47. What is the Network ID of 212.84.5.66/26?

- ❍ **A.** 212.84.5.0
- ❍ **B.** 212.84.5.64
- ❍ **C.** 212.84.5.128
- ❍ **D.** 212.84.5.192

48. You change the VLAN configuration of the Layer 2 switch port connected to your management terminal from VLAN 1 to VLAN 3. As you complete the configuration, your telnet connection is suddenly disconnected. What is the most probable reason for this to occur?

- ❍ **A.** An IP access list was created in the switch.
- ❍ **B.** Someone changed the IP address in VLAN 3.
- ❍ **C.** The IP address of the switch is in the management VLAN.
- ❍ **D.** Someone changed the password on the vty lines of the switch.

49. Which of the following are valid interface connections for Serial WAN connections? (Choose 3.)

- ❍ **A.** EIA/TIA-449
- ❍ **B.** V.35
- ❍ **C.** RJ-48
- ❍ **D.** RJ-44
- ❍ **E.** X.21

50. What does the c2600 portion of the Cisco IOS filename c2600-ipbase-1.122-1.T.bin represent?

- ❍ **A.** Hardware platform
- ❍ **B.** Feature set
- ❍ **C.** Train identifier
- ❍ **D.** IOS version

51. After telnetting from RouterA into RouterB, you realize that your `debug` outputs are not showing on the terminal screen in RouterB. How can you remedy this?

- ❍ **A.** RouterA#**terminal monitor**
- ❍ **B.** RouterA(config-line)#**terminal monitor**
- ❍ **C.** RouterA#(config-line)#**terminal monitor**
- ❍ **D.** RouterB#**terminal monitor**

52. You have created an access list and applied it inbound for your router's internet connection. You would like the router to send a message out the console port whenever inbound access is denied because of this access list. What command can you add to the end of your access list statements to enable this feature?

- ❍ **A.** report
- ❍ **B.** logging
- ❍ **C.** log
- ❍ **D.** record
- ❍ **E.** match

53. Which of the following is false regarding the successor and feasible successor?

- ❍ **A.** The lowest feasible distance is the successor route.
- ❍ **B.** Both are located in the topology database.
- ❍ **C.** The feasible successor is determined if the feasible distance is less than the advertised distance of the successor route.
- ❍ **D.** The successor route is placed in the routing table.

54. _____ allows for an end device to receive power over a copper ethernet cable.

- ❍ **A.** Long Reach Ethernet
- ❍ **B.** Gigabit Ethernet
- ❍ **C.** Fast Ethernet
- ❍ **D.** Power over Ethernet

55. What command configures a default route in a Layer 2 switch?

- ❍ **A.** ip route 0.0.0.0 0.0.0.0 FastEthernet 0/0
- ❍ **B.** ip default-gateway 172.16.1.1
- ❍ **C.** ip default-network 192.168.1.0
- ❍ **D.** default-route 172.16.1.1

56. You want to ensure that the router is communicating with the switch properly by viewing the status of both Layer 1 and Layer 2, as well as by viewing the number of active calls. What command permits this?

- ❍ **A.** show isdn layers
- ❍ **B.** display isdn layers
- ❍ **C.** show isdn status
- ❍ **D.** show isdn info

57. You walked away from your terminal for five minutes to get some coffee. When you returned, you noticed that someone has made configuration changes to your router. Which three commands will diminish this from happening in the future?

- ❍ **A.** Router(config-line)#**line-timeout 1**
- ❍ **B.** Router(config-line)#**login**
- ❍ **C.** Router(config)#**password *password***
- ❍ **D.** Router(config)#**exec-timeout 1**
- ❍ **E.** Router(config-line)#**password *password***
- ❍ **F.** Router(config-line)#**exec-timeout 1**

58. Your new junior technician is confused why traffic from VLAN 1 isn't being tagged with a VLAN identifier over the 802.1q trunk port. What should you tell him the reason is?

- ❍ **A.** They are baby giant frames, so there is no room in the frame.
- ❍ **B.** They are from the native VLAN.
- ❍ **C.** VLAN 1 should not be forwarded over a trunk.
- ❍ **D.** Only one VLAN is allowed over a trunk.

59. You are configuring an office to use a Cisco router to connect to the Internet. The onsite network administrator would like to publish an internal email server, two internal web servers, and an internal FTP server to the Internet so that outside users can access them. What is necessary for this configuration?

- ❍ **A.** You will need a public Internet IP address for each internal server. These addresses can be mapped using Static NAT features.
- ❍ **B.** You will need a single public Internet IP address for this configuration and use NAT Overload to share it between all four internal servers.
- ❍ **C.** You will need a single public Internet IP address for this configuration and use Static NAT to map specific ports to all four internal servers.
- ❍ **D.** You will need two public Internet IP addresses to accommodate the internal web servers. The FTP and email server can be mapped to individual ports on either of the addresses.

60. Which of the following conditions could result in the port to transition to a disabled state? (Choose all that apply.)

- ❍ **A.** A BPDU is detected on a BPDU Guard-enabled port.
- ❍ **B.** The port is not a root or a designated port.
- ❍ **C.** The switch connected to your port has a faster way back to the root.
- ❍ **D.** Port security violation.

61. Which of the following is not true regarding a loopback interface with OSPF?

- ❍ **A.** It is a virtual interface.
- ❍ **B.** It commonly has a 255.255.255.255 netmask.
- ❍ **C.** It ensures that an interface is always active for OSPF processes.
- ❍ **D.** The higher physical interface number becomes the Router ID.

62. Which of the following topologies is shown in the figure?

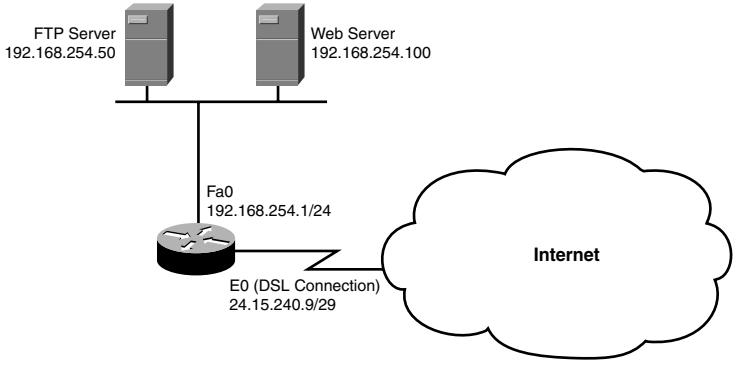


FIGURE PE.3 The loopback interface.

- ❍ **A.** Partial mesh
- ❍ **B.** Full mesh
- ❍ **C.** Ring mesh
- ❍ **D.** Hub and spoke

63. Given the following output, how can we close telnet session 2? (Choose 2.)

```
CCNA2620#show sessions
Conn    Host               Address           Idle      Conn Name
 1    131.108.100.152     131.108.100.152   0      131.108.100.152
 *2     126.102.57.63          126.102.57.63      0      126.102.57.63
```

- ❍ **A.** Press the Enter key and type **`exit`**.
- ❍ **B.** Type **`disconnect 2`**.
- ❍ **C.** Press the Enter key and type **`disconnect 2`**.
- ❍ **D.** Type **`close 2`**.

64. Which of the following is not a characteristic of link-state routing protocols?

- ❍ **A.** VLSM support
- ❍ **B.** Route summarization at any bit level
- ❍ **C.** Full routing updates at regular intervals
- ❍ **D.** Discontiguous network support

65. Which of the following is not part of the VLAN configuration process?

- ❍ **A.** Name the VLAN.
- ❍ **B.** Create the VLAN.
- ❍ **C.** Set the VTP domain to client mode.
- ❍ **D.** Assign the VLAN to a switch port.

66. Which WAN interface does not synchronize clocks for the bit stream of both the sending and receiving end of a serial link?

- ❍ **A.** BRI
- ❍ **B.** Synchronous Serial
- ❍ **C.** Asynchronous Serial
- ❍ **D.** HSSI

67. You connected your switch into a device at half-duplex. What is a possible reason for not using full-duplex?

- ❍ **A.** It is a 10Mbps port.
- ❍ **B.** You are connecting it to another switch.
- ❍ **C.** You are using a straight-through cable.
- ❍ **D.** You are connected to a hub.

68. Which of the following is not an additional feature of RIPv2 over RIPv1?

- ❍ **A.** Full update followed by hellos
- ❍ **B.** Update authentication
- ❍ **C.** Multicast updates
- ❍ **D.** Classless support

Answers to Exam Questions

1. **C**. The "invalid input detected at ^" terminal message indicates that the IOS understood the configuration command up to the caret marker. This type of message is typical when the command contains a typo. Answer A is the correction for an "Ambiguous Command" message. Answer B is the correction for an "Incomplete Command" message. Answer D is not viable because the terminal session is still connected.

2. **A**. The packet would be denied because of the implicit deny statement at the end of the access list. Answer B is incorrect because the first permit statement only matches the range of addresses from 192.168.5.16–31. Answer C is incorrect because the third permit statement only matches the range of addresses from 192.168.5.48–63. Answer D is incorrect because the last permit statement only matches the 192.168.5.0 network address.

3. **A**, **C**, and **D**. Telnet, HTTP, and FTP are all protocols supported by Layer 7, or the Application layer of the OSI model. Answer B is incorrect because JPEG is a Layer 6, or Presentation layer supported protocol.

4. **B**. You must use an extended ping in order to specify the datagram size when pinging an IP address. In order to do an extended ping in the Cisco IOS, you must be in Privileged EXEC mode, and the command is ping without specifying an IP address. Answer A is incorrect because that is a DOS command, not an IOS command. Answer C is incorrect because you do not specify the IP address after the ping keyword. Answer D is incorrect because you must be in Privileged EXEC mode.

5. **B**. The ip nat syntax can be quite cryptic because the Cisco router gives you plenty of flexibility with the form and directions of NAT translation. In this case, we are looking to create a Static NAT translation to allow TCP port 80 (HTTP) to pass through the Cisco router to the internal web server. There are two ways to accomplish this; we can create a Static NAT translation from the inside perspective or from the outside perspective. In this question, the only correct answer is the translation performed from the inside: ip nat inside source static tcp 172.16.55.10 80 interface fastEthernet 0/1 80. If we were to perform the Static NAT translation from the outside perspective, we would not be given the option to choose to translate from an interface (fastEthernet 0/1, in this case). Answers A, C, and D would result in an invalid syntax message.

6. **D**. DNS resolves hostnames into IP addresses. Answer A is incorrect because SMTP sends electronic mail across the network. Answer B is incorrect because NFS allows users with different operating systems (that is, NT and Unix workstations) to share files. Answer C is incorrect because NNTP offers access to Usenet newsgroup postings.

7. **B**. If the boot field in the configuration register is 2-F, the router or switch will load the IOS from Flash when no boot system commands are present. Answers A and C will load into ROMmon because the boot field is 0. Answer D has a 1 in the boot field, so it will load to RxBoot.

8. **B** and **C**. Cisco routers typically support DB-60, which is a 60-pin connection. Only one DB-60 interface is supported per WIC card. Because of this, Cisco developed the Smart Serial connector, which is much smaller and supports more condensed interfaces. Answer A is incorrect because EIA/TIA-449 connects to the CSU/DSU side of the connection. Answer D is incorrect because this is a LAN interface standard.

9. **C**. The Session layer of the OSI model handles dialog control among devices and determines the beginning, middle, and end of a session or conversation that occurs between applications (intermediary). The Application layer (Answer A) provides an interface between a host's communication software and any necessary external applications. The Presentation layer (Answer B) presents data to the Application layer. The Transport layer (Answer D) manages end-to-end connections and data delivery between two hosts.

10. **B** and **D**. During the learning and forwarding STP port states, the switch actively learns MAC addresses it receives on that interface. Answer A and C are incorrect because MAC addresses are not learned during the blocking and listening port states.

11. **B**. An interface ISDN switch-type setting overrides the global setting. Answer A is incorrect because you can override the global setting at the interface level. Answer C is incorrect because both settings are effective. Answer D is incorrect because this is a valid configuration.

12. **D**. SNMP uses port number 161. Answers A and B are incorrect because DHCP uses port numbers 67 and 68. Answer C is incorrect because TFTP uses port number 69.

13. **A**. When a configuration is saved, it is stored in NVRAM as the startup-config. Answer B is incorrect because the running-config is stored in RAM. Answer C is incorrect because POST, ROMmon, and RxBoot are located in ROM. Answer D is incorrect because the compressed IOS file is stored in Flash.

14. **A**, **B**, and **D**. They are all valid signaling types for Local Management Interface (LMI). Answer C is incorrect, as the ITU-T is a standards organization that actually created the Q.933a standard. Answer E is incorrect because this is the industry standard type of Frame Relay encapsulation, not an LMI signaling type.

15. **C**. Crosstalk is an electrical or magnetic field that is a result of one communications signal that can affect the signal in a nearby circuit. Answer A is incorrect because EMI is the interference caused by electromagnetic signals. Answer B is incorrect because attenuation occurs over long distances as a signal loses strength. Answer D is incorrect because bandwidth is the total amount of information that can traverse a communications medium measured in millions of bits per second.

16. **A**. OSPF ABRs do not perform automatic summarization. Route summarization entries must be manually configured with the area *area#* range *summaryaddress* command. Answers B, C, and D are all valid advantages of OSPF.

17. **F**. When applying standard access lists, it's always best to apply them closest to the destination. Because they can only permit or deny based on the source address, placing them too close to the source might allow or deny too much access. For example, if the access list were placed on the Fa0/0 port of the Homer router, Network 1 would not be able to access any resources on the network. All other answers are incorrect because they are not the closest to the Internet destination.

18. **B**. When connecting a switch to a PC, you must use a straight-through UTP cable. Answer A is incorrect because coaxial cable is typically used for cable television. Answer C is incorrect because cross-over cables are used to connect like devices such as switches to other switches or PCs to other PCs. Answer D is incorrect because thin coax (also known as thinnet) is used in older network topologies.

19. **D**. Answer D is the false answer because you must configure directly connected classful networks. Thus, 10.2.0.0 is incorrect because the classful network should be 10.0.0.0. Answer B is incorrect because, based on the output, the routing protocol configured is RIPv2 with update authentication. Answer A is incorrect because the administrative distance for RIPv2 is 120; however, the output shows the AD as 80. Answer C is incorrect because the output does show that update authentication is indeed configured.

20. **D**. Dynamic NAT allows you to configure multiple pools of IP addresses and translate between them. The router dynamically matches each IP address to one another as a request is made. Answer A is incorrect because Port Address Translation (PAT) is just another name for NAT Overload. Answer B is incorrect. Although Static NAT could perform this task, it would take quite a bit of configuration to manually map IP addresses in large pools. Answer C is incorrect because NAT Overload takes a group of IP addresses and translates them to a single (overloaded) IP address.

21. **A**, **B**, and **C**. 10BASE-2, 10BASE-5, and 10BASE-T are all 10Mbps IEEE 802.3 ethernet standards. Answer D is incorrect because Wi-Fi is a wireless technology that is defined by IEEE 802.11.

22. **C**. The summary route for 192.168.64.0 /19 summarized the networks from 192.168.64.0 /24–192.168.95.0 /24. Because five bits were stolen (25=32), 32 networks are being summarized. Answers A, B, and D are incorrect because these do not fall in the summary range.

23. **A** and **D**. HDLC and PPP are the only encapsulation types supported by Cisco on leased line connections. Answer B is incorrect because Frame Relay is an encapsulation used on a Frame Relay packet switched network. Answer C is incorrect because ISDN is a type of circuit switched technology.

24. **C** and **D**. Hubs and repeaters are hardware devices used at the Physical layer of the OSI model to extend a network. Answers A and B are incorrect because switches and bridges are hardware devices used at the Data Link layer to segment a network.

25. **B**, **C**, and **D**. Unicast, multicast, and broadcast addresses are ethernet address types used at the 802.3 MAC sublayer. Answer A is incorrect because IP addresses are logical addresses used at the Network layer of the OSI model.

26. **B**. If you add another switch to a VTP domain that is in server mode and has a higher revision number, other switches in the VTP domain will use the VLANs in the new server's database. If there are no VLANs in the database, the other switches will remove all the VLANs in their databases as well. Answer A is incorrect because a switch in client mode will not advertise its own VLANs. Answer C is incorrect because devices with a higher revision number will ignore the VTP advertisements of the new server. Answer D is probable, but Answer B is more likely than someone deleting your VLANs without you knowing.

27. **B**. The correct syntax is dialer idle-timeout <seconds>. All other commands (Answers A, C, and D) are invalid IOS syntax.

28. **B**. All multicast addresses start with 0100.5E. Answer A is incorrect because unicast addresses start with the OUI of the manufacturer NIC. Answer C is incorrect because broadcast addresses begin with FFFF.FF. Answer D is incorrect because IP addresses are not ethernet MAC sublayer addresses, and they use dotted decimal format rather than hexadecimal format.

29. **D**. Modems are typically connected to the auxiliary port and are used as a "last-resort" method of accessing the remote router. Answers B and C are incorrect: Because you no longer have IP connectivity to the router, you cannot use SSH and telnet. Answer A is incorrect because you are not able to console into the router because it is in a remote location. The only viable solution left is to call into a modem that is connected through the Auxiliary port.

30. **C**. For a low-cost connection, you could use a hub and spoke topology. With this design, you would only need a connection from the hub office to each of the spokes. Answer A is incorrect, as each router would need a separate connection for each and every other router in the topology. This would be quite expensive in a large topology. Answer B is incorrect, as you would still have more connections than a hub-and-spoke. Answer D is incorrect, as nonbroadcast multi-access (NBMA) does not affect the cost of Frame Relay.

31. **A**. Microsegmentation occurs when a switch creates a dedicated path for sending and receiving transmissions with each connected host. Answer B is incorrect because half-duplex only allows for one-way data transmissions at a time. Answer C is incorrect because full-duplex allows for two-way data transmissions. Answer D is incorrect because CSMA/CD is an algorithm used for arbitration on an ethernet network.

32. **B** and **D**. To speed up convergence for end devices such as computers, servers, and printers, you can enable PortFast, which will bypass the listening and learning port states. To secure that port from having a hub or switch connect to it and cause loops, you can enable BPDU guard, which will disable the interface if it receives a BPDU. Answers A and C will not speed up convergence for end devices.

33. **C**. Interesting traffic activates the link, causing it to connect and the traffic to be delivered. Answer A is incorrect because this is not interesting traffic as defined by DDR. Answer B is incorrect because interesting traffic should be delivered, not blocked. Answer D is incorrect because interesting traffic does not necessarily initiate at the router.

34. **C** and **D**. Switches and bridges are hardware devices used at the Data Link layer to segment a network. Answers A and B are incorrect because hubs and repeaters are hardware devices used at the Physical layer of the OSI model to extend a network.

35. **B**. Class A addresses have a first octet value of 1–126. Class B addresses have a first octet value of 128–191. Class C addresses have a first octet value of 192–223. All other answers are incorrect because they do not correctly identify this range.

36. **D**. Routing protocols will not advertise each other's networks unless redistribution has occurred. Answers A and B are incorrect. Because the routing protocols are not advertising the same network, administrative distance does not play into this. Answer C is incorrect because this reverses the networks the routing protocols are advertising.

37. **C** and **D**. The generic Static NAT syntax for TCP translations is ip nat inside source static tcp <inside_ip> <inside_port> <outside_ip/outside_interface> <outside_port>. In this case, only answers C and D match this syntax. Answers A and E flip the IP address and port numbers in the wrong location, which will produce a syntax error. Answer B uses port 20, which is used by FTP; however, only port 21 is used to initiate an FTP session. After a client initiates the incoming FTP session on port 21, the FTP server will establish an outgoing FTP data connection using port 20. Because of this, no incoming NAT translation is necessary for TCP port 20.

38. **B**. A T1 controller card can be installed in a router's T1 slot to communicate with and control the 24 DS0 channels. Answer A is incorrect because a GBIC interface module can be inserted into the Gigabit Ethernet slot to allow for different media connections to that port. Answer C is incorrect because if it is not built-in on a Cisco router via a BRI-U interface, the service provider requires separate BRI NT-1 hardware as a termination point for the communications line, which then connects to the Cisco router. Answer D is incorrect because HSSI is a high-speed interface that offers up to 52Mbps transmission rates to the WAN from a Cisco router.

39. **D**. Because the update is coming from two different sources with the same metric, RIP will load balance over both equal paths. Answers A and B are incorrect because the order the updates were received are negligible. Answer C is incorrect because the maximum hop count for RIP is 15.

40. **A**. Standard IP access-lists number from <1–99>. Answer B is incorrect because extended IP access lists number from <100–199>. Answer C is incorrect because the expanded range standard access list is <1300–1999>, and Answer D is incorrect because the expanded range extended access list is <2000–2699>.

41. **B**. The first octet is 32+16+8 = 56. The second octet is 128+32+16+2+1 = 179. The third octet is 64+16+4+2+1 = 87. The last octet is 128+64+16+8+2 = 218. So the address in dotted decimal format is 56.179.87.218. The last bit in the last octet was 0, which means that any address ending with an odd numbered octet can be eliminated. All other answers have the wrong decimal conversion.

42. **A**. EIGRP and IGRP can load balance over unequal paths by using the variance command. All other answers are unique differences between IGRP and EIGRP.

43. **A**. Cisco routers (new and old) all use a Cisco proprietary version of HDLC on their serial connections. Although there is an industry standard HDLC, very few vendors support it. Answer B is incorrect because there are no "backward compatible" WAN standards. Answers C and D are incorrect because newer Cisco routers still use the Cisco proprietary HDLC as the default encapsulation.

44. **C**. The broadcast IP of 212.84.5.66/26 is 212.84.5.127. The next network ID after 212.84.5.64 is 212.84.5.128. To determine the broadcast IP, you subtract 1 from the next network ID, which in this case is 212.84.5.127. All other answers are incorrect because they are not the broadcast IP.

45. **B**. The 10.1.100.0 is a network learned from IGRP, which is a classful network routing protocol. Despite the fact that the network is a subnetted major network in the routing table, the design is a FLSM design. Otherwise, the network would be summarized to its classful boundary. Answers A and D are incorrect. Hop count is not a factor in this exhibit because IGRP does not use hop count as its metric. Answer C is incorrect because Serial 0 has the IP address of 192.168.1.8 displayed as the connected interface entry.

46. **B**. The `show frame relay pvc` command provides you with statistics of each configured connection, as well as traffic statistics. Answer A is incorrect, as the output is not for LMI statistics. Answers C and D are incorrect, as there are no such commands.

47. **B**. The Network ID of 212.84.5.66/26 is 212.84.5.64. The CIDR notation represents subnet mask 255.255.255.192. The binary equivalent of the subnet mask host field is 11000000. The binary equivalent of 212.84.5.66 host field is 01000010. Using Boolean AND, the Network ID is 212.84.5.64. Answers A, C, and D are incorrect.

48. **C**. VLAN 1, the management VLAN, contains the IP address for the switch and CDP and VTP advertisements. If your terminal computer is not connected to the management VLAN, you will not be able to telnet to that switch. Answer A is incorrect because an IP access list cannot be configured in Layer 2 switches. Answer B is incorrect because the management VLAN is VLAN 1. Answer D will not disconnect the active telnet session.

49. **A**, **B**, and **E**. The five primary standards that are used for serial interface connections (to the CSU/DSU) are V.35, X.21, EIA/TIA-232, EIA/TIA-449, and EIA/TIA-530. Answer C and D are incorrect because RJ-48 is the standard for a T1 connection, and RJ-44 is not a defined standard at all.

50. **A**. The c2600 portion of the IOS filename represents the hardware platform. In this case, it is a Cisco 2600 series router. Answer B is incorrect because the term ipbase refers to the IP Base feature set. Answer C is incorrect because the train identifier is T for Technical. Answer D is incorrect because the IOS version is represented by 122 or version 12.2.

51. **D**. The terminal monitor command will copy and console messages to the telnet sessions of an IOS router or switch. This command is done in Privileged EXEC mode in the device you are telnetted into. All other commands (Answers A, B, and C) are incorrect because they are either on the wrong router or in the wrong mode.

52. **C**. By adding the log keyword to the end of an access list entry, the router will report any matches on that line to the console port. This logging can also be redirected to a reporting server. All other answers (A, B, D, and E) are invalid syntax.

53. **C**. The feasible successor is determined if the advertised distance of the route is less than the feasible distance of the successor route in the routing table. The feasible successor and the successor router are both maintained in the topology table. All other answers (A, B, and D) are true regarding the successor and feasible successor.

54. **D**. Power over Ethernet is a technology that allows for an end device to receive power over a copper ethernet cable. Answer A is incorrect because Long Reach Ethernet (LRE) is an ethernet specification developed by Cisco to provide broadband service over existing telephone-grade or Category 1, 2, or 3 wiring. Answers B and C are incorrect because Gigabit Ethernet and Fast Ethernet standards do not include the ability to supply power to an end device.

55. **B**. Because this is a Layer 2 switch, the gateway of last resort is configured by setting the default gateway. Answers A and C are incorrect because you cannot configure a default route or a default network in a Layer 2 switch. Answer D is not a valid command.

56. **C**. The show isdn status command displays Layer 1 status and Layer 2 status information. Answers A, B, and D are all invalid IOS commands.

57. **B** and **F**. To secure your console connection when you walk away from the IOS terminal, you need to decrease the exec-timeout and set the login and password. These configurations must be performed in the line configuration mode. All other answers are incorrect because they are performed in the wrong configuration mode.

58. **B**. With 802.1q trunks, traffic originating from the native VLAN is not tagged with a VLAN identifier. Answer A is incorrect because information can always be added to a frame, even if it is a baby giant. Answer C is incorrect because VLAN 1 is always forwarded over a trunk by default. Answer D is incorrect because many VLANs can be sent over a trunk.

59. **D**. NAT can accomplish some pretty amazing feats; however, sharing an IP address for two servers that use the same port number is not one of them. In this case, you will need two public Internet addresses to allow both internal web servers to be accessed on TCP port 80. The other servers can use port 21 (FTP) and port 25 (SMTP) on either of the public Internet IP addresses. Answer A could be used to solve this problem, but is not the best solution because it will be more costly to deploy than Answer D. Answer B is incorrect because NAT Overload will only enable the servers to share a single IP address when accessing the Internet, not when the requests originate from the Internet. Answer C is incorrect because you could only map TCP port 80 on the single IP address to one of the internal web servers. The other could not be accessed from the Internet.

60. **A** and **D**. The port will become disabled if a BPDU is detected on a BPDU Guard-enabled port, as well as if there is a port security violation. Answers B and C are incorrect because that would cause the port to be in a blocking state.

61. **D**. When using loopback interfaces with OSPF, the physical interfaces are no longer used to determine the Router ID. All other answers are true and play a significant role in the OSPF Router ID.

62. **A**. There are redundant links between the routers—however, there are not redundant links between all of the routers. Answer B is incorrect, as there are not redundant links between all of the routers. Answer C is incorrect, as even though the connections form a ring as shown here; if it were in the cloud, it would not look like this. Answer D is incorrect, as it is not a star or hub-and-spoke topology—there is no central point.

63. **A** and **B**. To disconnect the telnet session, you can type **`disconnect`** followed by the session number in the originating router or you can press the Enter key to resume the telnet session and type **`exit`** in the device you are telnetted in to close the telnet session. Answer C is incorrect because pressing Enter first will resume your session with the remote router and cause the disconnect command to fail. Answer D is incorrect because this is invalid syntax.

64. **C**. Link-state routing protocols (OSPF and IS-IS) do not send full routing updates at regular intervals. Answers A, B, and D are characteristic of link-state routing protocols; however, this question is looking for the false answer.

65. **C**. Setting the VTP domain to client mode will not allow you to configure any VLANs on the switch. All other answers (A, B, and D) are typically performed during a VLAN configuration process.

66. **C**. Asynchronous Serial does not synchronize the clocks for the bit stream of the sending and receiving end of a serial link. Answer B is incorrect because Synchronous Serial synchronizes clocks for the bit stream of both the sending and receiving ends of a serial link. Answer A is incorrect because Basic Rate Interface (BRI) consists of two 64Kbps B channels and one 16Kbps D channel. Answer D is incorrect because HSSI offers up to 52Mbps transmission rates to the WAN from a Cisco router.

67. **D**. When connecting to a hub, you must have the port running in half-duplex because CSMA/CD must be enabled. Answer A is incorrect because the speed is irrelevant. Answer B is incorrect because you can run full-duplex when connecting to switches. Answer C is incorrect because it does not matter what cable is used.

68. **A**. RIPv2 has update authentication, multicasts updates to 224.0.0.9, and can support classless routing. Answer A is not a feature because it is still a distance vector routing protocol that sends continuous updates every 30 seconds instead of Hello messages, such as RIPv1.

PART III

Appendixes

Appendix A Future Exam Topics

Appendix B CD Contents and Instalation Instructions

Appendix C Glossary

APPENDIX A

Future Exam Topics

Introduction

It is inevitable that technology will constantly change and evolve. With that being said, the Cisco CCNA exam too must evolve in line with current networking practices as it has done since its introduction in 1998. As we have witnessed over these years, the CCNA has shed outdated topics such as AppleTalk and IPX routed protocols. At the same time, it embraced several new concepts including several advanced topics that were once only studied in the CCNP program. In fact, if you were to tell CCNA candidates a few years ago that the CCNA exam contained EIGRP and OSPF, they would accuse you of taking the wrong exam.

The concepts in this book's chapters were written in accordance with the most current exam topics. This appendix contains a list of additional topics that incorporate current models and technologies that are likely to appear in future revisions of the CCNA exam. Because the concepts discussed in these topics are relevant to modern-day subjects, they might also prove useful to your current day-to-day professional responsibilities.

Cisco Enterprise Composite Network Model

In Chapter 1, "Standard Internetworking Models," we discussed three different layered models that were created to help with network design and implementation. The Enterprise Composite Network model was developed by Cisco to provide a guide for network designers to plan larger-scale networks. Distinct components rather than layers make up the structure of this network model. The three functional components are divided into smaller areas that are referred to as network modules, as represented in Figure A.1.

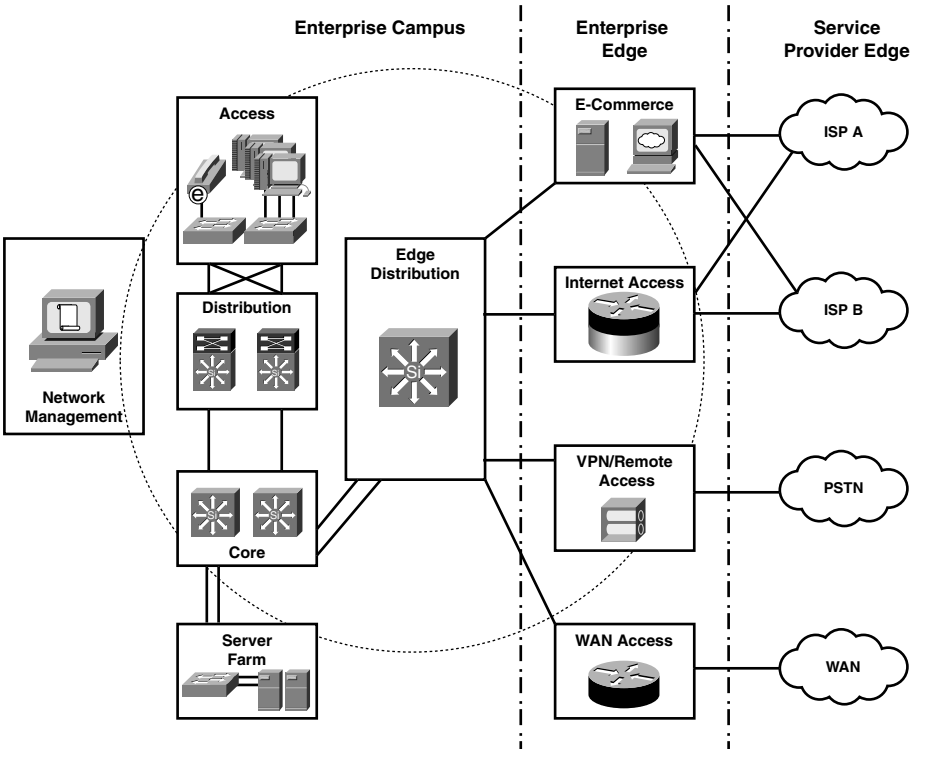


FIGURE A.1
Enterprise composite model.

The three functional components are

- Enterprise Campus
- Enterprise Edge
- Service Provider (SP) Edge

Enterprise Campus

The Enterprise Campus consists of the following four modules:

- Campus Infrastructure
- Edge Distribution
- Server Farm
- Network Management

The **Campus Infrastructure** module includes its own core, distribution, and access layers, which correlate to the Cisco 3-Layer Hierarchical model. These layers exist within a single building on the campus. Given a large location, a three-layer approach to the design will most likely be used with a building access layer (wiring closet), building distribution layer, and campus core layer. However, if there is a small location, a two-layer approach can be used. The two-layer approach combines the distribution layer with the backbone to form a backbone core. That core then works with the access layer. A moderately sized network can use either a two- or three-layer approach, whichever is more appropriate to their needs.

NOTE

You might also hear the terms campus backbone, building access layers, or building distribution used instead of campus infrastructure.

The **Edge Distribution** module provides an access point between the Enterprise Campus functional component and the Enterprise Edge component.

The **Server Farm** module consists of a group of servers found in a single location (such as a data center). These servers work together to increase capacity and processing speeds. Load balancing software along with hardware clustering provides redundancy, which is also critical to the efficiency of the network.

The **Network Management** module provides…you guessed it…management capabilities for the entire network. This includes network monitoring and intrusion detection.

Enterprise Edge

The Enterprise Edge consists of the following four modules:

- E-Commerce
- Internet Access
- VPN/Remote Access
- WAN Access

The **E-Commerce** module is used for business-related services. Here you might find a database server and firewall. Devices within this module are used in conjunction with the servers found within the Enterprise Campus component and the Internet Connectivity Module.

Example: An effective E-Commerce module would allow Internet shoppers to complete a secure online transaction by passing data from front-end web servers to back-end servers protected by the firewall.

The **Internet Access** module provides the Enterprise network access to the Internet. This can be achieved via a single or multi-homed link to the SP Edge. Although a single link will work, it also lacks redundancy.

The **VPN/Remote Access** module provides remote access services to the network. Remote access can be achieved via either a remote access terminal server or a VPN server.

The **WAN Access** module might also be called the Classic WAN module. Routers or Layer 3 switches would be appropriate hardware for WAN connectivity.

Chapter 15, "Wide Area Networks," covers the following WAN connection types that can be found at the WAN module of the Enterprise Edge:

- Leased Lines
- Circuit Switched
- Packet Switched
- Broadband
- VPNs
- Metro Ethernet (that is, the LAN WAN)

Chapter 15 also covers the following WAN Data Link Encapsulations:

- Serial Line Internet Protocol (SLIP)
- Point-to-Point Protocol (PPP)
- Cisco High Level Data Link Control (HDLC)
- X.25/Link Access Protocol, Balanced (LAPB)
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA)

Service Provider Edge

The Service Provider (SP) Edge consists of the following three modules:

- Internet Service Provider
- Public Switched Telephone Network (PSTN) Service Provider
- WAN Service Provider

The **Internet Service Provider** module refers to the connection between the Enterprise network and an Internet provider. There can be more than one ISP at the SP Edge, so each ISP would be considered a separate module.

The **PSTN Service Provider** module provides voice services to the network via dial-up technologies.

NOTE

Chapter 16, "ISDN," discusses a more specific dial-up technology called Integrated Services Digital Network (ISDN). ISDN has been a persistent topic on the CCNA exam.

The **WAN Service Provider** module allows for access between more than one site through WAN technologies such as ATM and Frame Relay.

All three SPs listed in the SP Edge component charge access fees for network connectivity.

IPv6

IPv6 is a workable IP version that was created in the event that the IP space from IPv4 is exhausted. Cisco routers are capable of routing IPv4 and IPv6 traffic in the event that networks start to use IPv6 addressing on a regular basis. At this point, organizations are primarily requesting small IPv6 networks from IANA for testing purposes to make sure that they are prepared for the day when IPv4 addresses are no longer available. IPv6 provides the same functionality as IPv4. Like IPv4, IPv6 also manages Network layer packet addressing and routing. The sheer size of assignable IPv6 addresses is astounding. The format of this version offers trillions of available IP addresses. For this reason, IPv6 should never experience a shortage of address space.

IPv6 Addressing

IPv6 is defined by RFC 2373 and 2374. IPv6 addresses are much longer than their 32-bit IPv4 address counterpart. Each address is 128-bits long and represented by 32 hexadecimal digits. As you will recall, IPv4 is represented by dotted decimal notation.

IPv6 addresses consist of two parts:

- A 64-bit network prefix
- 64-bit local identifier

Example IPv6 address: 2001:0BD2:12C3:08F1:000C:32**FF:FE**D2:16AB

As you can see by the example, each address is broken down into eight smaller groups of four hexadecimal digits. The last 64-bit section of an IPv6 address is used as a local identifier. This is typically generated using the MAC address of an interface. Remember, though, that MAC addresses consist of 48-bits, so there is a discrepancy of 16-bits. The solution to this issue is to add 0xFFFE into the 24th bit of the MAC address. I bolded the portion of the address that is inserted to add 16-bits in the previous example.

IPv6 address format summary:

- Defined by RFC 2373 and RFC 2374
- Consists of 128-bits with a 64-bit network prefix and a 64-bit local identifier
- Represented by 32 hexadecimal digits broken down into 8 smaller groups of 4
- Uses CIDR notations (slash notations) to discern a subnet range

As you can see, Ipv6 addresses are quite long and complex looking. If there is a 4-digit group of all 0s, that group can be removed from the address and it would look as follows:

Before the omission = 2001:0BD2:**0000**:08F1:000C:32FF:FED2:16AB/26

After the omission = 2001:0BD2::08F1:000C:32FF:FED2:16AB/26

Autoconfiguration

Remember how IPv4 uses Dynamic Host Control Protocol (DHCP)? DHCP enables a device to dynamically obtain the IPv4 address, default router, and DNS server if available. Well, DHCPv6 was created to work with IPv6 addressing. DHCP and DHCPv6 are both considered stateful protocols. With a stateful protocol, a dedicated server maintains a table of the information that was gathered. Unlike IPv4, IPv6 also supports a stateless protocol for autoconfiguration. This means that a dedicated server is no longer required.

With the exception of routers, IPv6 creates a unicast global address for each device. It also enables every NIC to have multiple IPv6 addresses. These address types include link-local, site-local, and global. At a minimum, each NIC will have a link-local address, but it is more likely that it will have a link-local and global address.

Example of a global address:

2001:0BD2:12C3:08F1:000C:32FF:FED2:16AB/64 scope global

Example of a link-local address:

FE80:0BD2:12C3:08F1:000C:32FF:FED2:16AB/10 scope link.

Integrating IPv4 and IPv6

How can we get IPv4 and IPv6 to interact?

Well, there are several ways to integrate the two versions. You can implement one of the following methods:

- Translation—Translates between the two IP versions.
- IPv6 over IPv4 Tunneling—Encapsulates IPv6 packets into IPv4 packets.
- Dual-Stack IP layer solution—Every node has an IPv4 and an IPv6 address.
- Gateway—A gateway mechanism allows access to IPv4 from IPv6 and vice versa.

Rapid Spanning Tree Protocol

One of the greatest drawbacks about PortFast, UplinkFast, and BackboneFast is that they require an all-Cisco network because these are Cisco proprietary functions. Luckily, the IEEE made its own revised version of Spanning Tree Protocol to incorporate these functions, use an updated algorithm for faster topology transitions, and be completely backward compatible with the original 802.1d STP. Enter Rapid Spanning Tree Protocol (RSTP), IEEE specification 802.1w.

RSTP Port States and Roles

RSTP adopted the 802.1d port states with a slight difference. Because the blocking and listening states were essentially non-operational in terms of actively discovering the topology of the network, RSTP has redefined these to be a discarding state. Learning and forwarding states, however, are still active spanning tree transition states in RSTP-enabled LANs.

In addition, RSTP still uses the concepts of a root port and designated ports. To incorporate additional functionality, RSTP created two more port roles specifically for designs in which you have two parallel links to a switch, as demonstrated in Figure A.2. Based on the principle of UplinkFast, the following two new port roles were created:

- *Alternate port*—A blocking (or I should say *discarding*) port that becomes the root port if the active root port fails.
- *Backup port*—A discarding port that becomes the designated port if the active designated port fails.

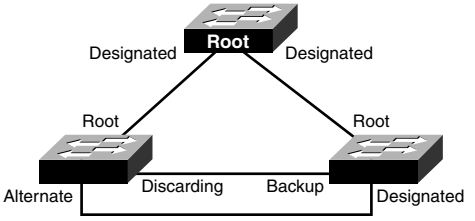


FIGURE A.2
Alternate and backup port switching design scenario.

Both of these new roles are still discarding frames; however, when the root or the designated port fails, they rapidly transition to a forwarding state.

Rapid Transition

One of the most unique functions of RSTP is its capability to converge in an expedient manner. The basis behind this feature is that it no longer relies on timers to transition to its port role. Instead, the two switches use a revised BPDU to negotiate the port roles that they should fulfill.

For instance, given the scenario shown in Figure A.3, imagine that you just connected the uplink from Switch A to the root bridge. Instead of idly transitioning to a forward state with timers, the switches negotiate their port roles. Namely, a switch sends a proposal to transition to a forwarding state to the other switch. Before agreeing to the proposal, the switches put all other ports connected to other switches (not end devices) in a discarding state to ensure that a loop does not occur. After this occurs, the switch can agree to the proposal and they can immediately start forwarding on that segment. If the port should not transition to a forwarding state (that is, should be discarding to avoid loops), no agreement is sent back. At that point, the switches send proposals out their newly discarded ports and the process occurs again, creating a wave of switches synchronizing to the change. Although this sounds as if there are many steps, the time to converge in a large network can range from several minutes (because each switch would take 30–50 seconds to forward) with 802.1d STP to a matter of seconds with RSTP.

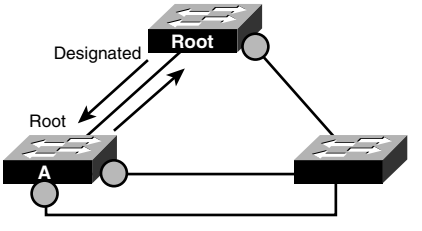


FIGURE A.3
RSTP synchronization convergence scenario.

EtherChannel

Although not an actual enhancement to Spanning Tree Protocol, EtherChannel proves to be a useful feature in Cisco switches to help overcome wasted bandwidth that might result from STP. For instance, consider the two switches illustrated in Figure A.4. Because these switches have multiple redundant links between the switches, Spanning Tree Protocol ultimately blocks three of the links to avoid a loop. If these were Gigabit Ethernet interfaces, three gigabits of throughput would be gone to waste.

FIGURE A.4
EtherChannel implementation.

EtherChannel solves this dilemma by bundling the individual links into a single virtual interface. In this manner, the switch does not block the other ports and distributes data across the individual links. If one of the individual links happens to fail, EtherChannel detects the failure and redistributes the load over the remaining links in a matter of milliseconds.

EtherChannel is a hardware feature present on most Cisco Catalyst switches today. Before configuring EtherChannel, you must connect all the interfaces (up to eight), and they must be configured identically (that is, speed, duplex, and so on). To assign them to an EtherChannel bundle, you have to navigate into each interface or use the `interface range` command and assign them to the same group number with the `channel-group` command, as follows:

```
Switch(config)#interface range FastEthernet0/1-8
Switch(config-if-range)#channel-group 3 mode on
```

This configuration places the first eight Fast Ethernet interfaces in the logical EtherChannel bundle number 3.

Switched Virtual Interfaces

An alternative to trunking to an external router is to use a Layer 3 switch to route in between the VLANs. Layer 3 switches combine the logical routing functionality of a router with the hardware speed of a switch because it uses ASICs to do some of the routing operations. So if the Layer 3 switch is faster than a router, why use routers? The answer is that Layer 3 switches do not have all the routing functionality that a router has. Specifically, you cannot purchase the Layer 3 switches with serial interfaces that can connect to a WAN. The Layer 3 switches are designed more to have routing functionality between VLANs in an ethernet LAN.

If you have a Layer 3 switch in your enterprise (certain models of the Catalyst 3550, 4000, and 6000 series of switches), you need to trunk to that switch and configure a different set of virtual interfaces to allow interVLAN routing. The result is called *switched virtual interfaces (SVI)*. The interfaces that you configure in the Layer 3 switches are, conveniently enough, VLAN interfaces.

To configure the switched virtual interfaces, you simply navigate to the VLAN interface number that matches your VLAN and assign it an IP address. For example, given the similar interVLAN scenario in Figure A.5, you are using the Layer 3 switch to route in between the two VLANs. You just need to create the VLAN interfaces and assign the IP addresses, as demonstrated in the following configuration:

```
Router(config)#interface Vlan 1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config)#interface Vlan 3
Router(config-if)#ip address 192.168.3.1 255.255.255.0
```

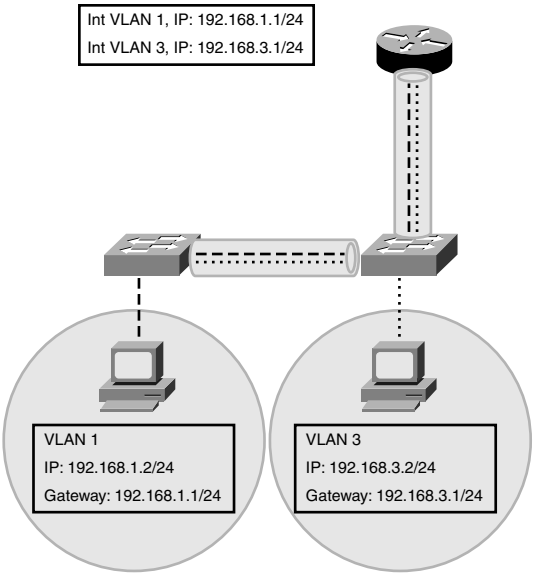


FIGURE A.5
SVI interVLAN scenario.

Quality of Service

A common theme among most networking devices today is the capability to provide some type of quality of service, or QoS, to the network traffic. As the name states, quality of service is the capability to give certain traffic priority over other traffic in a network. This functionality is critical with certain applications that require minimum delay or minimum packet loss, such as Voice over IP or video.

QoS is achieved by tagging priority traffic so that the routers and switches, in their internal processing, know to forward that traffic first if there is contention for traffic on a link. This tagging can actually span multiple devices to ensure that those devices configured with QoS give it priority as it spans our network.

At Layer 2, QoS is achieved through the use of some unused fields in the VLAN tags created by ISL or 802.1q trunks. By using bits in the VLAN tags, Layer 2 devices recognize that this traffic should be processed and forwarded over all others. When you tag this traffic at Layer 2, it is commonly referred to as Class of Service (CoS).

On-Demand Routing

The engineers at Cisco broke the routing protocol mold when they created the concept of On-Demand Routing (ODR). Specifically, they decided to produce a protocol that is exchanged between routers to advertise their networks without creating a routing protocol. The key element in this routing equation involves using CDP advertisements from stub routers, which can advertise their network information to the central router in a hub and spoke/star topology. The beauty of this concept is that by using CDP, it practically removes any routing configuration, as well as eliminates a need for additional routing protocol overhead. What's more, starting with version 12.1, ODR automatically creates a default route entry automatically in the routing table of the spoke routers toward the hub. The only downfalls to ODR are that its reliance on CDP means that it must be an all-Cisco network and it will not function if routing protocols are running in the network.

Configuring ODR is considerably easier than configuring any static route or routing protocol. You only have to configure the hub router with the following command in global configuration:

```
Router(config)#router odr
```

IS-IS Routing Protocol

The International Organization for Standardization (ISO) that gave us the OSI model also standardized its own protocol called Connectionless Network Protocol (CLNP). The IS-IS routing protocol was created to pass CLNP traffic between Intermediate Systems (routers to you and me); thus, IS-IS is a protocol for router-to-router communications.

So why are we discussing this routing protocol since our world seems to revolve around IP? In the early 1990s, many ISPs decided to use IS-IS in their internal networks over OSPF because IS-IS has low update overhead and can scale easily to impressively large networks. In addition, some government agencies started implementing IS-IS because they feared we would run out of public IPv4 addresses. Still not sure why we are discussing IS-IS? The reason is that IS-IS is being dusted off the shelves and implemented in large networks because IS-IS was improved to route IP networks as well, known as Integrated IS-IS.

Integrated IS-IS Characteristics

Integrated IS-IS is a classless link-state routing protocol with an administrative distance of 115. The fact that it is classless also means that IS-IS supports VLSM, manual route summarization, and discontiguous networks. IS-IS also maintains a routing table, a neighbor table, and a topology table just like OSPF.

In fact, IS-IS is similar to OSPF in several ways. Both routing protocols discover neighbors and form adjacencies with hellos, as well as use the concept of areas to break up their autonomous system (known as a domain for IS-IS). In addition, both use cost as their metric in determining the best route and run the SPF algorithm to determine the best path to an individual network. When a topology change occurs, routers running IS-IS will flood those updates to all their neighbors similar to OSPF.

IS-IS is also a hierarchical routing protocol in that certain IS-IS routers have special functions over others. The three possible level of IS-IS hierarchical routers are the following:

- Level 1 IS—L1 routers are responsible for routing traffic inside an area and only form adjacencies with other L1 routers.
- Level 2 IS—L2 routers are responsible for passing traffic in between areas to form an inter-area backbone and only form adjacencies with other L2 routers.
- Level 1/Level 2 IS—Similar to an ABR router, L1/L2 routers forms L1 adjacencies with other L1 routers and L2 backbone adjacencies to other L2 routers.

When L1 ISs need to send traffic from one area to another, they send traffic to their nearest L1/L2 IS in their area. This router will perform Level 2 (inter-area) routing to another L2 or L1/L2 IS in another area. The L1/L2 IS in the destination area will send the traffic to the appropriate L1 IS and to the destination network.

IS-IS also has a similar concept as OSPF's designated router to reduce routing update traffic in broadcast topologies. In fact, staying true to its nomenclature, the DR in IS-IS is called a designated IS, or DIS.

IS-IS differs from OSPF, however, in its idea of the backbone. IS-IS does not use a specific area for the backbone area. The backbone for IS-IS is actually composed of multiple Level 2 ISs interconnected to each other. This makes it much easier to expand the backbone because the routers do not need to concern themselves with connecting back to Area 0 as with OSPF. With IS-IS, you only need to add another L2 IS to extend the backbone.

Recall that Integrated IS-IS was an enhancement to IS-IS. Because this routing protocol was not originally created to route IP, it still uses CLNP as a transport for the routing updates. With that being said, Integrated IS-IS does not have a concept of a Router ID. Instead, IS-IS

uses NSAP addresses to identify the router's area and system ID. For example, the NSAP address 49.0012.00ca.0F13.4932.00 is broken down into the following components:

- 49—AFI (Authority and Format Identifier). 39=Data County Code, 47=international code designator, 49=private.
- 0012—Area identifier. Each router is in its own area unlike ABRs who have interfaces in two separate areas.
- 00ca.0F13.4932—Unique system identifier. Can use a MAC address, IP address, or even Frame Relay DLCIs to identify the device in the IS-IS domain.
- 00—Selector byte. Always set to 00 for routing devices.

Integrated IS-IS Configuration

Integrated IS-IS is extremely simple to configure. You merely have to start the IS-IS routing process using the router `isis` command. Once in the routing process, you assign the NSAP to the router with the network keyword as shown here:

```
(config)# router isis
(config-router)#network 49.0012.00ca.0F13.4932
```

The preceding configuration will enable CLNP routing between devices; however, to enable IP routing with Integrated ISIS as well, you need to type the following command on each interface you want to run Integrated IS-IS:

```
(config-if)#ip router isis
```

BGP

Border Gateway Protocol (BGP) is an exterior gateway protocol that routes in between autonomous systems. In fact, BGP is the routing protocol used in the Internet because the Internet is actually a bunch of internetworked autonomous systems. Each autonomous system is identified with a unique AS number. These AS numbers are different from the ones used in IGRP and EIGRP because they are uniquely assigned by the IANA (who manages the public IP address space and port assignments).

BGP can actually be considered two different types of routing protocols. When BGP is used to route between autonomous systems, the protocol is referred to as External BGP (EBGP). If BGP exchanges routes within an AS, the protocol is referred to as Interior BGP (IBGP). Oddly enough, because of BGP's loop free decision making methodology, external updates from eBGP neighbors have a lower administrative distance (thus trusted) than networks learned from iBGP neighbors.

BGP maintains a routing table separate from the IP routing table. The routes in this BGP table are initially exchanged with neighbors followed by frequent hellos similar to OSPF and EIGRP. To determine the best route to a destination, BGP does not use traditional metrics. In fact, BGP scrutinizes several properties of each route known as path attributes. Because these attributes can be configured and handled differently in each autonomous system depending on the routing policy, BGP is typically referred to as a policy-based routing protocol.

BGP Configuration

Entire books are dedicated to the many aspects and configurations that can occur with BGP. In the following example, we are going show you the fundamental configuration involved with BGP and how to define iBGP and eBGP neighbors to exchange updates with:

```
(config)# router bgp 65501
(config-router)#neighbor 10.1.1.1 remote-as 65501
(config-router)#neighbor 10.1.2.5 remote-as 65535
(config-router)#network 172.16.0.0
```

The configuration begins with starting the BGP routing process for AS 65501. As mentioned, this AS number is actually registered with IANA and cannot be arbitrarily chosen as we did with IGRP and EIGRP.

NOTE

Autonomous System numbers between 64512 and 65535 are deemed Private ASes by the IANA.

BGP does not use any automatic neighbor discovery messages like OSPF and EIGRP. Instead, you must manually define your neighbors and the autonomous systems they belong to. In the first neighbor statement, we are specifying the router with 10.1.1.1 as our iBGP neighbor since the AS number is the same as the one we configured in our routing process. The next statement is an eBGP connection since 10.1.2.5's AS is different from ours. Finally, the network statement is the network that we are advertising to our iBGP and eBGP neighbors. This network must be in our IP routing table in order for BGP to advertise it.

WAN Bandwidth Management Techniques

Recently, networking has entered into a new generation of delay and bandwidth-sensitive applications. We've become accustomed to our standard Web surfing, FTP, and online gaming-style applications. These applications have no true "requirements" when it comes to bandwidth or delay (despite what the online gamers might say). If there's more bandwidth

available and less delay, your web page or file transfer will occur faster. If there's less bandwidth or more delay, the web page or file transfer will happen slower. This primarily affects the user's convenience.

This is not to say that there have never been mission critical applications available. Mainframe traffic and Citrix applications have always been very delay-sensitive and have been given priority on the network. However, the tools available to assign priority to network traffic were rudimentary. Simply assigning priority to a certain application could mean network devastation. That application could take away all available bandwidth from all other applications, causing a symptom known as "network starvation." Unfortunately, back in this time, no mechanism existed to keep this from occurring. You could either give an application priority and hope that it did not eat your network alive, or you could treat all applications the same and hope that your mission critical applications would survive.

Today, the methods available to manage WAN bandwidth are much more customizable. These methods were developed in response to a great need as Voice and Video over IP began to demonstrate a viable business solution. The point of this reference is not to talk about the new, high-demand technologies (such as Voice and Video over IP), but rather, to discuss the QoS methods to manage this traffic. This will not, nor is intended to be, a complete discussion of all the QoS mechanisms available to you. It is meant to give you a high-level overview of the most effective QoS mechanisms since these are the most likely topics to pop up on the CCNA exam.

Queuing Options

Queuing falls under the QoS Congestion Management group of tools. These tools are useful when an interface on your router (or switch) runs out of bandwidth. By default, the router goes into a First-in First-out method of queuing for most interfaces. This means that the first packet that made it to the router has the most chance of making it out while the last packet has the least chance. Although this may seem like the most fair way of handling traffic congestion, it is not the most effective. What if the first packet to make it into the router is someone using Kazaa to download some "trial software"? And what if the last packet is a mission-critical database application? Instead of just accepting this default, Cisco has given us many queuing tools that can dictate how the traffic is handled in these cases. We'll discuss three of the most modern and popular methods here.

Weighted Fair Queuing

When I said that we'd discuss the most modern methods, that applies to every method except this one. Weighted Fair Queuing (WFQ) is one of the oldest queuing methods available. The concept behind it is simple: Low bandwidth senders get more priority than high bandwidth senders. Think of it this way: Imagine that you're sitting in a meeting and two people are talking on and on about a bunch of nonsense. Then, the "quiet guy" in the corner of the room

stands up and says, "I have something to say." What typically happens? Everyone stops talking and looks at the quiet guy because they're especially interested to hear what the "non-talker" has to say. In the same sense, your router is listening for the "quiet guys" of the network. The applications that are sending very little traffic gain priority over the high talkers of the network.

WFQ is turned on for all low-speed interfaces, by default. Cisco defines a low-speed interface as one that is 2.048Mbps or less. This is the speed of an E1 line (the European equivalent of the T1 line). Because it does use some memory and processor resources, Cisco recommends that you do not enable WFQ for any interface that is greater than this bandwidth amount. To turn on WFQ, simply go under the interface configuration mode and type the command **`fair-queue`**. Likewise, if you would like to disable WFQ, type the no **`fair-queue`** command.

Class-Based Weighted Fair Queuing

This is where we get into the fairly new queuing methods that have been released. Truth be told, WFQ usually means death to your critical high-bandwidth applications, such as Voice and Video over IP. Class-based WFQ (CBWFQ) gives you more control with the bandwidth you have available. Rather than just allowing the operating system to assign bandwidth to the low-demand applications, you get to pick certain applications to get specific amounts of bandwidth. For example, you could say that HTTP traffic gets 300Kbps of guaranteed bandwidth, whereas FTP gets 100Kbps. The rest of the traffic would then share whatever bandwidth was left over using the old WFQ mechanism. That's why this is called CBWFQ: You define classes of traffic that are guaranteed certain amounts of bandwidth. The rest of the traffic is lumped into one queue (or "treatment type") of WFQ.

Now the configuration gets a little more complex. When setting up CBWFQ, you will be using a fairly new mechanism that Cisco has created called the Modular QoS CLI (MQC). This mechanism defines three major steps:

1. Create class maps that define the types of traffic you would like to match.
2. Create policy maps that define what you want to *do* to the traffic you matched.
3. Apply the policy to an interface using the `service-policy` command.

I know that these steps might sound a little obscure right now, but as you see a few examples, they will start making a lot more sense. Rather than spend too much time in the concepts, I'll show you how this works as we configure it. We'll start off on a router named CBWFQ and define our class maps:

```
CBWFQ#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CBWFQ(config)#class-map ?
  WORD       class-map name
  match-all  Logical-AND all matching statements under this classmap
  match-any  Logical-OR all matching statements under this classmap
```

```
CBWFQ(config)#class-map match-all ?
  WORD  class-map name

CBWFQ(config)#class-map match-all MATCH_HTTP
```

In this first code snippet, we've gone into global configuration mode and used the class-map command to dictate the traffic that we'd like to match. As you can see, the first argument we can choose between is match-all or match-any. That's because each class map that we create can match many things. For example, I could create a class map that looks like this (this is a plain-English example rather than true syntax):

Class-map Jeremy's_Class

1. match HTTP
2. match source IP 10.1.1.1
3. match destination IP 5.1.1.1

This one class contains three match statements. If I created this class map with the match-all keyword, all three of these criteria must be met in order for the router to log a true match (and perform whatever tasks the policy-map tells it to do, but that's the next step). In this case, the source IP address 10.1.1.1 must be trying to access the destination IP address 5.1.1.1 using the HTTP protocol. That's why the match-all statement is seen as a logical-AND operation. We must match HTTP and 10.1.1.1 and 5.1.1.1. At that point, *all* of the criteria are matched, thus the match-all keyword.

The match-any keyword is useful if you'd like to match any of the statements under the class-map. In the previous example, if the protocol used was HTTP, a match statement would be logged. This is regardless of whether the source IP was 10.1.1.1 or the destination IP was 5.1.1.1. If the source IP address was 10.1.1.1, a match would be logged regardless of other criteria. It is like saying, "match HTTP, or match source IP 10.1.1.1, or match destination IP 5.1.1.1."

After we choose our match-any or match-all (I chose match-all), we just choose a logical name for our class-map. In this case, I used MATCH_HTTP. Note that this name is just logical: It has nothing to do with the function of the class-map. Now, let's keep going in the configuration:

```
CBWFQ(config)#class-map match-all MATCH_HTTP
CBWFQ(config-cmap)#?
QoS class-map configuration commands:
  description  Class-Map description
  exit         Exit from QoS class-map configuration mode
  match        classification criteria
  no           Negate or set default values of a command
  rename       Rename this class-map
```

```
CBWFQ(config-cmap)#match ?
  access-group         Access group
  any                  Any packets
  class-map            Class map
  cos                  IEEE 802.1Q/ISL class of service/user priority values
  destination-address  Destination address
  discard-class        Discard behavior identifier
  dscp                 Match DSCP in IP(v4) and IPv6 packets
  fr-de                Match on Frame-relay DE bit
  fr-dlci              Match on fr-dlci
  input-interface      Select an input interface to match
  ip                   IP specific values
  mpls                 Multi Protocol Label Switching specific values
  not                  Negate this match result
  packet               Layer 3 Packet length
  precedence           Match Precedence in IP(v4) and IPv6 packets
  protocol             Protocol
  qos-group            Qos-group
  source-address       Source address
```

Wow! That context-sensitive help is quite extensive. At first, class-map seems quite tame. From the CBWFQ(config-cmap)# configuration mode, we just have some basic commands, match being the most interesting. Once we type in **`match ?`**, we see just how many options we could use to define our match criteria. This is where I need to draw the line between the CCNA and CCVP certifications. In this book, I'd just like to address the access-group and protocol commands from the list.

If the command access-group sounds familiar, it's because you have successfully absorbed something from earlier in the book when we talked about access lists. Remember, you can create access lists all day, but they are useless until you apply them. That was the job of the access-group command. (It was actually ip access-group.) We would type that command under an interface followed by an access-list number and an in or out direction, and traffic filtering would begin. In this case, we're not applying an access list to perform traffic filtering; we're applying it to match traffic for QoS. You can use access lists to match just about any type of traffic, just like you can when you're using them for security on an interface. But Cisco decided to create an even easier way for many of the common protocols. That mechanism is called Network Based Application Recognition (NBAR).

NBAR is one of the "silent giant" features that has recently been introduced into the Cisco IOS. This utility allows you to match protocols based on their application layer data. Instead of just looking at port numbers, the Cisco IOS can look into the packet and recognize the application itself. For example, many technically savvy end users have found that you can access FTP servers on ports other than 21 just by adding a :<port number> to the end of an ftp request. For example, I could open Internet Explorer and type `ftp://BadFTPSite.com:8000` to access the BadFTPSite.com server using port 8000. As long as the BadFTPSite server is configured to

respond on port 8000, the FTP access goes through, even though the administrator might restrict FTP access. If you are using NBAR to match your traffic, it can recognize FTP regardless of the port number it is using. This requires a slight trade-off, however. Because NBAR looks into the packet to find the application layer data (known as a deep packet inspection), it will cost more processor and memory resources than an access list.

The configuration of NBAR is a piece of cake. I'll pick up our configuration example where I left it:

```
CBWFQ(config-cmap)#match ?
  access-group         Access group
  any                  Any packets
  class-map            Class map
  cos                  IEEE 802.1Q/ISL class of service/user priority values
  destination-address  Destination address
  discard-class        Discard behavior identifier
  dscp                 Match DSCP in IP(v4) and IPv6 packets
  fr-de                Match on Frame-relay DE bit
  fr-dlci              Match on fr-dlci
  input-interface      Select an input interface to match
  ip                   IP specific values
  mpls                 Multi Protocol Label Switching specific values
  not                  Negate this match result
  packet               Layer 3 Packet length
  precedence           Match Precedence in IP(v4) and IPv6 packets
  protocol             Protocol
  qos-group            Qos-group
  source-address       Source address

CBWFQ(config-cmap)#match protocol ?
  arp            IP ARP
  bgp            Border Gateway Protocol
  bittorrent     bittorrent
  bridge         Bridging
  cdp            Cisco Discovery Protocol
  citrix         Citrix Traffic
  compressedtcp  Compressed TCP
  cuseeme        CU-SeeMe desktop video conference
  custom-01      Custom protocol custom-01
  dhcp           Dynamic Host Configuration
  dns            Domain Name Server lookup
  egp            Exterior Gateway Protocol
  eigrp          Enhanced Interior Gateway Routing Protocol
  exchange       MS-RPC for Exchange
  fasttrack      FastTrack Traffic - KaZaA, Morpheus, Grokster...
  finger         Finger
  ftp            File Transfer Protocol
  gnutella       Gnutella Traffic - BearShare,LimeWire,Gnotella...
```

```
  gopher          Gopher
  gre             Generic Routing Encapsulation
  http            World Wide Web traffic
  icmp            Internet Control Message
  imap            Internet Message Access Protocol
  ip              IP
  ipinip          IP in IP (encapsulation)
  ipsec           IP Security Protocol (ESP/AH)
  irc             Internet Relay Chat
  kazaa2          Kazaa Version 2
  kerberos        Kerberos
  l2tp            L2F/L2TP tunnel
  ldap            Lightweight Directory Access Protocol
  llc2            llc2
  napster         Napster Traffic
  netbios         NetBIOS
  netshow         Microsoft Netshow
  novadigm        Novadigm EDM
  ntp             Network Time Protocol
  pad             PAD links
  pcanywhere      Symantec pcANYWHERE
  pop3            Post Office Protocol
  rcmd            BSD r-commands (rsh, rlogin, rexec)
  rip             Routing Information Protocol
  rsvp            Resource Reservation Protocol
  rtp             Real Time Protocol
  rtspplayer      RTSP players streaming protocol
  secure-ftp      FTP over TLS/SSL
  secure-http     Secured HTTP
<output omitted>
```

There you have it. The match protocol command enables the NBAR feature. I highlighted some of the protocols that I thought would be of special interest to you. In that list (which I trimmed down quite a bit to save some pages), you see the http and ftp protocols (not all that exciting), but you also see things such as kazaa2, napster, and gnutella. These are actually peer-to-peer file sharing applications that plague network administrators everywhere. They can be used to download illegal and restricted software from around the Internet. (Some argue in favor of the legal uses for these applications, which are probably the same people who argue that mounting a missile launcher to the top of their vehicle could be used for defensive driving.) The trouble with these applications is that they can change port numbers to find an opening through a network firewall. However, if you are using NBAR to restrict them, you can match the application signature itself rather than the port number it uses.

With that in mind, we just need to use NBAR to match HTTP traffic, which is what we'll use for this example:

```
CBWFQ(config-cmap)#match protocol http
CBWFQ(config-cmap)#^Z
CBWFQ#show class-map
 Class Map match-all MATCH_HTTP (id 1)
   Match protocol http

 Class Map match-any class-default (id 0)
   Match any
```

After the `match protocol http` command is typed in, I've exited out to privileged mode and used the `show class-map` command to check my work. In this case, I see two class maps: `MATCH_HTTP` (which I just created) and `class-default` (which the router created). The `class-default` class map is always on the router to catch all traffic that does not explicitly match one of the class maps that you create.

For the sake of this example, let's add just one more class-map to our configuration to give us a little more to work with:

```
CBWFQ(config)#class-map match-all MATCH_FTP
CBWFQ(config-cmap)#match protocol ftp
CBWFQ(config-cmap)#^Z
CBWFQ#show class-map
 Class Map match-all MATCH_HTTP (id 1)
   Match protocol http

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all MATCH_FTP (id 2)
   Match protocol ftp
```

Alright, now that we've matched the traffic we're concerned with, we can move onto the policy-map and tell the router what to do with that traffic.

The policy-map configuration is pretty simple. All you need to do is tell the router how to treat each class of traffic. In our example, I might have something that looks like this (this is a plain-English example rather than true syntax):

policy-map Jeremy's_Policy
    For the class MATCH_HTTP
        Guarantee 500Kbps of bandwidth
    For the class MATCH_FTP
        Guarantee 40Kbps of bandwidth

For everything else (class-default)
Use WFQ

I want to emphasize a couple key points before we get into the configuration. First, it's only necessary to create a single policy-map for all of your policies. Truth be told, you can apply different policies on up to 256 classes of traffic using a single policy-map. In addition, policy-maps are like access lists in the sense that you can only apply one per interface, per direction. Here's the real syntax to do exactly what my preceding plain-English example shows:

```
CBWFQ(config)#policy-map ?
  WORD  policy-map name

CBWFQ(config)#policy-map Jeremy's_Policy
CBWFQ(config-pmap)#?
QoS policy-map configuration commands:
  class        policy criteria
  description  Policy-Map description
  exit         Exit from QoS policy-map configuration mode
  no           Negate or set default values of a command
  rename       Rename this policy-map
  <cr>

CBWFQ(config-pmap)#class MATCH_HTTP
CBWFQ(config-pmap-c)#?
QoS policy-map class configuration commands:
  bandwidth       Bandwidth
  drop            Drop all packets
  exit            Exit from QoS class action configuration mode
  no              Negate or set default values of a command
  priority        Strict Scheduling Priority for this Class
  queue-limit     Queue Max Threshold for Tail Drop
  random-detect   Enable Random Early Detection as drop policy
  service-policy  Configure QoS Service Policy
  set             Set QoS values
  shape           Traffic Shaping
  <cr>

CBWFQ(config-pmap-c)#bandwidth ?
  <8-2000000>  Kilo Bits per second
  percent      % of total Bandwidth
  remaining    % of the remaining bandwidth

CBWFQ(config-pmap-c)#bandwidth 500
CBWFQ(config-pmap-c)#exit
CBWFQ(config-pmap)#class MATCH_FTP
CBWFQ(config-pmap-c)#bandwidth 40
CBWFQ(config-pmap-c)#exit
CBWFQ(config-pmap)#class class-default
```

```
CBWFQ(config-pmap-c)#?
QoS policy-map class configuration commands:
  bandwidth       Bandwidth
  drop            Drop all packets
  exit            Exit from QoS class action configuration mode
  fair-queue      Enable Flow-based Fair Queuing in this Class
  no              Negate or set default values of a command
  priority        Strict Scheduling Priority for this Class
  queue-limit     Queue Max Threshold for Tail Drop
  random-detect   Enable Random Early Detection as drop policy
  service-policy  Configure QoS Service Policy
  set             Set QoS values
  shape           Traffic Shaping
  <cr>

CBWFQ(config-pmap-c)#fair-queue
```

Let me talk through the highlighted commands. First, we created the policy just by typing `policy-map` and a logical name (in this case, Jeremy's_Policy). Once we press the Enter key, we are taken to the policy-map configuration mode, where we can configure up to 256 different policies for 256 different classes of traffic. Now, we just tell the router what to do for each class. First, we access the MATCH_HTTP class and tell the router to guarantee it at least 400Kbps of interface bandwidth (by using the `bandwidth 400` command). This does not *limit* HTTP traffic to 400Kbps, but rather, ensures that it gets at least 400Kbps of the interface bandwidth. If you're looking to limit traffic, that's the job of a QoS Policing policy, which you'll learn in the CCVP track.

Once we have guaranteed HTTP the 400Kbps, we drop back to the policy-map configuration mode (just by typing `exit`) and enter the configuration mode for the MATCH_FTP class (by typing `class MATCH_FTP`). Once under there, we use the same command (`bandwidth 40`) to guarantee FTP 40Kbps. We then drop back to policy-map configuration mode one more time and access the class-default class, which matches any traffic other than HTTP and FTP. To enable WFQ for this class, we just enter the `fair-queue` command. By combining all these policies together, you have configured a CBWFQ QoS policy. The last step is to apply it.

Think of applying a QoS policy in exactly the same way that you think of applying an access list. You'll need to get into the configuration mode for the interface that will be using the policy and apply it in either the inbound or outbound direction. When thinking of this direction, remember, you are the router. Do you want this to affect traffic going away from you (outbound) or traffic coming into you (inbound)? In this case, we'll assume that the Ethernet0 interface on our router connects to the Internet. We'll apply our policy outbound on that interface to ensure that people can browse the Web and perform FTP file transfers at a decent speed.

```
CBWFQ(config)#interface ethernet 0
CBWFQ(config-if)#service-policy ?
```

```
  history  Keep history of QoS metrics
  input    Assign policy-map to the input of an interface
  output   Assign policy-map to the output of an interface

CBWFQ(config-if)#service-policy output ?
  WORD  policy-map name

CBWFQ(config-if)#service-policy output Jeremy's_Policy
```

At this point, our CBWFQ QoS policy is in effect. All the criteria that we configured under the Jeremy's_Policy policy-map is applied to our Ethernet0 interface in the outbound direction.

Low Latency Queuing

CBWFQ gives you quite a bit of flexibility with how you want to allocate bandwidth to your different traffic types, but it misses one major piece: priority. CBWFQ can guarantee bandwidth, but it can't guarantee that some bandwidth has priority over other bandwidth. This might sound silly, so let me give you an example. Let's say that I divide up my bandwidth: 500Kbps for HTTP, 40Kbps for FTP, and 300Kbps for Citrix. Now, Citrix is my "priority" application. It needs to get across the network with minimal delay. If I'm using CBWFQ, I can say that Citrix is guaranteed that 300Kbps, but it might be the last 300Kbps of bandwidth sent. The HTTP might get its 500Kbps before the 300Kbps that Citrix is guaranteed. This means that the Citrix traffic will sit in a router memory buffer until the HTTP traffic is sent, and then the Citrix traffic will be sent. While it's sitting in that memory buffer, delay is accumulating, causing potential problems with the Citrix session.

This is where Low Latency Queuing (LLQ) steps into the picture. The full name of LLQ is actually Priority Queuing, Class-based Weighted Fair Queuing (PQ-CBWFQ). I'm sure that you can see why Cisco decided to use the much shorter name. All LLQ does is add a priority mechanism to the CBWFQ QoS method we just covered. As before, I'll explain how this works as I show you the configuration. Because the CBWFQ component is exactly the same, I'll add the priority mechanism to the policy that we created in the last example.

```
CBWFQ#show policy-map
  Policy Map Jeremy's_Policy
    Class MATCH_HTTP
       Bandwidth 500 (kbps) Max Threshold 64 (packets)
    Class MATCH_FTP
       Bandwidth 40 (kbps) Max Threshold 64 (packets)
    Class class-default
      Flow based Fair Queueing
      Bandwidth 0 (kbps) Max Threshold 64 (packets)
```

As shown here, the Jeremy's_Policy is still in place with the bandwidth accurately allocated to the HTTP and FTP applications. In order to add the Citrix priority traffic to this policy, we must first create a class map that matches the Citrix traffic.

```
CBWFQ#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CBWFQ(config)#class-map MATCH_CITRIX
CBWFQ(config-cmap)#match protocol citrix
CBWFQ(config-cmap)#exit
CBWFQ(config)#
```

As before, I used the NBAR mechanism to match the Citrix protocol. I could have done the same thing by creating an access list that matches the port numbers that Citrix uses (this is TCP port 1494 and UDP port 1604); however, it's much easier to just type `match protocol Citrix`, and let the router figure that out for us. Now, we need to assign the Citrix class map the 300Kbps of priority bandwidth:

```
CBWFQ(config)#policy-map Jeremy's_Policy
CBWFQ(config-pmap)#class MATCH_CITRIX
CBWFQ(config-pmap-c)#?
QoS policy-map class configuration commands:
  bandwidth       Bandwidth
  drop            Drop all packets
  exit            Exit from QoS class action configuration mode
  no              Negate or set default values of a command
  priority         Strict Scheduling Priority for this Class
  queue-limit     Queue Max Threshold for Tail Drop
  random-detect   Enable Random Early Detection as drop policy
  service-policy  Configure QoS Service Policy
  set             Set QoS values
  shape           Traffic Shaping
  <cr>

CBWFQ(config-pmap-c)#priority ?
  <8-2000000>  Kilo Bits per second
  percent      % of total bandwidth

CBWFQ(config-pmap-c)#priority 300
CBWFQ(config-pmap-c)#^Z
CBWFQ#show policy-map
  Policy Map Jeremy's_Policy
    Class MATCH_HTTP
      Bandwidth 500 (kbps) Max Threshold 64 (packets)
    Class MATCH_FTP
      Bandwidth 40 (kbps) Max Threshold 64 (packets)
    Class MATCH_CITRIX
      Strict Priority
      Bandwidth 300 (kbps) Burst 7500 (Bytes)
    Class class-default
      Flow based Fair Queueing
      Bandwidth 0 (kbps) Max Threshold 64 (packets)
```

Now, you can see that Citrix is allocated 300Kbps of "Strict Priority" bandwidth. This is called Strict Priority because the router never allows Citrix to exceed 300Kbps per second. Even if

there is 1000Mbps of available bandwidth, Citrix will only get 300Kbps of it. This keeps these priority applications from eating the network alive. An older version of QoS, called Priority Queuing (PQ), gave applications priority in much this same way; however, it had no way of limiting how much bandwidth those priority applications could use. If a priority application decided that it wanted the entire 1000Mbps of your connection, it could have it and "starve" the rest of the applications on your network. Because of this, Cisco introduced the LLQ mechanism that uses Strict Priority. (Many people call this "Policed Priority" because it is a hard limit.)

Because the Jeremy's_Policy policy map is already applied to the Ethernet0 interface, our job here is done. Citrix is automatically getting the *first* 300Kbps of bandwidth from the interface, while HTTP and FTP get the 540Kbps guaranteed to them after Citrix has been served.

Compression on WAN Links

There are times when the company budget just cannot expand to accommodate the high-speed WAN connections demanded by many of the applications we use today. Compression allows you to "stretch" the available WAN bandwidth by cutting down the amount of data that is sent between locations. Before the data is sent, it is compressed to a smaller size, which in turn improves the WAN performance.

When you initially hear about compression, it might sound like a no-brainer to turn it on. However, compression on WAN links allows you to make a trade-off: less available processor, memory resources, and speed on your router for more bandwidth on your WAN links. Depending on the use of your router, this might be a pretty good deal; however, there are many other considerations to take into account before enabling compression. For example, WAN link compression immediately changes your router from a Fast Switched device over to a Process Switched device. This causes an overall slowdown of traffic passing through the router. If your traffic is delay sensitive (like some of the traffic types we mentioned previously in the queuing section), this could push it into an unacceptable delay range.

Because of the significant impact that compression can have on your router and network, Cisco implemented multiple types of compression that can fit most organizations. These compression types fall into three categories:

1. Link Compression
2. Payload Compression
3. Header Compression

Link Compression

Link compression is one of the most popular compression types because it does just what the name implies: compresses all data on the link. For this reason, many people call this Interface

Compression. You can think of this method as the most thorough compression mechanism because no bit of data that passes through your router is left uncompressed. Likewise, this method usually causes the most load on your router's processor and memory resources. Three different types of link compression are available to administrators who run PPP encapsulation on their WAN connections. If you run HDLC, you are reduced to a single type of link compression. Let's do a quick discussion of the differences:

1. Stacker Compression

This compression mechanism is supported on both PPP and HDLC encapsulated links and is commonly abbreviated as STAC. This compression algorithm applies a "flat compression" to all traffic that passes through the router interface. I call it this because it makes no effort to compress based on the type of traffic going through. If you send FTP traffic, HTTP traffic, or online gaming traffic, the compression is always applied in the same way. This compression algorithm is the most efficient when used on interfaces that have many different types of traffic passing through them. This algorithm also tends to require more processor resources and less memory resources than other compression algorithms. To enable it on an interface, use this single command:

```
Router(config-if)#compress stac
```

Keep in mind that this command will only work on HDLC and PPP point-to-point serial connections.

2. Predictor Compression

This compression mechanism is supported only on PPP encapsulated connections. The concept behind the Predictor compression algorithm is really quite amazing. Instead of applying a "flat compression" algorithm to all the traffic passing through the router, the router attempts to predict what traffic will be sent next. Every router that supports the Predictor algorithm is equipped with a code book (I like to think of it as a recipe book) that contains compressed "signals" for common code strings used by applications. The best way to think of it is like sign language for routers. Instead of spelling out an entire word, the routers can just flash each other a hand signal, and if they're both equipped with the same code book, they'll both understand what is meant.

The Predictor algorithm is best used when the traffic types crossing the links are relatively the same. If the traffic changes often, the routers must continually switch and rebuild code books, which can decrease the efficiency of the algorithm. Unlike its Stacker sidekick, the Predictor algorithm requires considerable memory resources from your router and a little less processor resources. To enable this algorithm on a PPP connection, use the following command:

```
Router(config-if)#compress predictor
```

3. Microsoft Point-to-Point Compression

Microsoft has developed its own version of compression that is used within Windows for the PPP dial-up connections. Because dial-up connections within Windows are usually slow

modem links, it can be very beneficial to enable the Microsoft Point-to-Point Compression (MPPC) for any Cisco routers that receive incoming calls from these dial-up clients. Once again, just a single command is necessary to accomplish this:

```
Router(config-if)#compress mppc
```

Payload Compression

Not all network administrators are lucky enough to have dedicated point-to-point connections between all their locations. Technology such as Frame Relay is typically used to provide lower connection costs between sites. If you were to implement link compression on this type of connection, the link would fail because the service provider needs to be able to read DLCI information in the header of the frame (which would be rendered unreadable by the compression algorithm). In this case, you can use link-specific payload compression to compress just the payload (which is the data portion) of the packet and leave the header information untouched so that the service provider is able to read it. The forms of payload compression vary based on the type of WAN connection you have installed. For example, if you were to implement payload compression for Frame Relay, you would type the following command under the interface connected to the Frame Relay service provider:

```
Router(config-if)#frame-relay payload-compress
```

Because payload compression is specific to WAN technology, it tends to drag this topic far outside the scope of the CCNA curriculum. You can refer to documentation that can direct you on how to enable compression for your specific WAN connection type (such as ATM or MPLS).

Header Compression

If payload compression focuses on just compressing the data, header compression is exactly the opposite: It focuses on compressing just the header information. This type of compression is useful when you have many packets that carry a small amount of data on a low-speed link. For example, a telnet session sends packets that contain one byte of information each because the packets contain only one character each. Because of this, the header to data ratio is skewed heavily in the direction of the header. This concept also applies to Voice over IP (VoIP) technology, which has a small amount of data (voice) and a large amount of header in each packet. There are two primary types of header compression: TCP header compression and RTP header compression. RTP header compression is used specifically for VoIP communication and is quite outside the scope of what the CCNA exam encompasses. However, TCP header compression can be used for any TCP-based application. To enable TCP header compression, just use the following command:

```
Router(config-if)#ip tcp header-compression
```

This command will work on PPP or HDLC encapsulated interfaces. In order for this to function without completely devastating your WAN connection, it must be enabled on *both* sides.

APPENDIX B

CD Contents and Installation Instructions

The CD features an innovative practice test engine powered by MeasureUp, including a full practice exam that includes simulations, giving you yet another effective tool to assess your readiness for the exam. Cisco simulations validate a person's hands-on skills in addition to knowledge. MeasureUp's Cisco simulations model real-life networking scenarios by requiring the user to perform tasks on simulated Cisco networking devices. MeasureUp's simulations measure troubleshooting and problem-solving skills to address realistic networking problems. The CD also includes a helpful "Need to Know More?" appendix that will break down by chapter extra resources you can visit if some of the topics in this book are still unclear to you.

Multiple Test Modes

MeasureUp practice tests are available in Study, Certification, Custom, Adaptive, Missed Question, and Non-Duplicate question modes.

Study Mode

Tests administered in Study Mode enable you to request the correct answer(s) and explanation for each question during the test. These tests are not timed. You can modify the testing environment *during* the test by clicking the Options button.

Certification Mode

Tests administered in Certification Mode closely simulate the actual testing environment you will encounter when taking a certification exam. These tests do not allow you to request the answer(s) or explanation for each question until after the exam.

Custom Mode

Custom Mode enables you to specify your preferred testing environment. Use this mode to specify the objectives you want to include in your test, the timer

length, and other test properties. You can also modify the testing environment *during* the test by clicking the Options button.

Adaptive Mode

Tests administered in Adaptive Mode closely simulate the actual testing environment you will encounter when taking an adaptive exam. After answering a question, you are not allowed to go back; you are allowed to only move forward during the exam.

Missed Question Mode

Missed Question Mode enables you to take a test containing only the questions you missed previously.

Non-Duplicate Mode

Non-Duplicate Mode allows you to take a test containing only questions not displayed previously.

Question Types

The practice question types simulate the real exam experience.

Random Questions and Order of Answers

This feature helps you learn the material in a way that prevents you from memorizing questions and answers. Each time you take a practice test, the questions and answers appear in a different randomized order.

Detailed Explanations of Correct and Incorrect Answers

You'll receive automatic feedback on all correct and incorrect answers. The detailed answer explanations are a superb learning tool in their own right.

Attention to Exam Objectives

MeasureUp practice tests are designed to appropriately balance the questions over each technical area covered by a specific exam.

Installing the CD

The minimum system requirements for the CD-ROM are as listed here:

- Windows 95, 98, Me, NT4, 2000, or XP
- 7MB disk space for testing engine
- An average of 1MB disk space for each test

NOTE

If you need technical support, please contact MeasureUp at 678-356-5050 or email support@measureup.com. Additionally, you'll find Frequently Asked Questions (FAQs) at www.measureup.com.

To install the CD-ROM, follow these instructions:

1. Close all applications before beginning this installation.
2. Insert the CD into your CD-ROM drive. If the setup starts automatically, go to step 6. If the setup does not start automatically, continue with step 3.
3. From the Start menu, select Run.
4. Click Browse to locate the MeasureUp CD. In the Browse dialog box, from the Look In drop-down list, select the CD-ROM drive.
5. In the Browse dialog box, double-click on `Setup.exe`. In the Run dialog box, click OK to begin the installation.
6. On the Welcome Screen, click Next.
7. To agree to the Software License Agreement, click Yes.
8. On the Choose Destination Location screen, click Next to install the software to `C:\Program Files\MeasureUp Practice Tests\Launch`.

NOTE

If you cannot locate MeasureUp Practice Tests through the Start menu, see the section later in this appendix titled "Creating a Shortcut to the MeasureUp Practice Tests."

9. On the Setup Type screen, select Individual Typical Setup. Click Next to continue.
10. On the Select Features screen, click the check box next to the test(s) you purchased. After you have checked your test(s), click Next.
11. On the Enter Text screen, type the password provided in this receipt and click Next. Follow this step for any additional tests.

12. On the Select Program Folder screen, verify that the Program Folder is set to MeasureUp Practice Tests and click Next.
13. After the installation is complete, verify that Yes, I Want to Restart My Computer Now is selected. If you select No, I Will Restart My Computer Later, you cannot use the program until you restart your computer.
14. Click Finish.
15. After restarting your computer, choose Start, Programs, MeasureUp Practice Tests, Launch.
16. On the MeasureUp welcome screen, click Create User Profile.
17. In the User Profile dialog box, complete the mandatory fields and click Create Profile.
18. Select the practice test you want to access and click Start Test.

Creating a Shortcut to the MeasureUp Practice Tests

To create a shortcut to the MeasureUp Practice Tests, follow these steps:

1. Right-click on your desktop.
2. From the shortcut menu select New, Shortcut.
3. Browse to `C:\Program Files\MeasureUp Practice Tests` and select the `MeasureUpCertification.exe` or `Localware.exe` file.
4. Click OK.
5. Click Next.
6. Rename the shortcut MeasureUp.
7. Click Finish.

After you have completed step 7, use the MeasureUp shortcut on your Desktop to access the MeasureUp products you ordered.

Technical Support

If you encounter problems with the MeasureUp test engine on the CD-ROM, you can contact MeasureUp at 678-356-5050 or email support@measureup.com. Technical support hours are from 8 a.m. to 5 p.m. EST Monday through Friday. Additionally, you can find Frequently Asked Questions (FAQs) at www.measureup.com.

If you'd like to purchase additional MeasureUp products, telephone 678-356-5050 or 800-649-1MUP (1687), or visit www.measureup.com.

Glossary

10BASE-T An IEEE 802.3 ethernet standard that has a maximum segment length of 100m and has a 10Mbps data transmission speed. 10BASE-T can use Category 3, 4, or 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cables for connectivity.

802.1q IEEE frame tagging method over trunk ports that insert the 4-byte VLAN identifier inside the original ethernet frame.

A

ABRs Area Border Routers sit in between multiple areas in a hierarchical OSPF network. These routers are responsible for summarizing subnets to the rest of the OSPF autonomous system. Because they must maintain topology information from several areas, these routers are typically robust in resources.

Access Ports Switch ports that have a single VLAN assigned to them. These are typically used for connectivity between end devices.

`access-class` The command used to apply an access list to VTY ports.

ACTIVE, INACTIVE, and **DELETED PVC Status** The three states of a Frame Relay PVC. Active means that the connection is good on both ends. Inactive means that the remote router is misconfigured. Deleted means that the local router is misconfigured.

Adjacency A term that describes the state after two OSPF neighbors have synchronized their topology databases.

Administrative Distance Arbitrary values between 1 and 255 that are assigned to determine the trustworthiness of the routing sources.

Advertised Distance The composite metric to a destination that is being advertised from our EIGRP neighbors.

Application Layer Layer 7 of the OSI model provides an interface between a host's communication software and any necessary external applications (that is, email, file transfers, and terminal emulation). This layer can also evaluate what resources are necessary to communicate between two devices and determine their availability.

Areas Subdivisions of an autonomous system comprised of groups of contiguous networks and attached hosts. Used in link-state routing protocols to minimize routing update overhead and confine network instability.

ARP (Address Resolution Protocol) A protocol that maps a known IP address to a MAC address by sending a broadcast ARP. When the destination IP address is on another subnet, the sender will broadcast ARP for the router's ethernet port or default gateway, so the MAC address sent back will be that of the router's ethernet port.

ASP (AppleTalk Session Protocol) A session layer protocol that manages client/server based communications, but is specific to AppleTalk client and server devices.

Asynchronous A serial interface that does not synchronize the clocks for the bit stream of the sending and receiving end of a serial link.

Asychronous Transfer Mode (ATM) A packet switched connection type that reaches high speeds by dividing all packets into equal-sized cells of 53 bytes each.

Attenuation A term used to describe how a signal loses strength over long distances.

Autonomous System A collection of routing devices under the same administrative control.

Autonomous System Number An indicator in a IGRP and EIGRP configuration that identifies the autonomous system the routers are actively sending routing updates.

Auxiliary Port Out-of-band management connection used to connect to an external modem with a rollover cable.

B

Backbone Area Also known as the transit area, Area 0 is an area to which all other areas must connect.

Backbone Routers Any router that is connected to Area 0.

BackboneFast Cisco STP enhancement that skips the max-age timer when switches learn of a failure indirectly.

Backwards Explicit Congestion Notification (BECN) A signaling method used by a Frame Relay service provider that attempts to drop the speed of a router sending excessive data.

Balanced Hybrid Routing Protocols A class of routing protocols that use the best characteristics from link-state and routing protocols, these advanced routing protocols efficiently and quickly build their routing information and converge when topology changes occur.

Bandwidth The total amount of information that can traverse a communications medium measured in millions of bits per second. Bandwidth is helpful for network performance analysis. Also, availability is increasing but limited.

Bandwidth on Demand (BOD) A Cisco extension to the PPP Multilink concept that allows more DDR connections to be brought up as bandwidth is needed and disconnected as bandwidth is not needed.

`bandwidth` *`speed`* Interface configuration command that assigns a logical speed to the interface for accurate routing metrics.

`banner motd` *`delimiting_char banner delimiting_char`* Global configuration command to create a message of the day login banner.

BDR Backup Designated Routers are elected in OSPF as a redundant device in case the Designated Router fails.

Bearer Channel (B-channel) Used as a building block for ISDN connections. Provides 64Kbps of bandwidth per channel.

Bellman-Ford Algorithm Routing algorithm used by RIP and IGRP, which entails routing updates being received and updated before propagating the message to other routing devices.

Binary A computer language that is represented by a bit value of 0 or 1.

Blocking Ports that are not the root or the designated port in a STP election that are left in a blocking state. Data is not transmitted on these ports, but BPDUs can still be received.

Bluetooth A wireless technology that uses a short-range wireless radio connection to allow various devices to interconnect. Such devices include cell phones, PCs, and personal digital assistants (PDAs). The only requirement to establish connectivity is a 10 meter range (approximately 33 feet) between communicating devices. When in range, Bluetooth uses an RF link in the 2.4GHz range that has a 720Kbps per channel capacity to transfer voice or data.

Boolean AND A mathematical operation that can be used to identify the network ID and broadcast IP given an IP address and subnet mask.

Boot Field Last hexadecimal character in configuration register that specifies where to find an IOS.

`boot system` *`location filename`* Global configuration command that specifies locations and filenames to load the IOS.

Bootstrap Instructions loaded from ROM to activate the IOS loading code.

BPDU Guard Cisco enhancement to PortFast, which prevents loops by moving an access port to a disabled state if a BPDU is received.

BPDUs Layer 2 messages sent in a STP environment to advertise Bridge IDs, Root Bridge MAC address, and root path costs.

BRI (Basic Rate Interface) An Integrated Services Digital Network (ISDN) line that consists of two 64Kbps bearer (B) channels and one 16Kbps data (D) channel. Voice, video, and data traffic can be carried over the B-channels. Signals between telephone company switches use the D-channel.

Bridge A hardware device at the Data Link layer that connects two segments in a single network or two networks together. They simply forward data between those segments/networks without performing an analysis or redirection of the data.

Bridge ID Arbitrary switch identifier composed of a combination of Bridge Priority + MAC address.

Broadband A term used to describe high-speed Internet connections such as DSL or cable modems.

Broadcast An ethernet LAN address in which a frame is sent to all devices in the same LAN. Broadcast addresses will always be the same value, which is FFFF.FFFF.FFFF.

Broadcast Domain A group of nodes that can receive each other's broadcast messages and are segmented by routers.

Broadcast IP The last IP address in a network. Every host bit for the broadcast IP address will be turned on (or all 1s).

Broadcast Multi-access (BMA) Topology A BMA topology consists of multiple devices that access the same medium and can hear each other's broadcasts and multicast messages such as ethernet networks.

Broadcast Subnet The last subnet in a network, which has all 1s in the subnet field.

Bus Topology A network topology that is set up so that the network nodes are connected via a single cable (also referred to as a trunk or a backbone). Electrical signals are sent from one end of the cable to the other.

C

CAM Table Content-Addressable Memory table in RAM that stores MAC addresses in a switch.

CDP Cisco Discovery Protocol is a Layer 2 Cisco-proprietary protocol that advertises information to directly connected Cisco neighbors.

`cdp enable` Interface configuration command to enable CDP on a interface (on by default).

`cdp run` Global configuration command to enable CDP on a device (on by default).

Challenge Handshake Authentication Protocol (CHAP) A strong authentication type used with PPP encapsulation. Passwords are hashed and sent multiple times over the course of a WAN connection.

Channel Associated Signaling (CAS) A type of connection that incorporates signaling information with the data being sent. Also called Robbed Bit Signaling (RBS).

CIDR (Classless Interdomain Routing) A way to allocate and specify Internet addresses used in inter-domain routing which offers more flexibility than the original system of IP address classes.

Circuit Switched Networks A WAN connection type that encompasses dial-on-demand technologies such as modems and ISDN.

Cisco, ANSI, and Q933A LMI signaling The three forms of Frame Relay LMI signaling. Cisco IOS 11.2 and later automatically detect the Frame Relay signaling type. Earlier versions of the IOS must be coded manually.

Cisco Frame Relay Encapsulation A Cisco proprietary Frame Relay encapsulation that can only be used when communicating through a Frame Relay service provider to other Cisco routers.

Classful Routing Protocols Routing updates only contain the classful networks without any subnet mask. Summarization is automatically done when a router advertises a network out an interface that is not within the same major subnet. Classful routing protocols must have a FLSM design and will not operate correctly with discontiguous networks.

Classless Routing Protocols Routing updates can contain subnetted networks because the subnet mask is advertised in the updates. Route summarization can be manually configured at any bit boundary. Classless routing protocols support VLSM designs and discontiguous networks.

CLI (Command-Line Interface) An interface that defines the commands used to communicate with the IOS.

Client Mode VTP mode in which you cannot create, modify, or delete VLANs. Will forward advertisements received from server, but does not save VLAN configuration into VLAN database.

`clock rate` *`speed`* Interface configuration command that specifies the clocking speed in bps.

Collision Domain A group of nodes that share the same media and are segmented by switches. A collision occurs if two nodes attempt a simultaneous transmission.

Committed Information Rate (CIR) The minimum speed guaranteed to a customer by a Frame Relay service provider.

Common Channel Signaling (CCS) A type of connection that separates signaling information from the data transmission. ISDN is a CCS-style technology.

Composite Metric A metric used by IGRP and EIGRP comprised of bandwith+delay by default. Can also support Reliability, Load, and MTU as well.

`config-register` *`register`* Global configuration command to alter the configuration register.

Configuration Register 16-bit (four hexadecimal characters) value in NVRAM that specifies how the router or switch should operate during initialization.

Connected Interface As soon as we assign an IP address to a working (up/line protocol up) interface, the router associates the entire subnet of the interface's IP address in the routing table.

Console Port Out-of-band management connection used to connect to a PC with a rollover cable.

`copy` *`from to`* Privileged EXEC command that copies files from one location to another location.

Cost An arbitrary number typically based on the bandwidth of the link.

Count to Infinity When routers are continuously passing updates to unreachable networks between each other in a routing loop, the metric will continue to increase forever.

CPE (Customer Premise Equipment) The term that refers to customer owned equipment, such as the router and typically the CSU/DSU.

Crosstalk An electrical or magnetic field that is a result of one communications signal that can affect the signal in a nearby circuit.

CSMA/CD A process that sends a jam signal to notify the devices that there has been a collision. The devices will then halt transmission for a random back-off time.

CSU/DSU (Channel Service Unit/Data Service Unit) A device that serves as an intermediary between the service provider and the WAN router. In most cases, the CSU/DSU provides clocking for the router.

Ctrl+Shift+6, x Keystroke to suspend telnet sessions and cancel lookups and pings.

Cut-through Frame transmission method that only looks at the destination MAC address in an ethernet frame and forwards it.

D

Data Link Connection Identifier (DLCI) A data link address used by Frame Relay.

Data Link Layer Layer 2 of the OSI model ensures reliable data transfer from the Network Layer to the Physical Layer for transmission across the network.

Data Packet A packet that transports data across the internetwork and is supported by IP and IPX protocols.

DCE (Data Circuit-Terminating Equipment) Also called Data Communications Equipment. The term used to identify a device that connects the Data Terminal Equipment (DTE) to a service provider's communications line. Types of DCE are modems, CSU/DSUs, and BRI NT-1s.

Default Gateway A gateway of last resort in switches and PCs. This default gateway is the IP address that hosts and switches send their traffic to when the destination is on another segment.

Default Route A gateway of last resort for a router when there isn't a specific match for an IP destination network in the routing table (such as packets destined for the Internet).

Delta Channel (D-channel) Used to send signaling information on ISDN connections. Provides 16Kbps (for BRI) or 64Kbps (for PRI) of signaling bandwidth.

Demarc (Demarcation) The point at which the telco terminates its line to the customer.

Designated Port On each STP segment, the switch with the lowest cumulative cost to the root has the designated port.

DHCP (Dynamic Host Configuration Protocol) An Application layer protocol that works dynamically to provide an IP address, subnet mask, domain name, and a default gateway to network clients.

Dial on Demand Routing (DDR) A technology used to bring up network connections when needed and disconnect them once the need is satisfied. Typically used for ISDN connections.

Dialer Interface A logical interface that contains a configuration that can be applied to a physical interface when needed.

Dialer Map Used to manually map a remote IP address to the phone number a router should dial to reach it.

Dialer Pool A pool of physical interfaces that a logical, daler interface can draw from when attempting to make a connection.

Dialer Profile A newer form of DDR connection that allows you to define different configurations to be applied to an ISDN interface when certain destinations are dialed.

Dialer List/Dialer Group The syntax used to create a list of interesting traffic (dialer list) and apply that list to an interface (dialer group).

Dijkstra SPF Algorithm Routing algorithm used by OSPF and ISIS that builds and calculates the shortest path to all known destinations.

Discard Eligible (De) Any traffic exceeding the CIR in a Frame Relay network is automatically marked by the service provider as Discard Eligible, which means that it could be dropped in the case of network congestion.

`disconnect` *`conn#`* User or Privileged EXEC command to disconnect a suspended telnet session.

Discontiguous Networks Major networks separated by another major network that are automatically summarized causing routing confusion.

Distance Vector Routing Protocols A class of routing protocols in which the entire routing table is periodically sent to directly connected neighbors regardless of a topology change. These routing protocols manipulate the routing table updates before sending that information to their neighbors and are slow to converge when a topology change occurs.

DNA SCP (Digital Network Architecture Session Control Protocol) A proprietary Digital Equipment Corporation Networking (DECnet) Session layer protocol and is also referred to as a DECnet session.

DNS (Domain Name System) An Application layer protocol that resolves hostnames and fully qualified domain names, such as www.cisco.com, into IP addresses.

DR Designated Routers are elected in OSPF to minimize routing update overhead that can occur in broadcast and non-broadcast multi-access topologies.

DS1 (Digital Signal Level 1) Also called a T1, this line offers a 1.544Mbps data transmission speed. A single T1 consists of 24 digital signal level 0 (DS0) channels that are 64Kbps each and an additional 8Kbps that are reserved for management overhead.

DTE (Data Terminal Equipment) A device at the user end of a network that is connected to the service provider via the DCE device. Types of DTE are PCs, routers, and servers.

DTP Dynamic Trunking Protocol used by Cisco to negotiate trunking.

DUAL Diffusing Update Algorithm is the algorithm used by EIGRP to determine the best loop-free path to a destination, as well as alternate paths in certain conditions.

Dual Ring Topology A network topology that uses two rings for redundancy purposes. If there is a failure on one ring, the other will provide operability.

Duplex The communication mode of a device that might either be half-duplex or full-duplex depending on the connection type.

Dynamic NAT Automatically performs NAT translations between two or more pools of addresses.

E

EGP Exterior Gateway Protocols are routing protocols that advertise networks in between autonomous systems.

EIA/TIA-232, -449, and -530 Physical serial interface standards on CSU/DSU devices.

EIGRP Enhanced Interior Gateway Routing Protocol is a Cisco proprietary enhancement of IGRP to support classless routing, multiple routed protocols, a 32-bit composite metric, and the DUAL algorithm for fast convergence and loop-free routing.

EMI (Electromagnetic Interference) The interference caused by electromagnetic signals, which can decrease data integrity.

`enable password` *`password`* Global configuration command that sets a clear text password for entering Privileged EXEC mode.

`enable secret` *`password`* Global configuration command that sets an MD5 encrypted password for entering Privileged EXEC mode.

Encapsulation The process of adding a header or trailer to the Protocol Data Unit at each layer of the OSI model.

`erase startup-config` Privileged EXEC command that deletes the startup-config in NVRAM to return the router or switch to the original "out-of-box" configuration after reboot.

EtherChannel Cisco link aggregation method that bundles multiple links between two switches into a single logical link.

Ethernet A LAN specification that first hit the scene in the 1970s when Xerox needed a networking system to connect personal computers.

`exec-timeout` *`minutes seconds`* Line configuration command that specifies the length of terminal inactivity before closing the EXEC session.

Extended Access List A list of permit and deny statements capable of matching network traffic based on the protocol used, source IP address, source port number, destination IP address, and destination port number.

F

Feasible Distance The composite metric comprised of the advertised distance to a destination plus the composite metric to reach that advertising router from the local router.

Feasible Successor Routes Backup routes in the EIGRP topology table that will be enabled if the successor route fails. Determined if the advertised distance of the candidate feasible successor is less than the feasible distance of the successor route.

FEXT (Far-end Crosstalk) The crosstalk measured at the far end of the cable from where the transmission was sent.

Fiber A cable that uses light rather than electric signals to send data transmissions. These optical light signals travel a fiberglass core, and you might hear this technology referred to as fiber optics or optical cabling. Fiber is not susceptible to electromagnetic interference.

Filter A program or device that uses a defined set of criteria to break up data and signals.

Flapping A term used to describe a failing interface that is constantly going up and down.

Flash A type of system memory that is installed on either an electrically erasable, programmable, read-only memory (EEPROM), or Personal Computer Memory Card International Association (PCMCIA) card. Flash memory contains the Cisco Internetworking Operating System (IOS) image. The router uses Flash by default to locate the IOS when it is booted. Configuration files might also be stored on a Flash card. Flash is also nonvolatile memory.

Floating Routes A route with a higher administrative distance that will enter the routing table when the primary route fails.

Flow Control A process that provides buffer controls that prevent packet flooding to the destination host. Buffers store bursts of data for processing when the transmission is complete.

FLSM Fixed Length Subnet Mask design assume that subnet routes from different parts of their classful network all use the same subnet mask that they use. Any subnetted networks must contain the same subnet mask throughout the topology.

Forward-delay Timer Time to transition from listening to learning and learning to forwarding. Each forward-delay is 15 seconds.

Forwarding STP port stare in which the interface is transmitting and receiving data.

Forwards Explicit Congestion Notification (FECN) A signaling method used by a Frame Relay service provider that attempts to drop the speed of a router sending excessive data by having a receiving router send traffic back to the sender tagged as a BECN message.

Fragment-free Frame transmission method that checks the first 64 bytes for frame fragments (due to collisions) before forwarding the frame.

Frame A packet that is formatted by the Data Link layer of the OSI model for transmission to the Physical layer.

Frame Relay One of the more popular packet switched connection types that establishes site-to-site connections through a service provider network. Can attain speeds up to T3 and uses DLCI numbers as its Layer 2 addressing.

FTP (File Transfer Protocol) An Application layer protocol that allows a user to transfer files and provides access to files and directories.

Full Mesh Design A costly, but fully redundant, packet switched network design in which all routers are directly connected to all other routers through virtual circuits.

Full Mesh Topology A network topology that is set up so that each device is directly connected to every other device on the network. This connection method has built-in redundancy. If one link goes down, the device will transmit via another link.

Full-duplex Bidirectional transmissions enabling higher throughput because CSMA/CD is disabled. Connections to other switches or devices can be full-duplex.

G

GBIC (Gigabit Interface Converters) An interface module that can be inserted into the Gigabit Ethernet slot on a switch to allow for different media connections to that port. The physical media can range from copper to single-mode fiber. A GBIC is also hot swappable, so it can be installed without interrupting service to that switch.

H

Half-duplex One-way communication transmission with sub-optimal throughput because it operates in a collision domain in which CSMA/CD must be enabled. When connected to a hub, must run half-duplex.

High-level Data Link Control (HDLC) A WAN encapsulation capable of being used over Leased Lines and Circuit Switched connections. Does not have many features, but uses minimal network overhead when communicating. Cisco's version of HDLC is proprietary.

Hold-down Timers A routing loop mitigation process in which a router will ignore any information about an alternative route with a higher metric to a poisoned subnet for an amount of time.

Hop A metric determined by the number of routers along the destination path.

Host Mask 255.255.255.255 or /32 subnet mask used on loopback interfaces to represent a single host.

`hostname` *`hostname`* Global configuration command to name the router.

HSSI (High-Speed Serial Interface) A high-speed interface that offers up to 52Mbps transmission rates to the WAN from a Cisco router. The higher speed capacity is relevant if the corporate backbone requires high-speed Internet access and VPN connectivity.

HTTP (Hypertext Transfer Protocol) An Application layer protocol that enables web browsing with the transmission of Hypertext Markup Language (HTML) documents on the Internet.

HTTPS (Secure Hypertext Transfer Protocol) An Application layer protocol that enables secure web browsing using SSL. A secure connection is indicated when the URL begins with https:// or when there is a lock symbol at the lower right corner of the web page that is being viewed.

Hub A multiple port repeater. A smaller hub consists of 4–5 ports and might be called a workgroup hub. When data is received, the hub then retransmits that data out on all of the other ports.

Hub and Spoke Design One of the lowest cost designs in a packet switched network. All offices connect to a central office (the hub) through a single virtual circuit connection. If the hub router goes down, all connectivity through the packet switched network is lost.

ICMP (Internet Control Messaging Protocol) A Network layer protocol that provides ping and traceroute utilities.

Idle Timer/Fast Idle Timer Configuration parameters used with DDR connections to set the amount of time the connection should stay online without seeing interesting traffic.

IETF Frame Relay Encapsulation An industry standard Frame Relay encapsulation that can be used when communicating with non-Cisco routers through a Frame Relay service provider.

IGP Interior Gateway Protocols are routing protocols that advertise networks and metrics within an autonomous system.

IGRP Interior Gateway Routing Protocol is a Cisco proprietary distance vector routing protocol that uses a composite metric to determine the optimal path.

In-band Management signals traversing over the same networking paths and interfaces as the data stream.

Infrared A wireless technology that uses infrared beams to pass data across the network. A television remote uses infrared technology to send requests to the television set. Speeds can reach a maximum of 16Mpbs, and signals are used for short distance communications.

Inside Global Address NAT terminology that describes the public address assigned to the NAT gateway.

Inside Local Address NAT terminology that describes the private addresses behind the NAT gateway.

Integrated Services Digital Network (ISDN) A circuit switched network that combines multiple B-channels that can handle 64Kbps each with a single signalling (D) channel to form a WAN connection between two locations.

Interesting Traffic Used when configuring DDR to tell the router what traffic is valuable enough to initiate a call using the DDR connection.

Interface Configuration Configuration mode that sets parameters specific to the interface.

`interface range` *`media port_range`* Switch global configuration command that navigates several switch ports that will ultimately share similar configuration parameters.

Internetwork The connection of more than one network. These networks are linked together by hardware devices to function as a larger single network. Internetworks can also be referred to as an Internet.

InterVLAN Routing Traffic routed from one VLAN to another by using an external router or a Layer 3 switch.

Inverse ARP A method that allows a Frame Relay router to automatically discover the remote routers by sending Inverse ARP messages to each local DLCI number it receives from the service provider.

Inverse Mask/Wildcard Mask A complete reversal of the subnet mask that is used primarily when configuring OSPF and access list.

IOS (Internetworking Operating System) The software developed and maintained by Cisco to support a full array of system functions, applications (including Internet applications), and network hardware in a single software package.

IP (Internet Protocol) A Network layer protocol that uses logical or virtual addressing to get a packet from a source to its destination. IP addresses are used by routers to make forwarding decisions.

`ip access-group` The command used to apply an access-list to an interface.

`ip address address subnet_mask` Interface configuration command that assigns an IP address to an interface.

`ip default-gateway gateway_IP` Switch global configuration command that sets a default route/gateway of last resort for a Layer 2 switch.

`ip domain-lookup` Global configuration command that enables dynamic name resolution lookups.

`ip host hostname IP` Global configuration command to create a static map of a IP address to a hostname.

`ip name-server dns_server_IP` Global configuration command that specifies up to six DNS servers for dynamic resolution.

IPv4 (IPversion4) A version of IP addressing that uses 32-bit addresses grouped into four octets. Each octet has a minimum value of 0 and a maximum value of 255. IPv4 addresses are presented in dotted decimal format.

ISDN Switch-Type A configuration parameter that sets the type of signaling required to communicate with the service provider's ISDN switch.

ISL Cisco frame tagging method over trunk ports that encapsulates the original frame with a 26 byte header and a 4 byte CRC.

L

LAN (Local Area Network) An internetwork that is limited to a local or small geographical area. An example of a LAN would be the individual computers or workstations that are connected on one floor of a building.

Learning STP port state in which the interface begins to build MAC addresses learned on the interface.

Leased Lines Typically the most expensive WAN connection that constructs a dedicated, point-to-point connection between locations.

Line Configuration Configuration mode that sets parameters specific to the terminal line.

Link Control Protocol (LCP) A sublayer protocol of PPP responsible for negotiating authentication, multilink, compression, and call back.

Link-State Routing Protocols A class of routing protocols in which all possible link states are stored in an independent topology table in which the best routes are calculated and put into the routing table. The topology table is initially synchronized with discovered neighbors followed by frequent hello messages. These routing protocols are faster to converge than distance vector routing protocols.

Listening STP port state in which the interface begins to transition to a forwarding state by listening and sending BPDUs. No user data sent.

LLC (Logical Link Control) A Data Link sublayer defined by IEEE 802.2.

Local Access Rate/Line Speed The maximum physical speed a WAN connection is capable of reaching.

Local Management Interface (LMI) The signaling method used between a Frame Relay service provider and the customer premise equipment.

`login` Line configuration command that enables prompting of a password on the terminal lines.

Longest Match Rule In routing logic, the longest match rule dictates that when there are several subnetted entries for a destination network, the smallest and more specific subnet is chosen over others.

Loopback Interface A virtual interface that does not go down unless the router is turned off. Used by OSPF to determine the Router ID.

LRE (Long Reach Ethernet) An ethernet specification developed by Cisco to provide broadband service over existing telephone-grade or Category 1, 2, or 3 wiring. Speeds vary between 5–15Mbps and can reach a maximum segment length of up to 5000m.

LSAs Link State Advertisements are used by OSPF to send hello messages and update information on attached interfaces, metrics used, and other variables.

LSUs Link State Updates are a specific type of LSA that entails new information being sent to neighbor routers after an adjacency has been formed with that neighbor.

M

MAC (Media Access Control) A Data Link sublayer defined by IEEE 802.3.

MAC Address A hard-coded (burnt-in) address on the network interface controller (NIC) of the Physical layer node attached to the network.

MAN (Metropolitan Area Network) An internetwork that is larger than a LAN but smaller than or equal in size to a WAN.

Management VLAN VLAN 1 by default. The management VLAN contains the switch's management IP address, CDP, and VTP advertisements.

Max-age Timer Maximum length of time a bridge port saves its configuration BPDU information. Value is 20 seconds by default.

Metro Ethernet A new type of technology allowing for low-cost, high-speed fiber connections between offices within metropolitan areas.

Microsegmentation The process in which a switch creates a dedicated path for sending and receiving transmissions with each connected host. Each host then has a separate collision domain and a dedicated bandwidth.

Microsoft Point-to-Point Compression (MPPC) A PPP compression algorithm developed by Microsoft for Windows dial-up clients.

Modem A device that converts a digital signal into an analog signal for transmission over a telephone line. The signal is converted back into a digital format when it reaches the device on the other end of that telephone line.

Multicast An ethernet LAN address in which a frame can be sent to a group of devices in the same LAN. IEEE Ethernet multicast addresses always begin with 0100.5E in hexadecimal format. The last three bytes can be any combination.

Multimode A type of fiber cable that is generally used for shorter distances and is ideal for a campus-sized network.

Multiplexing Combining multiple messages over a single channel.

N

Named Access List An access list identified by a name rather than a number. Can be standard or extended, and allows the deletion of individual access list lines.

NAT (Network Address Translation) A technique that translates a private IP address to a public IP address for outbound transmission to the Internet. NAT also translates a public IP address to a private IP address for inbound transmission on the internal network.

NAT Overload Allows multiple internal clients to share a single Internet IP address using port numbers to distinguish requests.

NAT Pool NAT terminology that describes a pool of addresses that a router can use for NAT translations.

Native VLANs VLAN 1 by default. Traffic originating from the Native VLAN are not tagged over the trunk link.

Neighbor Table Table used by link-state and balanced hybrid routing protocols that maintains all neighbors discovered by receiving hello messages from other routers using the same routing protocol.

Network Control Protocol (NCP) A sublayer protocol of PPP responsible for enabling multiple Network layer protocols to work over a PPP-encapsulated WAN connection.

Network ID Also called a network number or subnet ID, this address is the first IP address in a network. Every host bit for the network ID address will be turned off (or all 0s).

Network Interface A network component that provides connectivity from an end-user PC or laptop to the public network. Depending on the interface, you might see up to three light-emitting diodes (LEDs) that help to determine status of the connection.

Network Layer Layer 3 of the OSI model determines the best path for packet delivery across the network. Routed protocols such as IP are used to determine logical addressing that can identify the destination of a packet or datagram. The most common network device found at the Network layer is a router; however, Layer 3 switches might also be implemented.

Network Termination, Type 1 (NT-1) Converts the two-wire ISDN line the service provider installs in your location to a four-wire connection that your internal devices can use.

Network Termination, Type 2 (NT-2) This optional device allows you to either split the ISDN signal or aggregate multiple ISDN connections into a single stream.

NEXT (Near-end Crosstalk) The crosstalk measured at the transmitting end of a cable.

NFS (Network File System)/Pertaining to a Session Layer A Session layer protocol that accesses remote resources transparently and represents files and directories as if local to the user system.

NFS (Network File System)/Pertaining to an Application Layer An Application layer protocol that allows users with different operating systems (that is, NT and Unix workstations) to share files.

NNTP (Network News Transfer Protocol) An Application layer protocol that offers access to Usenet newsgroup postings.

`no shutdown` Interface configuration command that administratively enables an interface.

Non-Broadcast Multi-Access (NBMA) A WAN network design that allows multiple clients to attach, but not send broadcast messages to each other. Frame Relay is an example of an NBMA network.

Non-Broadcast Multi-Access Topology A NBMA topology consists of multiple devices that access the same medium and cannot hear each other's broadcasts and multicast messages such as Frame Relay networks.

NTP (Network Time Protocol) An Application layer protocol that synchronizes clocks on the Internet to provide accurate local time on the user system.

NVRAM (Nonvolatile Random Access Memory) A type of system memory that stores the startup configuration. This configuration is loaded when the router is booted.

O

ODR On-demand routing is an enhancement to CDP that enables a stub router to advertise the connected IP prefix.

OSI Model A layered architecture model created by the International Organization for Standardization (ISO) to internetwork various vendor specific networks.

OSPF Open Shortest Path First is an open-standard classless routing protocol that uses cost as a metric and uses areas to minimize routing overhead.

OSPF Priority An arbitrary number configured on an OSPF interface to influence a DR and BDR election. Default is 1.

Out-of-band Management signals traversing over a dedicated channel separate from the data stream.

Outside Global Address NAT terminology that describes an Internet valid address accessible from any device connected to the Internet.

Outside Local Address NAT terminology that describes an Internet valid address as it is seen from the internal network.

P

Packet A unit of data that contains control information and might also be referred to as a datagram. Packets are used by the Network layer of the OSI model.

Packet Switched Networks A type of WAN connection that establishes connections using virutal circuits. ATM, Frame Relay, and X.25 fall under this category of connection.

Partial Mesh Design A packet switched network design that compromises between cost and redundancy by providing key locations with multiple virtual circuit connections.

Partial Mesh Topology A network topology that has direct connectivity between some of the network devices, but not all of them, such as the full mesh topology.

Password Authentication Protocol (PAP) A weak authentication type used with PPP encapsulation. Usernames and passwords are transmitted a single time in clear-text format.

`password` *`password`* Line configuration command that specifies the password to be prompted on a terminal line.

PAT (Port Address Translation) A technique that translates a Transport protocol connection (TCP or UDP) from an outside network host/port to an internal network host/port.

PDU (Protocol Data Unit) A unit that includes the message and the protocol/control information from the forwarding layer of the OSI model.

Permanent Virtual Circuit (PVC) A permanently established virtual circuit through a service provider network.

Physical Layer Layer 1 of the OSI model that moves bits between nodes. Electrical, mechanical, procedural, and functional requirements are defined at the Physical layer to assist with the activation, maintenance, and deactivation of physical connectivity between devices.

Ping (Packet Internet Groper) An echo request sent by a device that uses ICMP at the Network layer to validate that an IP address exists and can accept requests. The response is called an echo response.

Point-to-Multipoint/Multipoint Subinterfaces A subinterface that allows multiple DLCI numbers to be mapped to remote IP addresses under the same logical interface.

Point-to-Point Protocol (PPP) A WAN encapsulation type that provides many features and is supported by nearly all router vendors.

Point-to-Point Subinterfaces A subinterface typically used for Frame Relay that assigns a single DLCI number to a single subinterface and creates a point-to-point style connection through a packet switched cloud.

Point-to-Point Topology A network topology in which two routing devices are separated by a segment.

Poison Reverse A routing loop mitigation process in which a router receives a poisoned route and overrides the split horizon rule to send the subnet as "possibly down" back to the source.

POP3 (Post Office Protocol 3) An Application layer protocol that receives electronic mail by accessing an Internet server.

Port Redirection NAT terminology that describes statically translating from one port to another.

Port Security A method to ensure that a defined number of MAC addresses are dynamically learned on a switch port.

PortFast Cisco STP enhancement that skips the listening and leaning port states for end-devices.

POST Power-on self test performed by ROM chip to initially test the hardware on bootup.

Power over Ethernet A technology that allows for an end device to receive power over a copper ethernet cable. End devices that might use PoE include IP telephones, video cameras, and card scanners.

PPP Multilink An industry standard feature that allows multiple connections to be bundled into a single, logical connection between two network locations.

PPP over ATM (PPPoA) An encapsulation typically used by DSL service providers to gain the features of PPP over an ATM connection.

PPP over Ethernet (PPPoE) An encapsulation typically used by DSL service providers to gain the features of PPP over a Ethernet connection.

Predictor Compression A dictionary-based compression type that attempts to predict the traffic patterns that will be sent over a WAN connection. Is good for links that have very few types of traffic. Uses more memory resources than the sister compression type, Stacker.

Presentation Layer Layer 6 of the OSI model presents data to the Application layer and acts as a data format translator.

Primary Rate Interface (PRI) A type of ISDN connection that uses 23 B-channels and a single D-channel. Provides bandwidth equivalent to a T1 line.

Private IP Addresses Addresses that are not routable over the Internet. These include the 10.0.0.0/8 network, the 172.16.0.0–172.31.255.255/16 networks, and the 192.168.0.0–192.168.255.255/24 networks.

Privileged Exec Highest privileged command mode that allows full access to all commands.

Process ID A number between 1 and 65535 that represents a unique instance of an OSPF process. The process ID is locally significant (does not have to match in all routers in the OSPF autonomous system).

Proxy ARP (Proxy Address Resolution Protocol) A protocol that allows a router to respond to an ARP request that has been sent to a remote host. Some UNIX machines (especially Solaris) rely on Proxy ARP versus default gateways.

Public IP Addresses Addresses routable over the Internet.

Q

Q.921 The ISDN D-channel protocol used at the Data Link layer.

Q.931 The ISDN D-channel protocol used at the Network layer.

QoS Quality of Service is the method of prioritizing certain types of traffic when congestion affects performance.

R

RAM (Random Access Memory) A type of memory that is used for short-term storage of a machine's running IOS and running configuration. This is the only type of system memory that is not permanent.

RARP (Reverse Address Resolution Protocol) A protocol that maps a known MAC address to an IP address.

Redistribution The method of configuring routing protocols to advertise networks from other routing protocols.

`reload` Privileged EXEC command to perform a reboot of the router or switch.

Repeater A device consists of a transmitter and a receiver. When a signal is received by the repeater, it amplifies the signal and then retransmits. This effectively enables the signal to travel over a greater distance.

`resume conn#` User or Privileged EXEC command resumes a suspended telnet session.

Ring Topology A network topology that is set up so that one device is directly connected to two other devices on the same network. When a device emits a data signal transmission, it is sent in a single direction to the next connected device. The transmission continues to pass along each device successively until it arrives back at the original transmitting device. This method creates a ring or a loop.

RIP Routing Information Protocol is a standard distance vector routing protocol that uses hop count as its only metric.

RIPv2 RIP version 2 is an enhancement to RIP to support classless updates, router authentication, and multicast updates.

ROM (Read-Only Memory) A type of system memory that contains the basic code for booting a device and maintaining power-on self test (POST), ROM Monitor (ROMmon), bootstrap, and RXBOOT.

ROMmon ROM Monitor is a small codeset in ROM that allows you to perform elementary functions to manually get the router or switch back to a functioning state.

Root Bridge The base of the STP topology calculations elected based on the lowest Bridge ID.

Root Port Non-root bridge port that has the lowest cumulative cost to a root bridge.

Route Poison A routing loop mitigation process in which a router will set a failed subnet to an infinite metric and advertise that to its neighbor.

Route Summarization Process of advertising multiple network IDs into a single route.

Route Update Packets A packet that sends updates to neighbor routers about all networks connected to that internetwork and is supported by routing protocols such as RIP, EIGRP, and OSPF.

Routed Protocol A protocol such as IP that can be routed using a router.

Router ID The IP address that a device is known to an OSPF autonomous system. Determined by the highest active loopback IP address that is configured when the OSPF process starts. If your router does not have a loopback interface, it will use the highest physical interface IP address.

Router-on-a-Stick InterVLAN routing method by trunking to an external router with subinterfaces.

Routing Protocol A protocol that uses a routing algorithm to route traffic on an internetwork. RIP, OSPF, and EIGRP are examples of routing protocols.

Routing Protocols Protocols exchanged between routing devices to dynamically advertise networks.

Routing Table The routing logic stored in RAM, where packet forwarding decisions are made.

RPC (Remote Procedure Call) A Session layer protocol that is the basis for client/server communications. Calls are created on the client and then carried out on the server.

RSTP IEEE 802.1r Rapid Spanning Tree Protocol incorporating similar technologies as Cisco's PortFast, UplinkFast, and BackboneFast.

Running-config Active configuration running in RAM.

RxBoot Also known as a mini-IOS, RxBoot is a limited IOS in ROM with enough functionality to load an IOS from a TFTP server.

S

SAN (Storage Area Network) A subnetwork or special purpose network whose purpose is to allow users on a larger network to connect various data storage devices with clusters of data servers.

Server Mode Default VTP mode that enables you to create, modify, and delete VLANS. These VLANs are advertised to other switches and saved in the VLAN database.

`service password-encryption` Global configuration command that encrypts all passwords that are clear text in the configuration.

Service Provider IDentifiers (SPIDs) Sometimes required on ISDN lines upon dial-in for billing purposes.

Session Layer Layer 5 of the OSI model handles dialog control among devices.

Setup Mode Interactive dialog session to establish an initial configuration. Setup mode is automatically loaded when there is a missing startup-config in NVRAM.

`show cdp neighbors` User or Privileged EXEC command to display the Device ID, local interface, holdtime, capability, platform, and port ID learned from CDP advertisements of directly connected neighbors.

`show cdp neighbors detail` User or Privileged EXEC command to display the output of the `show cdp neighbors` command in addition to the Cisco IOS version and the Layer 3 address of directly connected neighbors.

`show controller` User or Privileged EXEC command to display the interface microcode including whether a DTE or DCE cable connected to the interface.

`show flash` User or Privileged EXEC command to display the filenames and sizes of IOS files stored in Flash memory.

`show interfaces` User or Privileged EXEC command to display the status of the interfaces as well as physical and logical address, encapsulation, bandwidth, reliability, load, MTU, duplex, broadcasts, collisions, and frame errors.

`show ip interface brief` User or Privileged EXEC command to display a summary of the interface statuses and logical addressing.

`show sessions` User or Privileged EXEC command to verify active telnet sessions initiated from local device.

`show version` User or Privileged EXEC command to display the IOS version, system uptime, amount of RAM, NVRAM, Flash memory, and configuration register.

SIA Timer Stuck In Active timer is enabled when an EIGRP router goes into an active state in the event of a topology change. The SIA timer is the amount of time a neighbor EIGRP router has to respond to a query. The default is 180 seconds.

Single-mode A type of fiber cable that is used to span longer distances than multimode fiber. Single-mode fiber also allows for a higher data rate and faster data transmission speeds.

SMTP (Simple Mail Transfer Protocol) An Application layer protocol that sends electronic mail across the network.

SNMP (Simple Network Management Protocol) An Application layer protocol that monitors the network and manages configurations.

Spanning Tree Protocol A protocol that eliminates loops caused by redundant connections on a network.

Split-Horizon A distance vector routing protocol loop prevention mechanism that prevents data from being sent back in the direction from which it was received.

SQL (Structured Query Language) A Session layer protocol that functions as a query language that requests, updates, and manages databases.

SSH Secure Shell protocol that enables terminal encrypted connections to remote devices with an IP address.

Stacker Compression A flat compression type that uses the same compression algorithm for all traffic types. Is a good compression for links that have many types of traffic. Uses more processor resources than the sister compression type, Predictor.

Standard Access List A list of permit and deny statements capable of matching network traffic based only on the source IP address.

Star Topology A network topology that is the most commonly implemented network design. With this topology, there is a central device with separate connections to each end node. Each connection uses a separate cable. You might also hear this called a hub-and-spoke topology.

Startup-config Saved configuration stored in NVRAM that is loaded when the router or switch boots.

Static Frame Relay Map A manual method of mapping a local DLCI number to the remote IP address it is capable of reaching over a Frame Relay cloud.

Static NAT Manually maps a NAT-translated address, typically between a public Internet address and a private internal address.

Static Routes Manual entries an administrator enters into the configuration that describe the destination network and the next hop.

Store-and-Forward Latency varying transmission method that buffers the entire frame and calculates the CRC before forwarding the frame.

STP (Shielded Twisted-pair Cable) A branch of twisted-pair cabling that uses an additional shield that provides an additional reduction of interference and attenuation.

STP (Spanning-Tree Protocol) IEEE 802.1d Layer 2 protocol that provides a loop-free topology in a switched network.

Stub Networks A network with a single entry and exit point.

Subinterfaces Logical extensions of a physical interface that are treated by the IOS as actual interfaces.

Subnet (Subnetworks) A smaller network created from a Class A, B, or C network.

Subnet Mask A 32-bit address used by a network device to identify which part of an IP address is the subnet portion.

Subnetting The process of breaking a large network of IP addresses down into smaller, manageable address ranges.

Successor Routes The route in a topology table with the lowest feasible distance to a subnet. This route is also placed in the routing table.

Supernet A summarized route.

SVIs Switched Virtual Interfaces created in a Layer 3 switch to perform interVLAN routing.

Switch A multi-port bridge that uses Application Specific Integrated Circuit (ASIC) to forward frames at the Data Link layer. Each port of the switch has a dedicated bandwidth.

Switched Virtual Circuit (SVC) An on-demand virtual circuit through a service provider network.

Synchronous A serial interface that synchronizes clocks for the bit stream of both the sending and receiving end of a serial link.

T

TCP (Transmission Control Protocol) A reliable connection-oriented Transport layer protocol. TCP uses acknowledgments, sequencing, and flow control to ensure reliability.

TCP Established A type of extended access list entry that can be added to allow return traffic, satisfying a client request.

TCP/IP (Transmission Control Protocol/Internet Protocol) A suite of protocols developed by the Department of Defense to assist with the development of internetworks.

Telnet A TCP/IP protocol that provides terminal emulation to a remote host by creating a virtual terminal.

`telnet` *`IP_address`* User or Privileged EXEC command to initiate a virtual terminal session to a remote device.

Terminal Adapter (TA) This device converts an ISDN signal into some other type of signaling.

Terminal Editing Keys Shortcut keys to navigate the cursor in lieu of the arrow keys.

Terminal Endpoint, Type 1 (TE1) This is an ISDN compatible endpoint, such as a router with an ISDN S/T or U interface.

Terminal Endpoint, Type 2 (TE2) This is an non-ISDN compatible endpoint, such as a router with no ISDN interfaces or an end-user PC, requiring a Terminal Adapter (TA) to understand the ISDN signal, such as a router with no ISDN interfaces or an end-user PC.

TFTP (Trivial File Transfer Protocol) An Application layer protocol that is a bare bones version of FTP that does not provide access to directories. With TFTP, you can simply send and receive files.

Token Ring A LAN protocol that uses a token-passing media access technology in a physical ring or physical star topology, which creates a logical ring topology. Token Ring is defined by the IEEE 802.5 standard.

Token-passing A process in which a three-byte token (or special bit pattern) is inserted in a frame and passed in a single direction from one node to another until it forms a complete loop. The node that has possession of the token is the only one that can send data at any given time on that LAN. Because only one node can send data at a time, collisions are avoided.

Topology Table Table used by link-state and balanced hybrid routing protocols that maintains every possible route to any given subnet along with its associated metric.

Traceroute A Network layer tool that traces the route or path taken from a client to a remote host. Traceroute also reports the IP addresses of the routers at each next hop on the way to the destination.

Transparent Bridge A bridge that goes unnoticed by the other devices on a network.

Transparent Mode VTP mode in which you can create, modify, and delete VLANs only on the local switch. Transparent switches do not participate in VTP but forward VTP advertisements received from servers. Also saves VLAN configuration in VLAN database.

Transport Layer Layer 4 of the OSI model is responsible for end-to-end connections and data delivery between two hosts. The capability to segment and reassemble data is a key functionality of this layer.

Triggered Updates A routing loop mitigation process in which a router will immediately shoot out an update as opposed to waiting for normal update interval.

Trunk An interconnection between switches that multiplexes traffic from all VLANs to other switches.

U

UDP (User Datagram Protocol) An unreliable connectionless Transport layer protocol. UDP headers contain only the source and destination ports, a length field, and a checksum.

Unicast An Ethernet LAN address that identifies the MAC address of an individual LAN or NIC card.

UplinkFast Cisco STP enhancement that skips the listening and leaning port states on redundant trunk links to distribution layer switch.

User EXEC Initial command mode with limited commands to test connectivity and verify statistics.

UTP (Unshielded Twisted-pair Cable) A branch of twisted-pair cabling that uses four pairs of colored wire. UTP is vulnerable to EMI and uses an RJ45 connector. There are five categories of UTP cable labeled Category 1 to Category 5.

V

V.35 A physical serial interface standard on CSU/DSU devices.

Variance A multiplier used in IGRP and EIGRP that enables these routing protocols to load balance over unequal paths.

Virtual Circuit A logical connection through a service provider network that makes the attached routers believe they are directly connected together.

Virtual Private Networks (VPNs) A type of network connection that allows secure transmission of network data over the Internet between two or more locations.

VLAN (Virtual LAN) A group of devices that can be part of a single LAN or multiple LANs that are joined together by software to create a single virtual network.

VLANs Layer 2 method of segmenting broadcast domains. Each VLAN created in a switch represents a logical grouping of devices into their own broadcast domain.

VLSM Variable Length Subnet Mask designs allow you to allocate an IP subnet according to the needed number of hosts for that subnet. Requires classless routing.

VMPS VLAN Membership Policy Server is a dynamic method of associating MAC addressed with VLANs.

VTP VLAN Trunking Protocol is a Layer 2 Cisco proprietary protocol that minimizes the administrative overhead involved in replicating VLAN configurations by having a VTP server advertise the VLAN configurations.

VTP Domains A collection of switches participating in VTP advertisements.

VTP Pruning Reduces unnecessary flooded traffic, such as broadcast, multicast, unknown, and flooded unicast packets to other switches by repressing flooded traffic to switches from inactive VLANs.

W

WAN (Wide Area Network) An internetwork that covers more than one geographical area.

Wildcard Mask Sometimes referred to as an inverse mask, the wildcard mask is used to identify to the IOS how much of an IP address should be applied to a criteria in a configuration statement. A zero means that the corresponding bit must match. A one means to ignore the corresponding bit value.

Windowing A process used by TCP in which windows are determined by the receiving system to limit the amount of data segments (bytes) that can be sent by the source device without an acknowledgment from the recipient. Window sizes vary and can change throughout the duration of a connection.

Wireless Fidelity A wireless networking standard defined by IEEE 802.11. The 802.11 standard allows for transmission speeds of up to 1–2Mbps and uses a Radio Frequency of 2.4GHz.

X-Z

X Window A Session layer protocol that communicates with remote Unix machines and allows the user to operate the device as if attached locally.

X.21 A physical serial interface standard on CSU/DSU devices.

X.25 The predecessor packet switched technology to Frame Relay. X.25 used excessive error checking, which slowed the connection down.

Zero Subnet Rule The first subnet in a network that has all binary 0s in the subnet field.

Index

Symbols & Numbers

A

B

C

D

E

F

G

H

I - J - K

L

M

N

O

P

Q - R

S

T

U

V

W - Z