

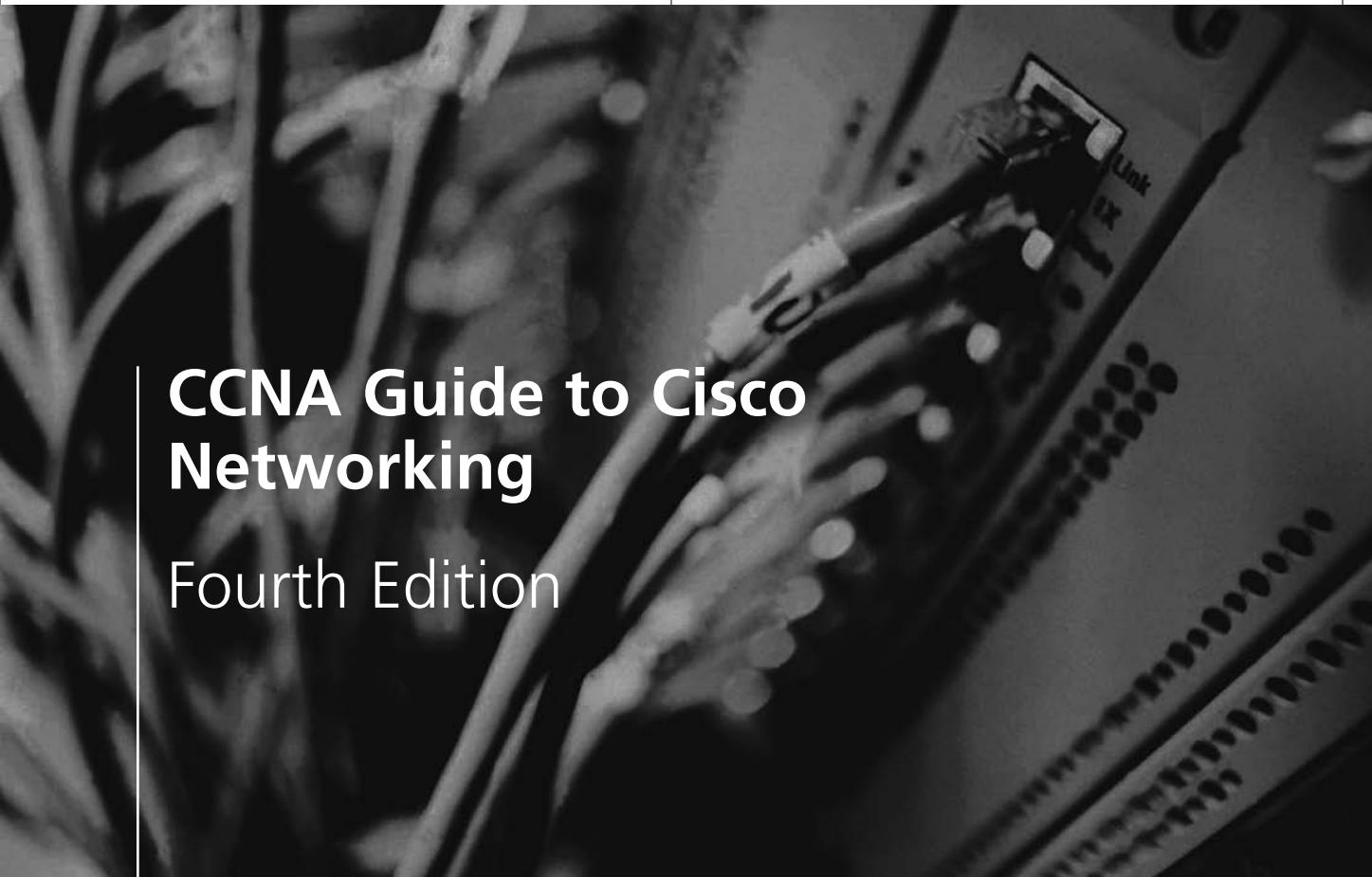
## **Cisco Certification Exam Objectives**

### **Exam # 640-802: Cisco Certified Network Associate**

This table maps the Cisco CCNA exam topics with the book chapter in which these topics are covered. There are eight categories of objectives assigned by Cisco.

Appendix A, CCNA Certification Objectives, provides a detailed exam objectives mapping grid.

<b>Exam Topic</b>	<b>Chapter</b>
Describe how a network works	1, 2, 3, 7, 8
Configure, verify, and troubleshoot a switch with VLANs and interswitch communications	2, 12, 13
Implement an IP addressing scheme and IP services to meet network requirements in a medium-size enterprise branch office network	4, 9
Configure, verify, and troubleshoot basic router operation and routing on Cisco devices	5, 6, 7, 8, 10, 14
Explain and select the appropriate administrative tasks required for a WLAN	2
Identify security threats to a network and describe general methods to mitigate those threats	14
Implement, verify, and troubleshoot NAT and ACLs in a medium-size enterprise branch office network	9, 10
Implement and verify WAN links	6, 11, 14



# CCNA Guide to Cisco Networking

## Fourth Edition

**Kelly Cannon**

**Kelly Caudle**

**Anthony Chiarella**



**COURSE TECHNOLOGY**  
CENGAGE Learning™

---

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

**CCNA Guide to Cisco Networking,  
Fourth Edition**

Kelly Cannon, Kelly Caudle,  
Anthony Chiarella

Vice President, Career and Professional  
Editorial: Dave Garza

Director of Learning Solutions:  
Matthew Kane

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Acquisitions Editor: Nick Lombardi

Senior Product Manager: Michelle  
Ruelos Cannistraci

Developmental Editor: Ann Shaffer

Editorial Assistant: Sarah Pickering

Vice President, Career and Professional  
Marketing: Jennifer McAvey

Marketing Director: Deborah S. Yarnell

Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Content Project Manager:  
Jessica McNavich

Art Director: Kun-Tee Chang

Cover photo or illustration:  
Stockbyte/Veer

Technology Project Manager:  
Joseph Pliss

Manufacturing Coordinator:  
Denise Powers

Copyeditor: Gary Michael Spahl

Proofreader: Brandy Lilly

Compositor: International Typesetting  
and Composition

© 2009 Course Technology, Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at  
**Cengage Learning Customer & Sales Support, 1-800-354-9706**

For permission to use material from this text or product,  
submit all requests online at [www.cengage.com/permissions](http://www.cengage.com/permissions)

Further permissions questions can be e-mailed to  
[permissionrequest@cengage.com](mailto:permissionrequest@cengage.com)

Library of Congress Control Number: 2008935580

ISBN-13: 978-1-4188-3705-1

ISBN-10: 1-4188-3705-9

**Course Technology**

25 Thomson Place  
Boston, MA 02210  
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: [www.international.cengage.com/region](http://www.international.cengage.com/region)

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For your lifelong learning solutions, visit [www.course.cengage.com](http://www.course.cengage.com)

Visit our corporate website at [www.cengage.com](http://www.cengage.com).

Printed in Canada

1 2 3 4 5 6 7 12 11 10 09 08

# Brief Contents

PREFACE	xv
CHAPTER 1 <b>Introducing Networks</b>	1
CHAPTER 2 <b>Network Devices</b>	25
CHAPTER 3 <b>TCP/IP</b>	53
CHAPTER 4 <b>IP Addressing</b>	87
CHAPTER 5 <b>Router and IOS Basics</b>	117
CHAPTER 6 <b>Router Startup and Configuration</b>	145
CHAPTER 7 <b>Routing Protocols</b>	171
CHAPTER 8 <b>Advanced Routing Protocols</b>	199
CHAPTER 9 <b>Network Services</b>	237
CHAPTER 10 <b>Access Lists</b>	259
CHAPTER 11 <b>PPP and Frame Relay</b>	301
CHAPTER 12 <b>Basic Switching and Switch Configuration</b>	337
CHAPTER 13 <b>Advanced Switching Concepts</b>	365
CHAPTER 14 <b>Network Security</b>	389
APPENDIX A <b>CCNA Certification Objectives</b>	423
APPENDIX B <b>Additional Resources</b>	429
APPENDIX C <b>A Networking Professional's Toolkit</b>	433
APPENDIX D <b>Command Summary</b>	443
APPENDIX E <b>Troubleshooting Summary</b>	453
LAB MANUAL	461
LAB MANUAL CHAPTER 1 <b>Introducing Networks</b>	463

**iv Brief Contents**

LAB MANUAL CHAPTER 2 <b>Network Devices</b>	<b>473</b>
LAB MANUAL CHAPTER 3 <b>TCP/IP</b>	<b>485</b>
LAB MANUAL CHAPTER 4 <b>IP Addressing</b>	<b>493</b>
LAB MANUAL CHAPTER 5 <b>Router and IOS Basics</b>	<b>507</b>
LAB MANUAL CHAPTER 6 <b>Router Startup and Configuration</b>	<b>525</b>
LAB MANUAL CHAPTER 7 <b>Routing Protocols</b>	<b>545</b>
LAB MANUAL CHAPTER 8 <b>Advanced Routing Protocols</b>	<b>555</b>
LAB MANUAL CHAPTER 9 <b>Network Services</b>	<b>569</b>
LAB MANUAL CHAPTER 10 <b>Access Lists</b>	<b>579</b>
LAB MANUAL CHAPTER 11 <b>PPP and Frame Relay</b>	<b>591</b>
LAB MANUAL CHAPTER 12 <b>Basic Switching and Switch Configuration</b>	<b>603</b>
LAB MANUAL CHAPTER 13 <b>Advanced Switching Concepts</b>	<b>617</b>
LAB MANUAL CHAPTER 14 <b>Network Security</b>	<b>629</b>
INDEX	637

# Table of Contents

PREFACE	xv
<b>CHAPTER 1</b>	
<b>Introducing Networks</b>	<b>1</b>
Introduction to Networking	2
Origin of Networking	2
Why Do We Use Networks?	2
Networking Terminology	3
Understanding the OSI Model	4
Reasons for Layering	5
Peer OSI Communication	6
Layer Functions	6
Chapter Summary	15
Key Terms	15
Review Questions	19
Case Projects	23
<b>CHAPTER 2</b>	
<b>Network Devices</b>	<b>25</b>
Repeaters	26
Hubs	27
Advantages and Disadvantages of Repeaters and Hubs	28
Wireless Access Points	28
Wireless Standards and Organizations	29
Wireless Network Components	30
Wireless Connectivity	30
Wireless Security Measures	30
Wireless Troubleshooting	31
Advantages and Disadvantages of Wireless Access Points	32
Network Segmentation	32
Bridges	33
Transparent Bridges	34
Source-Routing Bridges	34
Translation Bridges	35
Advantages and Disadvantages of Bridges	35
Switches	35
Advantages and Disadvantages of Switches	36
Routers	37
Physical vs. Logical Addresses	38
Advantages and Disadvantages of Routers	38
Brouters	39
Gateways	40
Ethernet Operations	40
CSMA/CD	40
Fast Ethernet	41
Gigabit Ethernet	41
Half- and Full-Duplex Communications	41

**vi Table of Contents**

Chapter Summary	42
Key Terms	43
Review Questions	46
Case Projects	51
 <b>CHAPTER 3</b>	
<b>TCP/IP</b>	<b>53</b>
Origins of TCP/IP	54
Overview of the TCP/IP Protocol Suite	54
Application Layer	55
Transport Layer	56
Internetwork Layer	62
Network Interface Layer	70
Understanding Frame Transmission	70
Routers on the Network	70
Network to Network	72
Dynamic or Static Tables	72
Transmitting Packets to Remote Segments	73
Routing Packets	74
The Cisco Three-Layer Hierarchical Model	76
Access Layer	77
Distribution Layer	77
Core Layer	77
Chapter Summary	78
Key Terms	79
Review Questions	82
Case Projects	85
 <b>CHAPTER 4</b>	
<b>IP Addressing</b>	<b>87</b>
IP Addressing	88
MAC to IP Address Comparison	88
IP Classes	89
Network Addressing	92
Broadcast Types	95
Subdividing IP Classes	95
Subnet Masking	96
Learning to Subnet	98
Subnetting Formulas	100
CIDR	101
Summarization	101
Variable Length Subnet Masks	102
Working with Hexadecimal Numbers	105
IPv4 versus IPv6	107
Transitioning to IPv6	108
Chapter Summary	109
Key Terms	110
Review Questions	111
Case Projects	115

<b>CHAPTER 5</b>	
<b>Router and IOS Basics</b>	<b>117</b>
Benefits of Routing	118
Cisco Router User Interface	118
Connecting via Terminal Programs	120
System Configuration Dialog	121
User Interface	121
Configuration Modes	123
Plethora of Passwords	125
Enhanced Editing	129
Command History	130
Configuring Router Identification	130
Configuring the Time and Date	132
Router Components	132
ROM	132
Flash Memory	133
NVRAM	133
RAM/DRAM	134
Interfaces	134
Chapter Summary	137
Key Terms	137
Review Questions	139
Case Projects	143
<b>CHAPTER 6</b>	
<b>Router Startup and Configuration</b>	<b>145</b>
Router Startup	146
Test Hardware (POST)	147
Router Configuration Files	147
Methods for Making Changes	148
IP on the Router	149
IP Connectivity	149
Telnet	150
IP Host Names	150
Ping and Trace	151
IP Route	152
Checking the Interface	152
CDP	155
Cisco IOS	156
Configuration Register	156
ROM Monitor Mode	159
RxBoot Mode	159
Boot System Commands	160
Backing Up and Restoring the IOS	160
Upgrading the IOS	161
Router Password Recovery	161
Security Device Manager	162
Chapter Summary	163
Key Terms	163
Review Questions	164
Case Projects	168

**viii Table of Contents**

<b>CHAPTER 7</b>	
<b>Routing Protocols</b>	<b>171</b>
Nonroutable Protocols	172
Routed Protocols	173
Routing Protocols	174
Two Types of IGPs	176
Routing Information Protocol	180
Enabling RIP Routing	181
Configuring RIP Routing for Each Major Network	182
Show ip protocol and debug ip rip Commands	183
Interior Gateway Routing Protocol	186
Static Routing	187
Adding Static Routes	187
Chapter Summary	190
Key Terms	191
Review Questions	193
Case Projects	197
<b>CHAPTER 8</b>	
<b>Advanced Routing Protocols</b>	<b>199</b>
Classful and Classless Routing Protocols	200
Routing Information Protocol version 2	206
Enhanced Interior Gateway Routing Protocol	210
EIGRP Components	213
EIGRP Configuration	217
Open Shortest Path First	220
OSPF Concepts	221
OSPF Operation	225
Single-Area OSPF Configuration	227
OSPF Authentication	228
Controlling Route Traffic	230
Chapter Summary	230
Key Terms	231
Review Questions	232
Case Projects	235
<b>CHAPTER 9</b>	
<b>Network Services</b>	<b>237</b>
Network Address Translation	238
Static NAT	239
Dynamic NAT	240
Port Address Translation	240
Configuring Network Address Translation	241
Configuring Static NAT	241
Configuring Dynamic NAT	242
Domain Name Service	244
Dynamic Host Configuration Protocol	246

Security Device Manager	248
Chapter Summary	253
Key Terms	253
Review Questions	254
Case Projects	257
<b>CHAPTER 10</b>	
<b>Access Lists</b>	<b>259</b>
Access Lists: Usage and Rules	260
Access List Usage	260
Problems with Access Lists	261
Access List Rules	262
Standard IP Access Lists	265
Standard IP Access List Examples	268
Monitoring Standard IP Access Lists	273
Extended IP Access Lists	273
Extended IP Access List Examples	274
The “Established” Parameter	277
Monitoring Extended IP Access Lists	278
Using Named Lists	279
Controlling VTY Line Access	279
Using Security Device Manager to Create Access Control Lists	280
Using Security Device Manager to Create a Router Firewall	286
Chapter Summary	295
Key Terms	296
Review Questions	296
Case Projects	300
<b>CHAPTER 11</b>	
<b>PPP and Frame Relay</b>	<b>301</b>
PPP	302
PPP in the Protocol Stack	302
Frame Format	303
Establishing PPP Communications	305
Frame Relay Standards and Equipment	308
Virtual Circuits	310
DLCI	310
Frame Relay Map	310
LMI	312
Inverse ARP	312
Encapsulation Types	313
Performance Parameters	316
Congestion	317
Frame Format	317
Frame Relay Topologies	318
Frame Relay Configuration	319
Basic Multipoint Configuration with Two Routers	319
Multipoint Configuration Using a Subinterface	321

**x Table of Contents**

Point-to-Point Configuration Using Subinterfaces	322
Frame Relay Static Mapping	324
Non-Cisco Routers	324
Keepalive Configuration	324
<b>Monitoring Frame Relay</b>	<b>324</b>
Chapter Summary	326
Key Terms	327
Review Questions	329
Case Projects	335
 <b>CHAPTER 12</b>	
<b>Basic Switching and Switch Configuration</b>	<b>337</b>
Ethernet Operations	338
CSMA/CD	338
Latency	340
Ethernet Errors	341
Gigabit Ethernet	342
Half- and Full-Duplex Communications	343
A Review of LAN Segmentation	344
Segmenting with Bridges	344
Segmenting with Routers	345
LAN Switching	346
Segmentation with Switches	346
Switch Operations	348
Switching Methods	348
Cut-Through Forwarding	349
Switch User Interface	351
Modes and Passwords	351
Setting the Host Name	352
IP on the Switch	352
Configuring Switch Ports	353
Securing Switch Ports	353
Chapter Summary	354
Key Terms	355
Review Questions	359
Case Projects	363
 <b>CHAPTER 13</b>	
<b>Advanced Switching Concepts</b>	<b>365</b>
Spanning Tree Protocol	366
Virtual LANs	370
Benefits of VLANs	372
Dynamic vs. Static VLANs	373
VLAN Standardization	373
Creating VLANs	374
Link Types and Configuration	375
VLAN Trunking Protocol	377
Nonswitching Hubs and VLANs	378
Routers and VLANs	378
Chapter Summary	382

Key Terms	382
Review Questions	384
Case Projects	388
<b>CHAPTER 14</b>	
<b>Network Security</b>	<b>389</b>
General Network Security	390
Protecting the Hardware	390
Protecting Software	391
Malware Prevention	391
Firewalls	393
Permissions, Encryption, and Authentication	395
Mitigating Security Threats	397
Secure Shell (SSH) Connections	398
Disabling Unnecessary Services	398
Patch Management	399
Virtual Private Networks (VPNs)	400
IPSec	401
IPSec Protocols	401
IPSec Authentication Algorithms	402
IPSec Encryption Algorithms	402
IPSec Key Management	402
IPSec Transform Sets	402
Creating VPNs with the Security Device Manager (SDM)	402
Cisco Security Audit Wizard	409
Chapter Summary	414
Key Terms	414
Review Questions	417
Case Studies	420
<b>APPENDIX A</b>	
<b>CCNA Certification Objectives</b>	<b>423</b>
<b>APPENDIX B</b>	
<b>Additional Resources</b>	<b>429</b>
Internet Resources	430
Standards Organizations	430
Technology Reference	430
Networking Overviews and Tutorials	431
Technical Forums	431
Cisco Routers	431
Exam Preparation Resources	431
<b>APPENDIX C</b>	
<b>A Networking Professional's Toolkit</b>	<b>433</b>
<b>APPENDIX D</b>	
<b>Command Summary</b>	<b>443</b>
Identification and Navigation	444
Passwords	446

**xii Table of Contents**

Router/Switch General and Startup Configuration	446
Examining the Router and Switch	447
Interface Configuration	447
IP Commands	448
Access Lists	450
WAN Configuration	450
SWITCH/VLAN Configuration	451
<b>APPENDIX E</b>	
<b>Troubleshooting Summary</b>	<b>453</b>
Router Troubleshooting Commands	454
Switch Troubleshooting Commands	456
Using Troubleshooting Commands	458
Troubleshooting Example	458
<b>LAB MANUAL</b>	461
<b>LAB MANUAL CHAPTER 1</b>	
<b>Introducing Networks</b>	<b>463</b>
Lab 1.1 Understanding the OSI Model	464
Lab 1.2 Understanding the Five Steps of Data Encapsulation	466
Lab 1.3 Identifying Data Link and Network Layer Addresses	468
Lab 1.4 Connection-Oriented vs. Connectionless Communications	471
<b>LAB MANUAL CHAPTER 2</b>	
<b>Network Devices</b>	<b>473</b>
Lab 2.1 Simulating a Network by Connecting a CSU/DSU, Router, Switch, Bridge, Three Hubs, and Nine Computers	474
Lab 2.2 Understanding Various Device Functions	477
Lab 2.3 Understanding the Difference Between Bridges and Switches	478
Lab 2.4 Understanding Wireless Parameters and Terminology	481
<b>LAB MANUAL CHAPTER 3</b>	
<b>TCP/IP</b>	<b>485</b>
Lab 3.1 Determine IP and MAC Header Information in an ARP Request and ARP Reply	486
Lab 3.2 Determine IP and MAC Header Information in an RARP Request	488
Lab 3.3 Determine IP and MAC Header Information for a Data Packet	489
<b>LAB MANUAL CHAPTER 4</b>	
<b>IP Addressing</b>	<b>493</b>
Lab 4.1 Determine an IP Addressing Scheme for Network 192.3.2.0	494
Lab 4.2 Decode the IP Address 172.16.31.255 /20	496
Lab 4.3 Decode the IP Address 120.15.179.255 /18	499
Lab 4.4 Design an Efficient IP Addressing Scheme for Network 176.10.0.0	500
Lab 4.5 Perform Binary/Decimal/Hexadecimal Conversions	504

<b>LAB MANUAL CHAPTER 5</b>	
<b>Router and IOS Basics</b>	<b>507</b>
Lab 5.1 Connect the Internetwork Lab	508
Lab 5.2 Configure HyperTerminal to Access a Cisco Router	511
Lab 5.3 Use the System Configuration Dialog to Configure a Cisco Router	513
Lab 5.4 Configure Console and Aux Passwords	517
Lab 5.5 Use Help, the Command History, Enhanced Editing Features, and the Show Command	519
<b>LAB MANUAL CHAPTER 6</b>	
<b>Router Startup and Configuration</b>	<b>525</b>
Lab 6.1 Configure IP Addresses and IP Hosts	526
Lab 6.2 Install, Configure, and Use a TFTP Server	531
Lab 6.3 Configure a Message and Interface Description	533
Lab 6.4 Use the CDP, Ping, Trace, and Telnet Commands	535
Lab 6.5 Use Boot System Commands and the Configuration Register	539
Lab 6.6 Investigate the Security Device Manager (SDM) Interface	542
<b>LAB MANUAL CHAPTER 7</b>	
<b>Routing Protocols</b>	<b>545</b>
Lab 7.1 Understand Terms and Concepts Related to Routing	546
Lab 7.2 Configure Static Routes	548
Lab 7.3 Configure RIP	551
<b>LAB MANUAL CHAPTER 8</b>	
<b>Advanced Routing Protocols</b>	<b>555</b>
Lab 8.1 Identify the Characteristics of Various Routing Protocols	556
Lab 8.2 Configure RIPv2	557
Lab 8.3 Configure EIGRP	561
Lab 8.4 Configure OSPF in a Single Area	563
<b>LAB MANUAL CHAPTER 9</b>	
<b>Network Services</b>	<b>569</b>
Lab 9.1 Configure NAT	570
Lab 9.2 Configure DHCP	572
Lab 9.3 Use SDM to Configure NAT, DHCP, and DNS	575
<b>LAB MANUAL CHAPTER 10</b>	
<b>Access Lists</b>	<b>579</b>
Lab 10.1 Create and Apply a Standard IP Access List on the Lab-d Router	580
Lab 10.2 Create and Apply an Extended IP Access List on the Lab-b Router	584
Lab 10.3 Create and Apply a Named Access List on the Lab-c Router	588
<b>LAB MANUAL CHAPTER 11</b>	
<b>PPP and Frame Relay</b>	<b>591</b>
Lab 11.1 Configure PPP with CHAP and PAP	592
Lab 11.2 Set Up a Test Frame Relay Network	595

**xiv Table of Contents**

Lab 11.3 Configure the Lab-c Router to Simulate a Frame Relay Switch	598
Lab 11.4 Configure the Lab-b and Lab-d Routers for Frame Relay	600
 LAB MANUAL CHAPTER 12	
<b>Basic Switching and Switch Configuration</b>	<b>603</b>
Lab 12.1 Configure a Cisco 2950 Switch Using the CLI	604
Lab 12.2 Evaluate Hub Performance	609
Lab 12.3 Evaluate Switch Performance	612
 LAB MANUAL CHAPTER 13	
<b>Advanced Switching Concepts</b>	<b>617</b>
Lab 13.1 Understand Switching and LAN Design Concepts and Terminology	618
Lab 13.2 Configure “Router on a Stick”	620
 LAB MANUAL CHAPTER 14	
<b>Network Security</b>	<b>629</b>
Lab 14.1 Using the SDM Security Audit Wizard	630
Lab 14.2 Configure a Router Firewall Using the SDM	631
Lab 14.3 Creating VPNs with the SDM	634
INDEX	637

# Preface

## The undisputed worldwide leader in networking equipment, Cisco

manufactures routers, switches, access servers, and network management software designed to interconnect LANs and WANs around the globe. The proliferation of networks in the workplace and the popularity of the Internet have contributed to an increasing need for networking professionals with both LAN and WAN configuration skills. Employers are looking for qualified people to fill the demand for these networking jobs, and certification is a great way to prove you have what it takes. The primary objective of this book is to help you prepare for and pass the Cisco Certified Network Associate Exam (CCNA). This certification (Exam 640-802), is the foundation certification upon which other Cisco certifications are built. It validates the ability to install, configure, operate, monitor, and troubleshoot routed and switched Cisco networks. The CCNA certification can also be obtained by taking two exams rather than one (640-822 then 640-816). Passage of the exam 640-822 earns the Cisco Certified Entry Network Technician (CCENT) certification. This relatively new certification provides recognition of certain networking knowledge and router configuration skills at a slightly lower level than the CCNA designation. This book can be used to prepare for any of the three exams listed above.

Hands-on learning is the best way to master the networking skills necessary for both the CCENT and CCNA certifications and a career in wide-area networking. This book contains more than 50 hands-on exercises that apply networking concepts, such as IP addressing, routing, and switching, as they would be applied on Cisco equipment in the real world and on CCENT and CCNA exams. In addition, each chapter offers multiple review questions and case projects to reinforce mastery of the CCNA topics.

The inclusion of the lab manual at the end of this text provides a substantial and effective learning experience. In addition, the appendices provide crucial test-taking information such as a list of essential commands, as well as troubleshooting techniques and references.

This book is suitable for use in any Cisco CCNA course. As a prerequisite, students should have basic networking knowledge, such as the skills learned in an introductory networking course.

## Intended Audience

*CCNA Guide to Cisco Networking, Fourth Edition* serves as a comprehensive guide for anyone who wants to obtain a solid background in basic Cisco networking concepts, and is an ideal tool to use to prepare for CCENT/CCNA certification. This book guides you through the basics of networking, configuration, and troubleshooting of Cisco routers and switches. To best understand the material in this book, you should have a background in basic networking concepts and have worked with PC hardware. This book is intended for use in a classroom or an instructor-led training environment with access to Cisco routers and switches. When you finish the book, you should understand and be able to perform all objectives covered on the CCNA Exam #640-802.

## Chapter Descriptions

Here is a summary of the topics covered in each chapter of this book:

**Chapter 1**, “Introducing Networks,” introduces the OSI reference model and identifies why the industry uses this layered approach to networking. It also explores the five steps of data encapsulation, the function of a MAC address, and the difference between connection-oriented and connectionless network service.

In **Chapter 2**, “Network Devices,” you learn all about the different devices used on a network and the advantages and disadvantages of using particular devices. The devices include hubs and repeaters, bridges and switches, wireless access points, brouters and routers, and gateways. Devices are discussed in the context of network segmentation, because it is important to understand which devices segment the network and which do not. You will also be introduced to Ethernet, Fast Ethernet, and Gigabit Ethernet operations.

In **Chapter 3**, “TCP/IP,” you learn about TCP/IP—the language of the Internet. TCP/IP is a suite of many protocols, including ICMP, UDP, TCP, ARP, and RARP. It is important to be able to describe the functions performed by these protocols. You will also learn about the benefits of using ping and trace to troubleshoot IP and how IP packets are transmitted. Finally, you learn the Cisco three-layer hierarchical model used for network design by Cisco professionals.

In **Chapter 4**, “IP Addressing,” you learn the different classes of IP addresses, how to configure and subdivide an IP network, and advanced routing concepts such as CIDR, summarization, and VLSM. You will convert between decimal, binary, and hexadecimal numbering systems. Finally, you learn the differences between IPv4, which is in use now on most networks, and IPv6, which is the future of IP.

In **Chapter 5**, “Router and IOS Basics,” you learn about the components of the router and the basic configuration commands. This includes various configuration modes and prompts, passwords, context-sensitive help, and enhanced editing features. It also includes instructions on how to configure the HyperTerminal program in Windows to access the router, and how to configure the router using the system configuration dialog.

**Chapter 6**, “Router Startup and Configuration,” explains the boot process in a Cisco router and how to manipulate the process. You are introduced to CDP, a proprietary protocol of Cisco, which is enabled by default on all Cisco routers and switches. In addition, configuration of IP on the router is discussed. This chapter also details troubleshooting connection problems using show commands, ping, trace, and telnet. Finally, you are introduced to Cisco’s new Security Device Manager, which is a web-based tool for configuring Cisco routers.

In **Chapter 7**, “Routing Protocols,” you learn to differentiate among routable, non-routable, and routing protocols. Routing protocols are categorized as either Exterior Gateway Protocols or Interior Gateway Protocols. The focus of this chapter is Interior Gateway Protocols and the two categories therein, which include distance-vector and link-state. You learn about the count-to-infinity problem with distance-vector routing protocols, along with different ways to combat this problem. This chapter also details how to configure the most popular distance-vector routing protocol-RIP. Finally, you learn how to configure static routing and default routes.

**Chapter 8**, “Advanced Routing Protocols,” introduces several advanced routing concepts on the 640-802 exam. Classful and classless routing are described in detail. The chapter introduces RIPv2, Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF). Controlling routing traffic is also covered.

**Chapter 9**, “Network Services,” discusses the various services used on a network and explains how to use a Cisco router to implement these services. Included in the discussion is Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), and Domain Name Service (DNS). You learn how to configure these services using both the command line interface as well as the new Security Device Manager.

**Chapter 10**, “Access Lists,” covers the dual purpose of access lists, which are flow control and security. You learn the syntax of the two types of lists found on the CCNA exam. These include standard IP and extended IP lists. You learn the usage and rules of access lists and how to configure and apply them. You also learn how to control access to the VTY line with access lists and how to monitor your lists on the router. Finally, you learn how to create named access lists and how to use the Security Device Manager to create access lists, as well as a firewall.

In **Chapter 11**, “PPP and Frame Relay,” you learn about PPP encapsulation and how to configure PPP and its options on a Cisco router. You also learn about PPP multilink and how to enable it. In addition to PPP configuration, you also learn about Frame Relay standards and equipment, and about the role of virtual circuits and performance parameters in Frame Relay. This chapter covers the various Frame Relay topologies and explains how to configure and monitor Frame Relay on Cisco routers.

**Chapter 12**, “Basic Switching and Switch Configuration,” covers the features and benefits of Fast Ethernet, as well as the guidelines and distance limitations governing its use. In addition, it discusses network segmentation and introduces basic traffic management concepts. In this chapter, you also study basic concepts relating to Cisco switches and learn how to operate them. Finally, you learn how to perform and verify switch configuration tasks, and how to implement basic switch security.

In **Chapter 13**, “Advanced Switching Concepts,” you gain experience with the Spanning Tree Protocol and learn about its benefits. You also learn about the usefulness of virtual LANS and practice configuring a VLAN. Finally, you study the VLAN trunking protocol (VTP) and learn how to configure it.

**Chapter 14**, “Network Security,” explains the distinction between the various types of network threats and discusses ways to mitigate these threats. In this chapter, you also learn how to implement SSH on Cisco routers and switches. Finally, you practice configuring a VPN using the Cisco Security Device manager.

**Appendix A**, “CCNA Certification Objectives,” lists each CCNA certification objective and the chapter in which it is covered.

**Appendix B**, “Additional Resources,” provides additional sources of information on subjects covered in this course.

**Appendix C**, “A Networking Professional’s Toolkit,” provides pictures of networking tools, along with their proper names and uses.

**Appendix D**, “Command Summary,” provides a list of the commands presented in this course. You should review these commands before you attempt the CCNA certification examination.

**Appendix E**, “Troubleshooting Summary,” provides a list of commonly used troubleshooting commands and a description of their output. You should review these commands before you attempt the CCNA certification examination.

The **Lab Manual** chapters map to the main text chapters and provide necessary hands-on skills for working with networking equipment in general, and for configuring Cisco routers and switches. The Cisco CCNA certification Exam #640-802, as well as the two other exams leading to the CCNA (640-822 and 640-816), includes simulation questions that mirror actual router and switch configuration. Configuration of the routers and switches in the lab is essential to performing successfully on these exams. Even students who are not interested in becoming a CCNA still need to master the equipment if they will configure it on the job. In addition, working with the networking equipment enhances students’ understanding of the material presented in their lectures. Finally, students work on the labs in teams. They help each other and learn from each other’s successes and mistakes.

---

## Book Features

To aid you in fully understanding Cisco networking concepts, this book includes many features designed to enhance your learning experience:

- **Chapter Objectives**—Each chapter begins with a detailed list of the concepts to be mastered. This list gives you a quick reference to the chapter’s contents, and is a useful study aid.
- **Chapter Summary**—Each chapter’s text is followed by a bulleted summary of the concepts introduced in that chapter. These summaries provide a helpful way to revisit the major ideas covered in each chapter.
- **Key Terms**—All the terms within the chapter that were introduced with boldfaced text are collected in the Key Terms list at the end of the chapter. This list helps you check your understanding of all major terms.
- **Review Questions**—The end-of-chapter assessment begins with a set of review questions that reinforce the ideas introduced in each chapter. Answering these questions ensures that you have mastered the important concepts. The review questions can also be used to help prepare for the CCNA exam.
- **Case Projects**—At the end of each chapter, there are several Case Projects. In these extensive examples, you implement the skills and knowledge gained in the chapter through real design and implementation scenarios.

---

## Lab Manual Features

To ensure a successful experience for instructors and students alike, this book includes the following sections for each lab:

- **Lab Objectives**—Every lab has a brief description and list of learning objectives.
- **Materials Required**—Every lab includes information on hardware, software, and other materials you need to complete the lab.
- **Estimated Completion Time**—Every lab has an estimated completion time, so that you can plan your activities accurately.

- **Activity**—The actual lab activity is presented in this section. Logical and precise step-by-step instructions guide you through the lab.
- **Certification Objectives**—Each chapter lists the relevant objectives from Cisco’s CCNA Exam #640-802.
- **Review Questions**—Every lab provides follow-up questions to help reinforce concepts presented in the lab.

---

## Text and Graphic Conventions

Additional information and exercises have been added to this book to help you better understand what is being discussed. Icons throughout the text alert you to these additional materials. The icons used in this book are described below.



Notes present additional helpful material related to the subject being discussed.

**NOTE**



Tips offer extra information on resources, how to attack problems, and time-saving shortcuts.

**TIP**



Case Projects are more involved, scenario-based assignments. In these extensive case project examples, you are asked to independently apply what you have learned in the chapter.

**CASE PROJECTS**

---

## Instructor’s Materials

The following supplemental materials are available when this book is used in a classroom setting. All of the supplements available with this book are provided to the instructor on a single CD-ROM (ISBN: 1423925750).

**Electronic Instructor’s Manual**—The Instructor’s Manual that accompanies this textbook includes additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.

**Solutions**—This supplement provides answers to all end-of-chapter materials, including Review Questions, Case Projects, and the Activity projects in the Lab Manual.

**ExamView®**—This textbook is accompanied by ExamView, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView includes hundreds of questions that correspond to the topics covered in this text, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers, and they save the instructor time by grading each exam automatically.

**PowerPoint Presentations**—This book comes with Microsoft PowerPoint slides for each chapter. They can be used as a teaching aid for classroom presentation, can be made available to students on the network for chapter review, or can be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics that you introduce to the class.

**Figure Files**—All of the figures in the book are reproduced on the Instructor Resources CD, in bitmap format. Similar to the PowerPoint presentations, these can be used as a teaching aid for classroom presentation, can be made available to students for review, or can be printed for classroom distribution.

---

## Test Prep Software

Two kinds of exam preparation software are included on the CD-ROM at the back of this book:

**CoursePrep** software from MeasureUp provides hundreds of sample exam questions that mirror the look and feel of the CCNA 640-802 exam. For more information about MeasureUp test prep products, or to order the complete version of this software, visit their Web site at [www.measureup.com](http://www.measureup.com).

**CertBlaster** software from dti Publishing Corp. also offers hundreds of sample exam questions in a variety of testing modes: Study, Certification, Assessment, Flash Drill, and Adaptive. For more information about CertBlaster and other dti Publishing products, visit their Web site at [www.certblaster.com](http://www.certblaster.com). The unlock code for the CertBlaster questions is: c\_ccna (case sensitive).

---

## Acknowledgments

Many talented people participated in the creation of this book. The Development team thanks Jessica McNavich, Content Project Manager at Cengage Learning, and Rajni Pisharody of International Typesetting and Composition, for their attention to detail. Also, many thanks to John Bosco and his excellent team of technical editors at Green Pen Quality Assurance. A special thanks to our reviewers, Bill Beatty, Brian Goodman, Joseph Hart, and Cynthia Wright for their dedication to the project, and for their very helpful feedback.

### Kelly Caudle

First, as I try to do with each project, I want to thank the Lord for blessing me each and every day. I must also thank my editors at Course Technology for their patience and for their hard work. Furthermore, I want to thank Kelly Cannon for all her hard work during this project; without Cannonball, the book would not be nearly as error-free as it is. A special thanks also goes to my colleagues at Stanly Community College, who put up with me during my “book” sessions. I want to especially thank Mike Hogan for helping me out of jams more than once. Last, I thank my wonderful wife Susan for her love, support, and encouragement.

### Kelly Cannon

I thank Course Technology for the opportunity to be involved in the world of academic publishing. I also thank my writing partner Kelly Caudle for working with me on this project.

Although we were always miles apart, whenever we communicated, we were in agreement. I would also like to thank Anthony Chiarella for stepping in and picking up the slack. In addition, I am grateful to Ann Shaffer and Michelle Ruelos Cannistraci for all of their hard work. They are both great at what they do, and I hope to work with them again in the near future. Of course, I want to thank my wonderful family, Jim, Veronica, and Adrienne, and my parents, who had the foresight to bring me to the greatest country in the world, where I continue to be blessed with opportunities.

### **Anthony Chiarella**

I would like to thank my wife, Nicole, and my two children who put up with me whenever I embark on a new journey. I would also like to thank Michelle Ruelos Cannistraci for bringing me into this project. I am thankful for the support I received from our development editor, Ann Shaffer. It was paramount in my ability to stay on track and keep the project moving. Finally, I'd like to thank Kelly Cannon and Kelly Caudle for their efforts in this project.

---

## **Hardware Requirements**

The following is a list of hardware required to complete all the labs in the book. Many of the individual labs do not have all of these requirements. In terms of routers and switches, if you have a Cisco Academy CCNA lab setup, you have the necessary equipment for the routing and switching labs in Chapter 5 through the end of the book. The hardware required for Chapters 1 through 4 is minimal. The routing and switching lab setup, in addition to any other hardware required, is as follows:

- Four 2600 series routers with power cables (could substitute a different series but must have two serial interfaces and one Fast Ethernet interface)
- One 2600 series router with power cable (could substitute a different series but must have two serial interfaces and two Fast Ethernet interfaces)
- Two Cisco series 2950 switches (or other appropriate series switch) with power cord
- Five hubs with power cables (can substitute switches)
- Three V.35 DTE cables (male) with serial end to match serial interface on routers
- Three V.35 DCE cables (female) with serial end to match serial interface on routers
- Rollover cables for the routers and switches
- Five RJ-45 to DB-9 connectors (do not need these if rollover cables have a DB-9 end)
- Six computers running Microsoft Windows Vista or XP2, with NICs installed
- HyperTerminal installed on all Windows computers
- One Windows Internet computer with a NIC configured and the TCP/IP protocol configured
- Transceivers for the router Ethernet ports, if these ports use an AUI connection instead of RJ-45
- TFTP server software on a CD or USB drive (preferably Cisco's, which is TFTPSERV.EXE)
- Power strips

- Nineteen UTP patch cables
- One CSU/DSU (can substitute a router if necessary, and it does not have to work; it is for simulation purposes only, and is only used in Lab 2.1)
- One bridge (does not have to work; it is for simulation purposes only, and is only used in Lab 2.1)
- Transceivers for the bridge connections if the bridge uses AUI connections instead of RJ-45 (only used in Lab 2.1)
- Three hubs (do not have to work; they are for simulation purposes only, and are only used in Lab 2.1)
- Nine NICs with RJ-45 transceivers to simulate nine host computers (do not have to work; they are for simulation purposes only, and are only used in Lab 2.1)
- One serial cable with a compatible connector for a serial interface on a router on one end and a V.35 connector on the other end to attach to the CSU/DSU. If another router will be used instead of the CSU/DSU, the cable connector should match the serial interface on the additional router (does not have to work; it is for simulation purposes only, and is only used in Lab 2.1)

1

chapter

# Introducing Networks

**After reading this chapter and completing the exercises, you will be able to:**

- Identify and describe the functions of each of the seven layers of the OSI reference model
- Identify the reasons why the networking industry uses a layered model
- Define and explain the conversion steps of data encapsulation
- Define and describe the function of a MAC address
- Describe connection-oriented network service and connectionless network service, and identify the key differences between them

**This chapter introduces the fundamentals of computer networking. You**

will learn about the reasons for networking, some networking terminology, and a bit about the different types of networks. Specifically, you will learn about networking standards and types of networking equipment. Throughout this book, you will periodically revisit these concepts, learning about them in more detail.

---

## Introduction to Networking

The term computer network, or simply **network**, refers to the connection of two or more computers by some type of medium. For example, a computer connected to the Internet over the public telephone system is part of a network. Two computers connected by a wire cable also form a network. In addition to wire cables, you can use **fiber-optic cable**, **infrared**, and **radio equipment** to create and maintain a connection between two or more systems, thereby forming a network.

### Origin of Networking

Industry experts find it difficult to date the precise origin of networking, because many devices have been networked throughout history. For example, in the 1930s, electrical engineers used a device called the Network Analyzer for simulating electrical power grids. In the early days of computing, mainframe computers were sometimes connected to each other by cables. This type of network allowed mainframes to share computing power.

Today, systems that are part of a network do not have to be identical. A modern network can include a wide variety of computers, peripheral components, and even other networks. As a matter of fact, the largest computer network in the world, the Internet, connects a huge number of computer systems. Mainframes, IBM and IBM-compatible personal computers (PCs), and Macintosh, UNIX, and NetWare systems are all part of the Internet. Televisions, vending machines, and light switches are also part of computer networks today because creative electrical engineers have developed methods to add network interfaces to these devices.

### Why Do We Use Networks?

Some people might use the words “efficiency” or “necessity” in answering the question “Why do we use networks?” Realistically, the question could be answered in one word: convenience. As people have grown more dependent on technology, their need for networked devices has increased.

People expect interoperability from electronic devices. For instance, every person who has a videocassette recorder (VCR) expects it to work with a television set. When connected, the two devices are essentially networked to provide the user with the ability to watch television, play movies, and record television programs. Many people integrate their televisions and VCRs with their home stereos to form a larger networked system. In many ways, a computer network is no more complex than a home entertainment system.

Computer networks allow for the transfer of files, data, and even shared applications without copying anything to floppy disk. In addition, networks allow computers to share items such as printers, scanners, fax machines, processors, disk drives, and other resources.

Networked computers can share data and peripherals. Without a network, people have to find other methods for transferring data between computers. These methods include copying the data to a flash drive or another type of storage medium, and physically moving that data to another system—a method called “sneakernet,” because shoes provide the transport medium between computers.

## Networking Terminology

New terminology for networking and networking components emerges almost daily. Therefore, the creation of a complete and up-to-date list of networking terminology would be impossible. In this section, you will learn the most widely used networking terminology.

1

**Media** The term **media** refers to the wire cabling, such as coaxial or the more commonly used twisted-pair, that form the connections in most networks. Some networks employ fiber-optic cable. While it is more expensive than wire cabling, it is less susceptible to **electromagnetic interference (EMI)**, which is frequently caused by nearby motors or fluorescent lighting. Other networks use **wireless** transmission media, such as infrared or radio signals. With wireless communication, a connection is made between the devices sending and receiving the signals, with air, rather than cable, used to host the communication.

**Client/Server Networks** Client/server networks have computers that are servers and computers that act as clients to those servers. In a client/server network, the **servers** host the resources for the clients to use and provide security, while a **client** is the computer that requests resources from the server. The term **client** sometimes also refers to a human user. For example, a server might have a printer, or resource, attached to it for clients to use. You may see a variety of servers on a network:

- *Print server*—Hosts the connection to a printer so that clients can send print jobs to the printer
- *File server*—Maintains storage space for data that is shared with clients
- *Database server*—Hosts a database that clients can use to read/write and share information in an organized system with other clients
- *Remote access server (RAS)*—Allows clients to dial in, usually over the public telephone system, to establish connections and to access network resources from a remote location
- *Web server*—Provides content on the Internet for clients to connect to when “browsing” the Internet

**Peer-to-Peer** When every computer on a network acts as both a client and a server, the network is a peer-to-peer network. In a **peer-to-peer network**, all computers can share resources, such as files, printers, and applications, with other computers. Peer-to-peer networks are also known as “**workgroups**” because all computers are on the same level and can share resources with other computers. A peer-to-peer network has no dedicated server.

**LAN, WAN, MAN, SAN** Depending on the size of the network, you can use different terms to describe it. For example, a **local area network (LAN)** is contained within a company or department and located in a single geographic area, usually a building or part of a building. A **wide area network (WAN)** spans multiple geographic areas and is usually connected by common telecommunication carriers. The term **metropolitan area network (MAN)** refers to the intermediate stage between a LAN and a WAN; a MAN network is confined within the boundaries of a city, campus, or town and is larger than a LAN. In actual practice, the term is used infrequently. The term **storage area network (SAN)** is relatively new; it refers to a series of storage devices, such as tapes, hard drives, and CDs, that are networked together to provide very fast data storage for a network or subnetwork. The devices on a SAN are physically separate from the servers. This makes the network more scalable and flexible,

because any server can exchange data with any storage device, and additional storage devices can be added more quickly and simply.

**Network Operating System** A **network operating system** (NOS) allows communication, security, and distribution of data, files, and applications over a network. In the early days of PC computing, most PCs could not communicate on a network with other computers. This gave rise to two distinct terms: the stand-alone operating system (OS), which could not communicate on a network, and the networking OS, whose main purpose is network communications. Almost all computers today are networked in some way. Most business servers are running a NOS such as Microsoft Server 2003, Linux, MAC OS X, or Novell NetWare. The clients are typically running Windows XP or Vista or MAC.



Network administrators sometimes call the device or computer at which a user works an **end system**.

**NOTE**

**NIC** A **network interface card** (NIC) is a device that allows a computer or other device to connect to a network through the media. This device is also known as a network adapter, network card, or network interface. The NIC is a physical component that connects to the internal hardware of the computer system. The NIC allows a physical connection to the network media.

**Networking Hardware** **Networking hardware** is a generic term that describes all the physical components of a network, such as the NIC, cable, hub, switch, router, and any related connectors or devices. Any device or physical component that is used to connect computers in a network is considered to be network hardware.

**Networking Software** The programs used to run a network are known as **networking software**. They include the NOS(s) and all client/server networking software programs, such as shared applications like e-mail and database applications.

**Virtual Private Networks** A **virtual private network** (VPN) is a network that uses a public communications infrastructure (like the Internet) to facilitate private communication between a company LAN and remote employees. Remote employees work from home or are located somewhere other than their workplace. Although they require extra security measures, VPNs provide a relatively inexpensive way to connect remote and mobile users with the company's private network. Very often, businesses want to provide some limited access to their communications infrastructure to nonemployees. This may include business partners, suppliers, vendors, and others who deal with the company but are not employees. The part of the company's network that allows access to these nonemployees is called the **extranet**, which is accessed over or through the Internet. Conversely, the part of the company's network that allows access to employees is called the **intranet**, which is completely separate from the Internet. Virtual private networks can be intranet VPNs or extranet VPNs. Alternatives to VPNs include owned or leased lines, which are much more expensive.

## Understanding the OSI Model

As computer networks became popular in the early 1980s, many different networking implementations were created. In the years following, compatibility and communication problems among these different network implementations became pervasive. The wide variety of hardware and software made communication between heterogeneous systems nearly impossible.

In 1984, the International Organization for Standardization (ISO) presented the Open Systems Interconnection (OSI) model. In developing the OSI model, ISO examined existing protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP), Systems Network Architecture (SNA) from IBM, and Digital Equipment Corporation's proprietary networking model (DECNET). Based on their examination of existing protocols, ISO recommended a seven-layer network model called the OSI model.

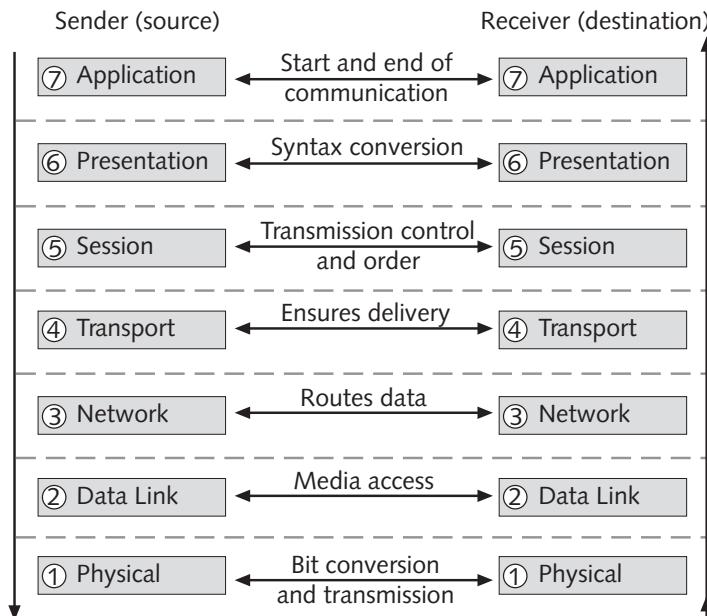
Most networking vendors agreed to support the OSI model in one form or another. The model allows vendors to implement networks that permit communication among the wide variety of network implementations. The OSI model is not an absolute standard for computer networks; it is used as a reference model for how networks should be built. Because it is a reference model, it makes an ideal tool for learning how networks function.

## Reasons for Layering

As previously mentioned, the OSI model has seven layers. A layered networking model is advantageous because it:

- Simplifies the networking model by dividing it into a finite number of components, which makes it easier to comprehend and use
- Enables programmers to specialize in a particular level or layer of the networking model
- Provides design modularity, which allows upgrades to a specific layer to remain separate from the other layers
- Encourages interoperability by promoting balance between different networking models
- Allows networking vendors to produce standardized interfaces

Figure 1-1 shows the layers of the OSI model: Physical layer, Data Link layer, Network layer, Transport layer, Session layer, Presentation layer, and Application layer. In the figure,



**Figure 1-1** OSI reference model

**6** Chapter 1 Introducing Networks

the number beside each layer represents the number associated with it. For instance, the Network layer is commonly referred to as layer 3.

As a group, these layers form the OSI protocol stack. A **protocol** is a defined method for communicating between systems. Computers must use a common protocol to communicate properly. Many different protocols are available for use on networks today; two examples are TCP/IP and IPX/SPX. You can think of a protocol as a common language between two computers. Just as humans must speak a common language to communicate, computers must use a common protocol. The TCP/IP protocol (which is really a group of protocols) is the language of the Internet.

As shown in Figure 1-1, communications begin at the Application layer (layer 7) when the sender initiates a network transmission. The data travels down the OSI stack to the Physical layer (layer 1) and out to the physical layer of the receiving device. If this receiving device is the final destination, the data travels up the OSI stack until it reaches the Application layer and becomes available to the user.



For an easy way to remember the seven layers, from layer 7 to layer 1, use the following saying: All People Seem To Need Data Processing (Application, Presentation, Session, Transport, Network, Data Link, Physical). To remember layer 1 to layer 7, use Please Do Not Throw Sausage Pizza Away (Physical, Data Link, Network, Transport, Session, Presentation, Application).

## Peer OSI Communication

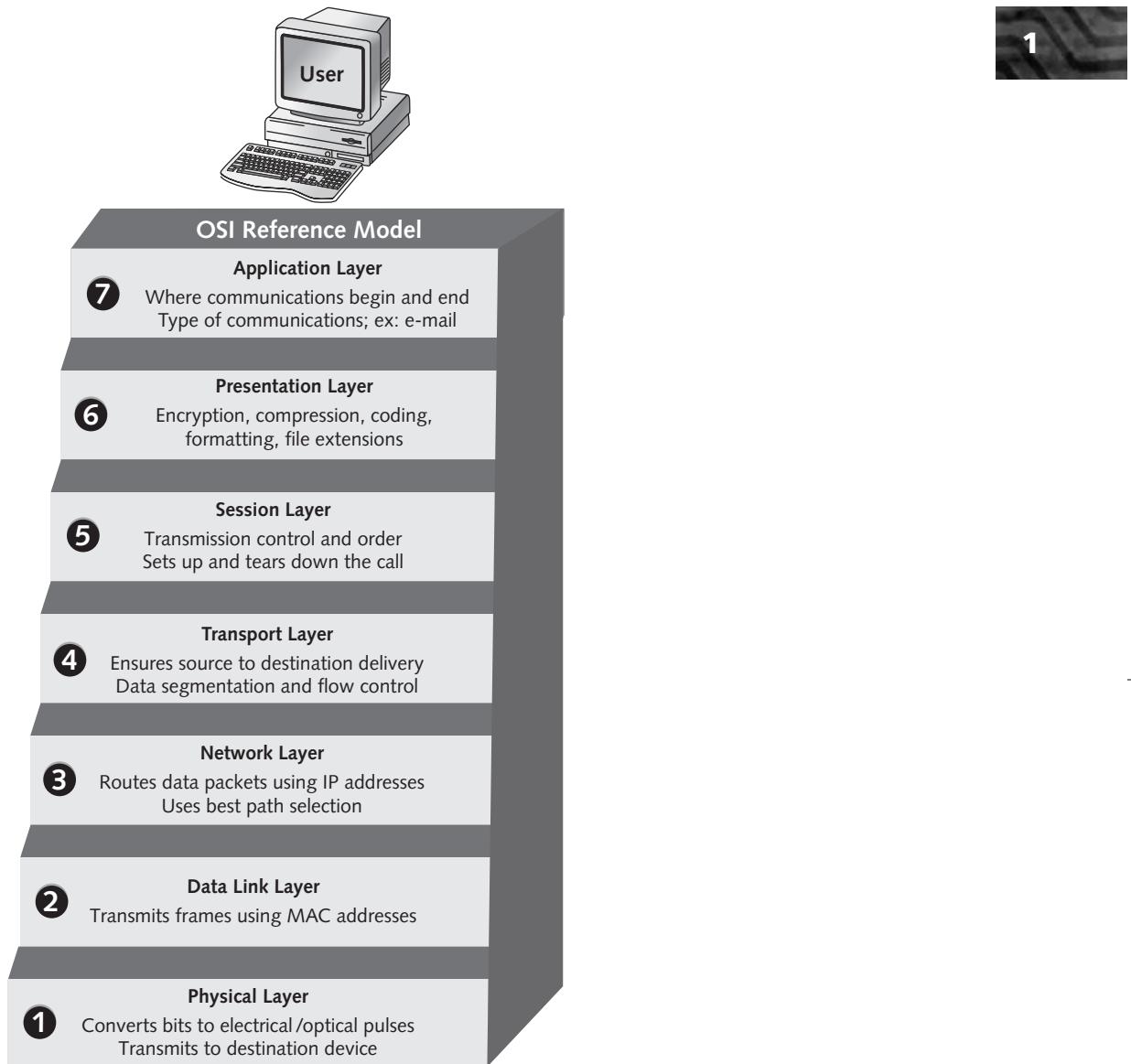
The seven layers of the OSI reference model communicate with one another via **peer communication**. In other words, each layer will only talk to its peer on the opposite side of the communications process. As a result, each layer is unaware of the activities of all other layers of the model. Figure 1-1 indicates peer communication, where the layers on the source node only talk with the opposite and equivalent layers on the destination node.

Peer communication allows error checking to occur on two separate layers simultaneously. Even if the Transport layer is already providing reliable transmission of data, the Data Link layer is unaware of what goes on above it and will provide Data Link error control in the form of the cyclic redundancy check (CRC).

Each layer does provide services to the layer above it and receives services from the layer below it, but the layers do not acknowledge these services in any way. Instead, each layer concentrates only on its specific function in the overall communications process. As a result, each layer of the OSI model takes information from the layer above, encapsulates that information into specific formats, and passes the information to the layer below.

## Layer Functions

The OSI model was developed as an industry standard for companies to use when developing network hardware and software to ensure complete compatibility. As previously stated, each layer in the OSI model performs a specific function in the transmission process. Although most modern networks do not implement the OSI model exactly as it is defined, the model remains an excellent reference and learning tool. Consequently, the functions of each OSI model layer are defined in the following sections. Figure 1-2 summarizes these functions.



**Figure 1-2** Layer Functions



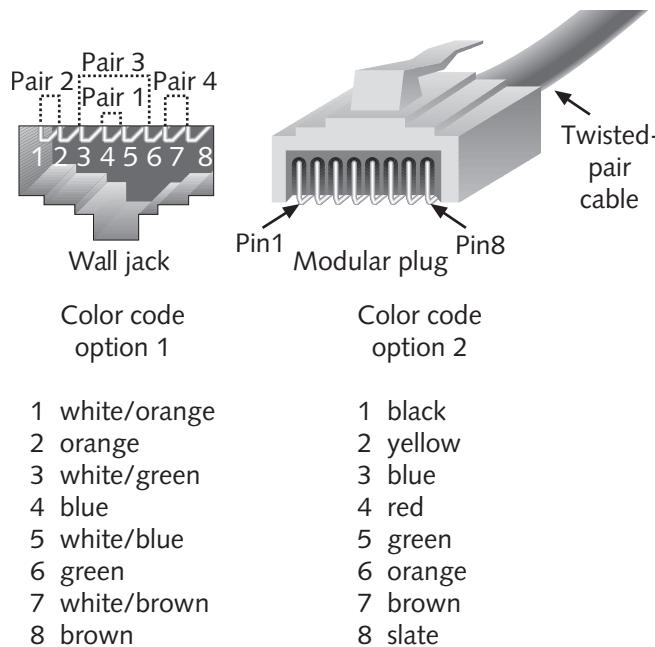
Although the OSI model distinguishes seven layers in the communication process, most real-world implementations of protocol stacks do not use seven distinct layers. For example, TCP/IP uses a four-layer approach, while IPX/SPX loosely maps to the OSI model. Still, as mentioned earlier, the model is useful to help conceptualize the network communication process.

**Physical (Layer 1)** Layer 1 in the OSI model is the Physical layer. It has the following responsibilities:

- Definition of the physical characteristics of the network hardware, including cable and connectors
- Representation of binary digits as voltages (encoding)
- Transmission of signals on the wire

The Physical layer defines the mechanical, electrical, and procedural events that occur during the physical transmission of electronic signals on the wire. In essence, the Physical layer's task is to transmit the actual signals on the network. This layer defines the physical characteristics of the transmission media (cabling/wire, radio waves, infrared, fiber/glass, etc.), the network card, and other physical items such as hubs, repeaters, transceivers, connectors, and wall jacks.

As an example of a Physical layer definition, consider the Electronic Industries Association/Telecommunications Industry Association (EIA/TIA) 568B specification. The 568B specification defines a wiring system for data-grade cable, as shown in Figure 1-3.



**Figure 1-3** 568B twisted-pair wiring scheme

Because a computer stores information in binary form (as a one or a zero digit), the Physical layer must convert that information into a signal for physical transmission. The network card at the Physical layer converts the data into electrical, radio, or light signals and transmits the signal on the network media. At a set measurement interval, the receiving NIC detects the presence of a signal as a binary one (1) and its absence as a binary zero (0). Signals are sent by the source and received by the destination at a common interval so that the code (signal on/signal off) is interpreted correctly at the destination.

The physical devices must follow some type of standard when encoding and decoding these binary digits into and from electrical signals. The encoding method defines specific measurement intervals that are to be used when interpreting signals as binary digits.

Connectors, cables, and devices such as **repeaters** (devices that boost the signal) and hubs (multiport repeaters) are all Physical layer items. In the process of choosing cable, network administrators often consider the following criteria:

- Expense
- Physical location
- Distance
- Security requirements
- Transmission speed required

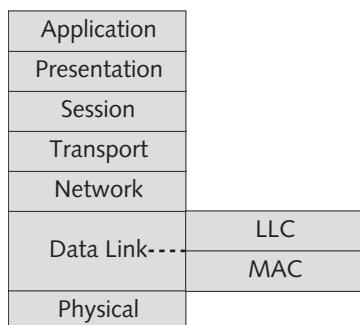
Network devices and networking media will be discussed in greater detail later in this book.

**Data Link (Layer 2)** The layer just above the Physical layer on the OSI protocol stack is the Data Link layer. This layer has several responsibilities:

- NIC software functions, including the identification of the source and destination nodes via their physical addresses (Media Access Control addresses)
- Definition of how data is packaged for transport in smaller units known as **frames**
- Error notification

In the Data Link layer, the information to be transmitted receives its final formatting. The data is prepared for transmission, and a Cyclic Redundancy Check (CRC) is added. The CRC is information that is used to determine whether data was corrupted during transmission. Once assembled, the data is placed in a frame.

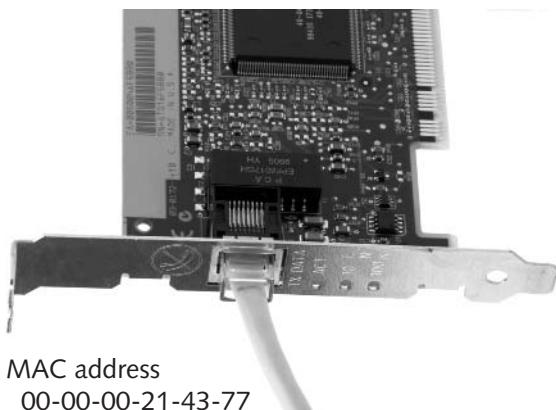
The Data Link layer has two sublayers that further articulate its functions: the **Logical Link Control (LLC)** layer and the **Media Access Control (MAC)** layer. The **Institute of Electrical and Electronics Engineers (IEEE)** created these sublayers to identify and isolate the separate responsibilities required at this level of the protocol stack. The LLC sublayer defines how data is packaged for the network. The LLC function is significant because it allows data frames to be packaged differently for different types of networks. Essentially, the LLC is the portion of the Data Link layer that provides the linking function between the Physical layer and the higher layers. Figure 1-4 shows the OSI layers, including the two sublayers.



**Figure 1-4** Data Link layer subdivision

## 10 Chapter 1 Introducing Networks

The MAC sublayer defines the media access method and provides a unique identifier for the network card. The identifier, called a MAC address, is a 48-bit address represented as a 12-digit hexadecimal number given to each network card during production, as shown in Figure 1-5. Every network interface card on your network must have a unique MAC address. This **physical address** provides a way to distinguish one computer from another on the network.



**Figure 1-5** Network adapter

(Image © Timothy Geiss, 2008. Used under license from Shutterstock.com.)

When manufacturers produce network cards, they burn the MAC address into the circuitry of the NIC. The IEEE assigns the first six hexadecimal digits of a MAC address to NIC manufacturers. Thus each manufacturer has its own six-digit identifier, sometimes called the Organizational Unit Identifier (OUI) or block ID. Large companies such as Cisco and 3Com may have more than one OUI. The last set of six hexadecimal digits is assigned by the vendor itself and is sometimes called the serial number or the device ID. Together, the 12 digits in a MAC address must form a unique number. Note that because the MAC address is added during the manufacturing process, it is a permanent marking. For this reason, the address is also known as a **Burned in Address (BIA)**. The only way to change your computer's BIA is to replace the network card.

Because a computer uses a MAC address to identify itself on the network, the MAC address is an integral component when computers open communication pathways to transmit data on the network. On an **Ethernet** or Carrier Sense Multiple Access with Collision Detection (CSMA/CD) network, when one computer (the source) wants to communicate with another (the destination), the source computer sends the data frame out on the wire. The data frame is then sent to the appropriate portion or segment of the entire network. On that segment, every network interface receives and evaluates the message. When a NIC finds a match between its MAC address and the one listed in the data frame, the frame is copied and passed up the protocol stack. Even when one NIC finds a match, the data frame is still moved along the network until each NIC on the segment has evaluated the frame. When computers send out broadcast messages (messages intended for every machine on a given segment), every computer will accept the frame and pass it up the protocol stack.

Many LANs and WANs contain several segments. Dividing a network into segments enhances performance. If you did not divide a network, every NIC on that network would take the time to receive and evaluate every message, which is costly. When networks are segmented, regular broadcasts and frames meant for the local segment are not passed to other

segments. Because segmentation reduces the amount of frames that each NIC must check and evaluate, it increases network performance.

1

**Network (Layer 3)** Layer 3 in the OSI model is the Network layer. This layer has the following functions:

- Software/logical addressing for data **packets**, such as IP, IPX, and AppleTalk
- Data routing and connectivity
- Best path selection

The Network layer routes data and provides connectivity to remote networks using the most efficient path. The Network layer contains software-addressing information for data packets, which makes network segmentation and routing possible.

The protocols at the Network layer allow computers to route packets to remote networks using a **logical address**. This logical address is used by routers to forward the packet to the correct network. The type of logical address depends on the type of Network layer protocol used. For example, if the network uses the Internet Protocol (IP), an example of a logical address could be the following IP address: 192.168.1.1. Like the MAC address, the logical address must be unique for the computer on the network. Unlike the MAC address, which is permanent, the logical address usually can be assigned and modified by the person in charge of the network.

The Network layer and IP addresses are discussed in greater detail later in this book.

**Transport (Layer 4)** The Transport layer provides host-to-host data transportation, and is concerned with quality of service and reliability. The responsibilities of the Transport layer include the following:

- End-to-end, error-free transmission and delivery between the ultimate sender and ultimate receiver
- Flow control
- Data segmentation into maximum transmission unit (MTU) size
- Messaging service for the Session layer

Protocols that reside at the Transport layer can be connection-oriented or connectionless. **Connection-oriented** protocols, such as TCP, require an acknowledgment (ACK) of the receipt of data packets. If an ACK is not returned for a given packet in a given time, the connection-oriented protocol will retransmit. Conversely, **connectionless** protocols, such as User Datagram Protocol (UDP), do not require an ACK.

Connectionless services are often deemed unreliable because they do not ensure that the data was properly received. Data sent by a connectionless transport is also called a **datagram**. A letter sent through the post office is similar to a datagram. A person who sends regular mail through the post office does not receive an acknowledgment from the post office when the letter is delivered. If the person wants an acknowledgment, he or she has to confirm with the letter recipient. Connection-oriented services are termed reliable because they ensure receipt. Using the post office analogy again, assume that a letter was sent through the post office with a return receipt requested. This type of delivery could be considered reliable because the sender receives notification when the

**12** Chapter 1 Introducing Networks

letter is successfully delivered. The connection-oriented services of the Transport layer help create a “session” between two computers. Computers that share large amounts of data often establish sessions. This is especially true when computers are linked for application-sharing purposes.

The Transport layer protocols negotiate across the link for the highest number of data segments to be sent before an acknowledgement is required. A system that transfers large files over the network will typically negotiate relatively larger MTU sizes. Larger MTU sizes increase network efficiency.

**Session (Layer 5)** The Session layer enables two applications on the network to have an ongoing conversation or dialog. This is especially useful when applications are shared across the network or when computers are joined for game playing. Examples of Session layer protocols include NetBIOS, Structured Query Language (SQL), Remote Procedure Call (RPC), and X-Windows.

The Session layer provides the following services:

- Control for data exchange (full or half duplex)
- Clocking or timing
- Failure recovery
- Initial link setup and link termination when communications complete

The Session layer tells the receiving computer where a transmission begins and ends. When a large amount of data must be passed between two computers, the data most likely is broken into several pieces. The Session layer ensures clear identification of the beginning and end of such a data transfer.

The Session layer allows the transfer of a large set of data across the network. For example, if you want to save a file to a network file server, your computer will attempt to open a session with the network server. Once the session is established, your computer will break the data into tiny packets and send them across the network until all the packets have been received by the server and written to the file server’s disk drive. The Session layer also provides the ability to interrupt and recover the session if there is a need to wait for other data transmissions that are occurring on the local segment. If the line fails momentarily, the Session layer will also attempt to recover the session.

**Presentation (Layer 6)** The Presentation layer prepares the data from the Application layer for transmission over the network. It also reformats data received from the lower layers in the protocol stack for the Application layer. Presentation layer components include file extensions and coding schemes such as BMP, WAV, JPEG, MIDI, HTML, EBCDIC, and ASCII.

The Presentation layer has the following responsibilities:

- Data translation
- Data formatting
- Data syntax restructuring
- Data encryption
- Data compression

The Presentation layer receives data from the Application layer. Because the data can come in several different formats, the Presentation layer must translate the data into a format that all computers on the network can interpret. In some cases, the Presentation layer must restructure the data before it can be sent across the network.

This layer also provides encryption services when data encryption is used in network communications. For outbound communications, the Presentation layer will encrypt data prior to transmission. For inbound data, the Presentation layer decrypts the data before passing it up to the Application layer. The Presentation layer may also compress outbound data or decompress inbound data. Data compression reduces the size of the data that is sent across the network and, in many cases, improves network performance.

After the Presentation layer reformats, compresses, and/or encrypts data, no further restructuring of the data takes place. The lower layers add headers and trailers, but they do not reconfigure the data.

### **Application (Layer 7)** Layer 7 is the Application layer. It has the following responsibilities:

- Initiating the request for network services
- Providing network services to applications such as e-mail and Web browsers

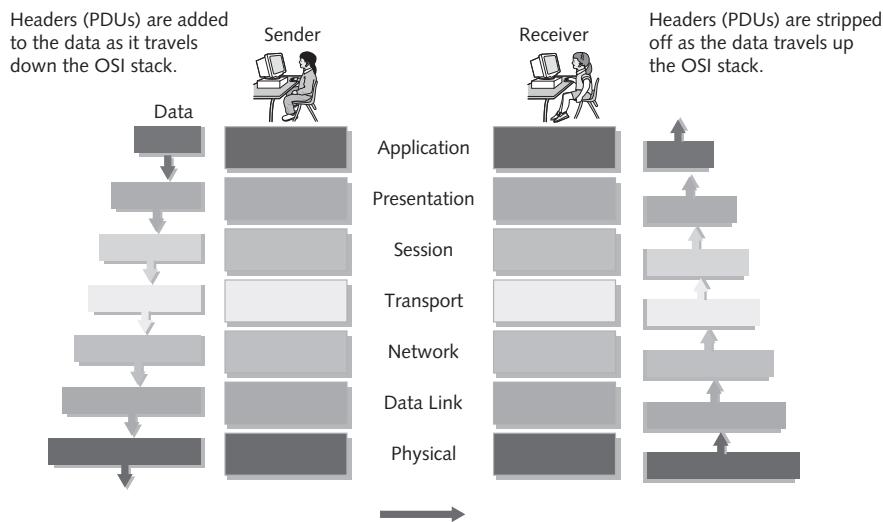
The Application layer is at the very top of the OSI protocol stack. This layer is concerned with user interaction with the computer and the network. In this layer, the user's actions may result in network access and the beginning of communications. The Application layer contains many protocols and utilities, such as telnet, FTP, HTTP, DNS, SMTP, and SNMP, which provide services to the computer applications being used. Note that application programs like Microsoft Word, Eudora Mail, and Netscape are not in the Application layer. Application programs, as well as the users of those programs, are outside the model, above the Application layer. For example, a user may use the Outlook e-mail program. That program is not in the Application layer, but the e-mail protocol SMTP (Simple Mail Transfer Protocol) that supports programs such as Outlook is in the layer. Data from the Application layer is passed directly to the Presentation layer.

**Data Encapsulation** Data is sent from one computer to another in a data packet. The packet contains data from the sending application and more information added by the protocol stack. Prior to transmission across the network, the data packet is organized into a data frame at layer 2.

Each layer in the protocol stack may add a **protocol data unit** (PDU) to the data as it is passed down the layers. A PDU, which is also known as a header or a trailer, is specific information that is sent from one layer on the source computer to the same layer on the destination computer. This type of communication is called peer communication. As the layers pass the data through the stack, the addition of a header and/or trailer is called **encapsulation**. When data is passed down the protocol stack, the header or trailer of the next-lower layer encapsulates it. It is helpful to think of encapsulation as "wrapping."

The data packet is passed over the network from the source computer to the destination computer. It is assembled as it travels down the protocol stack of the source computer and disassembled as it travels up the protocol stack of the destination computer, as shown in Figure 1-6.

## 14 Chapter 1 Introducing Networks

**Figure 1-6** Data encapsulation

As the destination computer unpacks the data packet, the data is checked. Once the data packet is completely disassembled, the original information that was transmitted is delivered to the receiving application. Table 1-1 describes the five steps of data encapsulation.

Step Number	Event	Description
1	Data conversion	When the application generates a message to be sent out on the network, the data is converted into a standard data format. This occurs at OSI layers 5, 6, and 7, which are also known as the "upper layers."
2	Segmentation header added	The Transport layer segments the data into maximum transmission units (MTUs) to ensure that hosts on both ends can communicate.
3	Packet creation with network header	Data is placed into a data packet or datagram, and a network header with logical addressing information is added. This occurs at layer 3, the Network layer.
4	Frame header and trailer for network link	The data frame is prepared for the type of network protocol that is in use. A frame header (including the source and destination MAC addresses) and trailer are added at the Data Link layer. These MAC addresses effectively wrap the IP addresses that were added at layer 3.
5	Bit transmission	The frame is sent across the wire as bits at the Physical layer; ones and zeros are encoded and transmitted along the physical network as pulses.

**Table 1-1** Five steps of data encapsulation

## Chapter Summary

1

- Two or more computers connected by media form a network. Computers can use a network to share resources such as printers, disk space, and applications.
- Before computers were networked, file transfers were usually conducted by users physically walking copies of data (on floppy disk or other magnetic media) to another computer, a system called “sneakernet.”
- The earliest networks had no standardization, so interoperability between the various proprietary network implementations was rare. The ISO developed the OSI model in the mid-1980s to standardize networking models.
- Data transmission can be connection-oriented or connectionless. Connection-oriented transmission requires that packets be acknowledged as received. Connectionless transmission does not require acknowledgments.
- The OSI networking model has seven layers, which simplify the networking model by dividing it into a finite number of complex components. This layering allows engineers to specialize in specific layers, and the modularity allows them to upgrade components at one layer without affecting other layers. The layered model also encourages interoperability among the various networking vendors by providing them with a standard architecture.
- The Physical layer, the first and lowest layer of the OSI model, handles the physical transmission of data across the network.
- The Data Link layer, the second layer of the OSI model, interacts with the networking hardware by controlling the link and supporting communications with the network interface; this layer also interacts with the MAC address.
- The Network layer, the third layer of the OSI model, supports logical addressing and routing of data packets.
- The Transport layer, the fourth layer, segments data that is to be sent out on the network into MTUs.
- The Session layer, the fifth layer, establishes and maintains connections between computers during data transfers.
- The Presentation layer, the sixth layer, handles data translation, encryption, and formatting for transmission on the network or for interpretation by the Application layer.
- The Application layer, the seventh and highest layer, handles the interface between the network and the user.
- When the network user sends data to the network, it goes through a five-step data encapsulation process. This process takes place as the data packet travels down the OSI protocol stack.

## Key Terms

**ASCII (American Standard Code for Information Interchange)** A standardized method for formatting binary information and text for communications and printer control. The acronym ASCII is pronounced “ask-ee.”

**Application layer** The seventh layer of the OSI model, which is responsible for requesting network services and for providing services to applications.

**16** Chapter 1 Introducing Networks

**BMP** A Windows Bitmap (BMP) file, a graphical image type used with Microsoft Windows applications.

**Burned in Address (BIA)** The MAC address that is permanently added to the network card during the manufacturing process.

**Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** The network access method used by Ethernet networks.

**client** A computer that operates on a network and requests and uses the services of other computers on the network, but does not necessarily provide any services to other computers.

**client/server** A type of networking in which a few dedicated computers, called servers, share files, printers, disk drives, and other resources with a group of client computers.

**connection-oriented** Network communications that require acknowledgment. On the OSI reference model, the decision to use connection-oriented communications is made at the Transport layer.

**connectionless** Network communications that do not require acknowledgment. On the OSI reference model, the decision to use connectionless communications is made at the Transport layer.

**cyclic redundancy check (CRC)** The process that ensures that data was not corrupted during transmission. This is accomplished by comparing CRC calculations before and after transmission.

**Data Link layer** The second layer of the OSI protocol stack, which defines the rules for sending and receiving information across the network media. It encodes and frames data for transmission and provides error detection and control. This layer has two parts: LLC and MAC.

**datagram** A message or packet that is sent across a network and does not require acknowledgment by the destination station.

**electromagnetic interference (EMI)** Electronic noise that disrupts signals on cables. This noise is frequently caused by motors and generators, but can also be caused by sunspots and other natural EMI-producing phenomena.

**encapsulation** A process that occurs during transmission through the protocol stack, in which data from the higher layers is wrapped in a protocol header and/or trailer.

**end system** The location and/or set of controls that the user can manipulate to interact with a computer or a network.

**Ethernet** A standard networking architecture that defines the physical layout, lengths, and types of media that can be used. There are many variations of Ethernet, but most use the CSMA/CD network access method.

**EBCDIC (Extended Binary Coded Decimal Interchange Code)** A standardized formatting method for both binary and text files for communications and printer control. IBM developed EBCDIC. The acronym EBCDIC is pronounced “eb-see-dick.”

**extranet** An area of a company’s network allowing access by nonemployees such as business partners, vendors, and suppliers.

**fiber-optic cable** A type of cable that conducts light signals through glass or plastic to generate network signals. Fiber-optic cable allows for transmission rates of 100 megabits per second or greater. It is impervious to electromagnetic interference because it sends light signals rather than electric signals along the cable.

**frame** A segment of data. The words “frame” and “data packet” are often used interchangeably, although technically a frame is found at layer 2 of the OSI model and a packet is found at layer 3.

**hexadecimal** A numbering method that relies on a base of 16. Hexadecimal digits can be 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, or F.

**infrared** Invisible light at the upper end of the electromagnetic spectrum. It is used in most hand-held remote control devices for televisions, stereos, and videocassette players. It is also used in some types of computer networking, especially for data transfers between laptop and desktop systems.

**Institute of Electrical and Electronics Engineers (IEEE)** A technical professional society that fosters national and international standards. Its Web site is [www.ieee.org](http://www.ieee.org).

**International Organization for Standardization (ISO)** An association that attempts to standardize and define items that increase communication and compatibility in many different industries.

**intranet** The part of a company’s network that is restricted to employee use only.

**local area network (LAN)** A group of computers and other devices typically connected by a cable. A LAN is normally located in a single geographic region such as a building or floor in a building.

**logical address** A network address that can be assigned and modified by the person in charge of the network. This type of address appears at the Network layer of the OSI model.

**Logical Link Control (LLC) layer** A sublayer of the Data Link layer that forms the connection between the other software in the protocol stack and the networking hardware (such as the NIC and the cables).

**media** The cable, glass, or telephone lines that host the signal from one computer to another on a network.

**Media Access Control (MAC) layer** A sublayer of the Data Link layer that defines the hardware address of the physical network interface. In addition, it discards corrupted packets and identifies which packets were directed to the local system.

**metropolitan area network (MAN)** An intermediate specification that defines networks confined to a fairly restricted geographic area, such as a campus, town, or city. These private networks span multiple geographically separate locations that are near one another.

**network** Two or more computers connected by some type of media.

**network interface card (NIC)** A hardware device that transmits and receives electronic signals on a network.

**Network layer** The third layer of the OSI conceptual networking model, which allows communications to be routed on a network. It provides a logical address for computers on a network.

**network operating system (NOS)** Operating software that has networking components built into its structure.

**networking hardware** All the physical components of a network, such as the NIC, cable, hub, switch, router, and any related connectors or devices.

**networking software** The programs used to run a network.

**Open Systems Interconnection (OSI)** A seven-layer reference model created by the International Organization for Standardization (ISO) to define and separate networking hardware and software into distinct layers and functions. This model helps to ensure that the various networking implementations are compatible.

**packet** A group of data that is transmitted across a network.

**peer-to-peer network** A type of network in which the clients can also function as servers.

**peer communication** The method of communication among the levels of the OSI model, in which each protocol in the OSI protocol stack encodes its own protocol data unit into the network hierarchy, so that it can communicate with the equivalent layer on the destination computer.

**physical address** Also called the MAC address. It is burned into the network interface card (NIC) during the manufacturing process.

**Physical layer** The first layer of the OSI conceptual networking model, which defines the physical media and electronic transmission methods used in networking.

**Presentation layer** The sixth layer of the OSI network model, responsible for data formatting and encryption.

**protocol** A definition of rules for communication between two or more computers. Computers must have a common protocol (or a translator) in order to communicate.

**protocol data unit (PDU)** Information added to a data packet by the layers of the protocol stack. It can be header or trailer information that is attached to the data packet prior to transmission.

**Remote Procedure Call (RPC)** A method used to establish communications between computer systems at the Session layer.

**repeater** A device that repeats or boosts a network signal along network wire. It reduces signal degradation and increases the maximum usable length of network cable.

**server** A computer that shares resources with other devices on a network.

**Session layer** The fifth layer of the OSI model, which controls the connection between two computers sharing data. It maintains, defines, and recovers connections that are established between two computers.

**storage area network (SAN)** A subsystem of networked storage devices that are physically separate from the servers.

**Structured Query Language (SQL)** A computer language used to query, manipulate, and communicate with databases.

**Transport layer** The fourth layer of the OSI reference model, which segments and reassembles data frames. It also provides for connection-oriented and connectionless communications.

**virtual private network (VPN)** A private communications link over public communications infrastructure, such as the Internet.

**WAV** A Windows Audio file, an audio file format used with Microsoft Windows applications.

**wide area network (WAN)** A network that spans two or more geographically diverse locations and typically uses public telecommunications carriers to connect its individual segments.

**wireless** Communications that are not conducted over physical wires or cables. These communications can include infrared, radio, and other types of transmissions that are sent through the air between two or more locations.

**X-Windows** A standard graphical user interface (GUI) used on UNIX systems.

## Review Questions

1

1. Which of the following best describes the Presentation layer?
  - a. establishes, maintains, and manages sessions between applications
  - b. translates, encrypts, or prepares data from the Application layer for network transmission
  - c. handles routing information for data packets
  - d. provides the electrical and mechanical transmission of data
  - e. handles link control and uses the MAC address on the network interface card (NIC)
2. Which of the following best describes the Network layer?
  - a. handles routing information for data packets
  - b. provides the electrical and mechanical transmission of data
  - c. handles link control and uses the MAC address on the NIC
  - d. establishes, maintains, and manages sessions between applications
  - e. translates, encrypts, or prepares data from the Application layer for network transmission
3. Which of the following best describes the Session layer?
  - a. translates, encrypts, or prepares data from the Application layer for network transmission
  - b. handles routing information for data packets
  - c. provides the electrical and mechanical transmission of data
  - d. handles link control and uses the MAC address on the NIC
  - e. establishes, maintains, and manages sessions between applications
4. Which of the following best describes the Transport layer?
  - a. provides the electrical and mechanical transmission of data
  - b. handles link control and uses the MAC address on the NIC
  - c. establishes, maintains, and manages sessions between applications
  - d. segments and reassembles data and provides either connection-oriented or connectionless communications
  - e. translates, encrypts, or prepares data from the Application layer for network transmission
5. Which of the following best describes the Data Link layer?
  - a. provides the electrical and mechanical transmission of data
  - b. handles link control and uses the MAC address on the NIC
  - c. establishes, maintains, and manages sessions between applications
  - d. translates, encrypts, or prepares data from the Application layer for network transmission
  - e. handles routing information for data packets

**20** Chapter 1 Introducing Networks

6. Which of the following best describes the Physical layer?
  - a. establishes, maintains, and manages sessions between applications
  - b. translates, encrypts, or prepares data from the Application layer for network transmission
  - c. provides the electrical and mechanical transmission of data
  - d. handles link control and uses the MAC address on the NIC
  - e. provides network services to the user
7. Which of the following best describes the Application layer?
  - a. establishes, maintains, and manages sessions between applications
  - b. translates, encrypts, or prepares data for network transmission
  - c. provides network services to the user
  - d. handles routing information for data packets
  - e. provides the electrical and mechanical transmission of data
8. Which of the following accurately describe the Media Access Control (MAC) address? (Choose all that apply.)
  - a. It is a physical number set during the manufacturing process.
  - b. This address is a layer in a network segment.
  - c. MAC addresses contain 12 hexadecimal numbers.
  - d. Computers use this address to uniquely identify themselves on the network.
  - e. An IP address is one example of this type of address.
9. Which of the following accurately describe the network address? (Choose all that apply.)
  - a. It is a physical number set during the manufacturing process.
  - b. This address is used when routing communications between different network segments.
  - c. The Data Link layer uses this address.
  - d. This address is set at layer 3 of the OSI model.
  - e. An example of this type of address is an IP address.
10. Connection-oriented services are also known as \_\_\_\_\_ services.
  - a. reliable
  - b. unreliable
  - c. datagram
11. Connectionless services are also called \_\_\_\_\_ services.
  - a. reliable
  - b. acknowledgment
  - c. unreliable
12. Which of the following describes services that receive an acknowledgment from the destination? (Choose all that apply.)
  - a. datagram
  - b. reliable

- c. connection-oriented
  - d. connectionless
  - e. unreliable
13. Place the following steps of data encapsulation in their correct descending order:
- a. frame headers and trailers added
  - b. segment header added
  - c. bit transmission
  - d. packet creation and network header
  - e. data conversion
14. Which of the following correctly defines a WAN?
- a. a network contained within a single geographic location and usually connected by a privately maintained medium
  - b. a network spread over multiple geographic areas and usually connected by publicly and privately maintained media
  - c. a network spread over a single metropolitan area
15. Which of the following best describes a LAN?
- a. a network that is contained in a single geographic area such as a building or floor in a building
  - b. a countywide network that spans multiple geographic locations
  - c. a large network that is connected by both publicly and privately maintained cabling spread over multiple geographic regions
16. Which of the following reasons for providing a layered OSI architecture are correct? (Choose all that apply.)
- a. to provide design modularity, which allows upgrades to a specific layer to remain separate from the other layers
  - b. to simplify the networking model by dividing it into 14 layers and 12 sublayers
  - c. to discourage interoperability between disparate networking models
  - d. to enable programmers to specialize in a particular layer
  - e. to allow for standardized interfaces from networking vendors
17. On a network, computers must use a common \_\_\_\_\_ in order for communication to occur.
- a. protocol
  - b. operating system
  - c. manufacturer
  - d. hardware platform
18. Before networks, what did people use to transfer files?
- a. sneakernet
  - b. protocols

**22** Chapter 1 Introducing Networks

- c. interface cards
  - d. Ethernet
19. A protocol is to a computer as a(n) \_\_\_\_\_ is to a person.
- a. identity
  - b. personality
  - c. language
  - d. personal philosophy
20. Which of the following are network hardware? (Choose all that apply.)
- a. NIC
  - b. NOS
  - c. LLC
  - d. network media
  - e. connectors
21. Which of the following are network software? (Choose all that apply.)
- a. components that map to the Application layer of the OSI model
  - b. NIC
  - c. NOS
  - d. media connectors
22. All networking vendors follow the OSI model and design seven-layer architectures. True or False?
23. Communications on a network originate at the \_\_\_\_\_.
- a. destination
  - b. breaker
  - c. peak
  - d. source
24. Transmitted signals are bound for a \_\_\_\_\_ computer.
- a. destination
  - b. breaker
  - c. peak
  - d. source
25. Information transmitted on a network is called a(n) \_\_\_\_\_.
- a. package
  - b. expresser
  - c. data destination
  - d. data frame
  - e. E-pack

26. Which of the following are layers of the OSI model? (Choose all that apply.)
- a. OSI
  - b. Physical
  - c. IEEE
  - d. Data Link
27. Which layer of the OSI model is responsible for media access and packaging data into frames?
- a. Network layer
  - b. Physical layer
  - c. Data Link layer
  - d. Transport layer
28. At which layer of the OSI model will encryption and compression occur?
- a. Presentation layer
  - b. Session layer
  - c. Application layer
  - d. Network layer
29. Which of the following lists the layers of the OSI model from layer 7 to layer 1?
- a. Application, Session, Transport, Network, Presentation, Data Link, Physical
  - b. Physical, Data Link, Network, Transport, Session, Presentation, Application
  - c. Application, Presentation, Session, Transport, Network, Data Link, Physical
  - d. Presentation, Application, Session, Network, Transport, Data Link, Physical
30. The \_\_\_\_\_ layer is responsible for finding the best path to route packets within an internetwork.
- a. Transport
  - b. Network
  - c. Session
  - d. Data Link



---

## Case Projects



1. Jennifer, Moe, and Lisa recently passed the Network+ certification exam and have been hired to perform network support at your company. Moe has been complaining that memorizing the layers of the OSI model was difficult and a waste of time. He understands why protocol developers need to know about it, but thinks that network administrators and support people only need to know which protocols are operating on the network in question. Explain to Moe the reasons for using the OSI model. How could detailed knowledge of the model be valuable in Moe's network-support position?

**24** Chapter 1 Introducing Networks

2. Lisa overhears your conversation with Moe and asks your opinion about data encapsulation. She is confused about the layers in which encapsulation occurs. Explain the five steps of data encapsulation to her.
3. Jennifer is unsure in which layer the MAC addresses function. Because the MAC is on the NIC and is associated with the physical media, she asks why this address is associated with the Data Link layer. Explain to Jennifer the functions of the Data Link layer and the sublayers within this layer. Where exactly does the MAC address fit in?
4. Create a mnemonic device to help Jennifer, Moe, and Lisa a helpful way to remember the layers of the OSI model. In addition, make a list of three key words associated with each layer to help them remember the layer's function.
5. This afternoon, you will be explaining the OSI model to senior management. Design a flowchart showing how the OSI model facilitates the transferring of data from a source to a destination node.



chapter 2

## Network Devices

**After reading this chapter and completing the exercises, you will be able to:**

- Explain the uses, advantages, and disadvantages of repeaters, hubs, wireless access points, bridges, switches, and routers
- Define the standards associated with wireless media
- Explain basic wireless connection parameters, security, and troubleshooting
- Define network segmentation
- Explain network segmentation using bridges, switches, routers, brouters, and gateways
- Explain Ethernet operations
- Define Fast Ethernet and Gigabit Ethernet

## Many devices help control and extend the usable size of a growing network.

These devices have a wide variety of functions and are added to networks to allow a greater number of computers to exist on the network; to extend the usable distance of the network; to segment, or localize, traffic on the network; to subdivide the network so problems are easier to isolate; and to join existing networks together. In this chapter, you will learn about the different devices that can be used to accomplish these objectives. The devices include repeaters, hubs, bridges, switches, routers, brouters, wireless access points, and gateways. In addition, you will learn about Ethernet, which is the most prolific network technology in use on LANs today. This chapter will explain a variety of Ethernet operations including CSMA/CD, Fast Ethernet, Gigabit Ethernet, and half- and full-duplex communications.

---

## Repeaters

The number of **nodes** on a network and the length of cable used influence the quality of communication on the network. As data leaves the source, or transmitting station, the NIC converts the data to electrical impulses if copper wire is used, or to light signals if a fiber-optic cable is used. As the signal travels the length of the cable, the distance traversed weakens it. The nodes that copy and pass on the signal also degrade it. This degradation of signal clarity is called **attenuation**.

Repeaters work against attenuation by repeating signals that they receive on a network, typically cleaning and regenerating the digital transmission in the process. For example, a digital signal communicates one of two different states (one or zero) in its communication stream. On a network connected by wire media, the presence of voltage signifies a one, and the absence of voltage signifies a zero. However, as attenuation occurs, the digital signal may become increasingly difficult to decipher. If left uncorrected, attenuation could make the signal unreadable. A repeater takes the attenuated signal, cleans it up, and then sends the clear and crisp digital stream to the rest of the network, as shown in Figure 2-1.

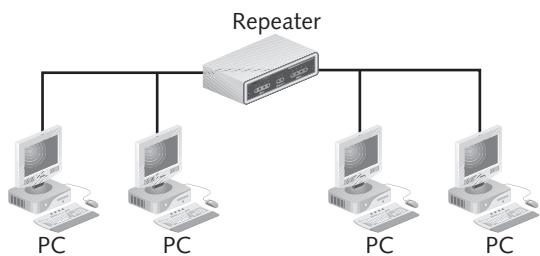


**Figure 2-1** Repeater

Note that on analog networks, devices that boost the signal are called **amplifiers**. These devices do not have the same signal regeneration capabilities as repeaters because they must maintain the shape of the received signal. Therefore, noise tends to be amplified with the signal.

Because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they are Physical layer (layer 1) devices on the OSI model. This means that most repeaters cannot distinguish between a good signal and a corrupt signal. Thus, they normally repeat everything. On optical networks, signal amplification is handled by **optical repeaters**. Optical repeaters use either a light-emitting diode (LED) or diode laser per optical signal. The type of fiber (multimode or single mode), and the distance of the cable run determine the necessary type of optical repeater.

Some repeaters can be used to connect two physically different types of cabling. For example, a repeater might connect a twisted-pair cable to a coaxial cable. However, repeaters cannot reformat, resize, or otherwise manipulate the data. In other words, when a network uses different physical media but the same data type and packet structure, a repeater can be used as a connection device. Figure 2-2 shows a repeater on a bus network.

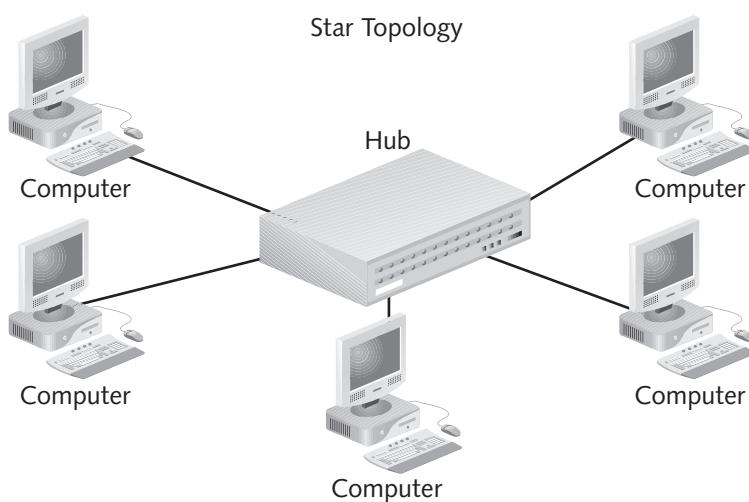


**Figure 2-2** Repeater in the network

## Hubs

A **hub** is a generic connection device used to tie several networking cables together to create a link between different stations on a network. Most hubs are plugged into electric power and are **active hubs**. They usually amplify or repeat signals that pass through them, similar to repeaters. Because they have multiple inbound and outbound connections, these hubs are also known as multiport repeaters. A hub that merely connects cables on a network and provides no signal regeneration is called a **passive hub** and is not a repeater.

Often, a hub forms a central point on a network where the cables come together. A star topology often has a hub at its center. Topology usually refers to the physical layout of network cable and devices. When all stations are connected to a central hub, the topology is known as a star because of its appearance. Figure 2-3 shows a star topology with a hub in the center.



**Figure 2-3** Star topology

## Advantages and Disadvantages of Repeaters and Hubs

Because repeaters and hubs simply repeat and clean up a signal, network administrators mainly use them to increase the usable distance of a network. They have little impact on network speed because they do not perform any processing.

Familiarize yourself with the following advantages of using repeaters and hubs on your network:

- Repeaters and hubs can extend a network's total distance.
- Repeaters and hubs do not seriously affect network performance.
- Certain repeaters can connect networks using different physical media.

Although repeaters and hubs provide many advantages, they do have disadvantages. The following list describes the disadvantages of using them on the network:

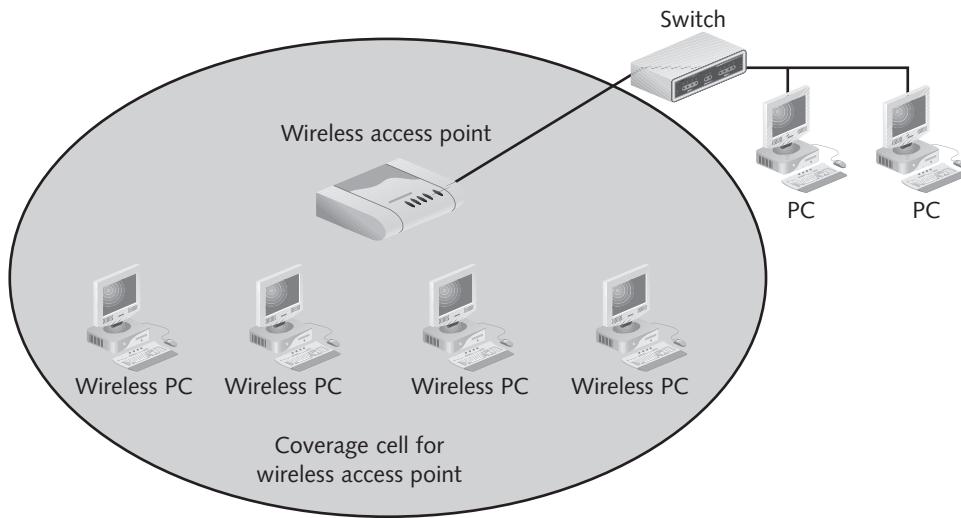
- Repeaters and hubs cannot connect different network architectures, such as **Token Ring** and **Ethernet**.
- Repeaters and hubs do not reduce network traffic.
- Repeaters and hubs do not segment the network.

Repeaters and hubs do not reformat data structures, so they cannot connect networks that require different types of frames. Also, they do not reduce network traffic because they repeat everything they receive. Because they repeat without discrimination, the number of repeaters and hubs must be limited on your network. Too many of these devices on a network could throw off network communication timings by repeating frames after they normally would have been dropped. Such a circumstance would create noise on the wire and increase the likelihood of packet collisions, which would reduce network performance.

Repeaters also do not segment a network. That is, they do not create logical or physical divisions of the network. On an Ethernet network, frames that are broadcast on a given segment may collide. This happens when two or more stations transmit at the same time. Devices that “see” the traffic of other devices are said to be on the same **collision domain** as those devices. Since repeaters and hubs do not segment a network, computers that are separated by these devices are susceptible to data frame collision.

## Wireless Access Points

The proliferation of wireless technologies and **wireless local area networks (WLANs)** has led to the creation of a new network device known as a wireless access point. **Wireless access points** provide cell-based areas where wireless clients such as laptops and PDAs can connect to the network by associating with the access point. Each access point and wireless client must contain a radio transceiver that matches the wireless technology on the network or there can be no communications between them. While wires do not run between the clients and the access point, the access point is typically wired into a switch so that the clients have full access to the LAN and the WAN. Although wireless access points operate at the Physical and Data Link layers of the OSI model, in most respects, a wireless access point functions exactly like a hub. Bandwidth on the access point is shared, so all clients are on the same collision domain. Therefore, as more clients associate with an access point, the available bandwidth per client decreases. Figure 2-4 shows a wireless access point connected to a switch.



2

**Figure 2-4** Wireless access point in the network

## Wireless Standards and Organizations

In 1999, a nonprofit organization named the Wi-Fi Alliance was created to drive the adoption of a single worldwide wireless standard—namely IEEE 802.11. The Wi-Fi Alliance tests and certifies wireless devices that implement the universal IEEE 802.11 specifications. This guarantees a certain level of compatibility when using wireless devices that are labeled as “Wi-Fi compliant.” The IEEE created the 802.11 specification and all of its manifestations.

The IEEE standards for WLANs use unlicensed, but not unregulated, radio frequencies. The most common standards are 802.11a, 802.11b, and 802.11g. 802.11n is the latest standard but is still in the works. Table 2-1 shows the various standards and their corresponding frequencies, transmission methods, and data rates.

Standard	Frequency Band (GHz)	Transmission Method	Data Rates (Mbps)
Original 801.11	2.4	infrared, frequency hopping spread spectrum, direct sequence spread spectrum	1, 2
802.11b	2.4	direct sequence spread spectrum	1, 2, 5.5, 11
802.11a	5	orthogonal frequency division multiplexing	6, 9, 12, 18, 24, 36, 48, 54
802.11g	2.4	direct sequence spread spectrum and orthogonal frequency division multiplexing	1, 2, 5.5, 11 and 6, 9, 12, 18, 24, 36, 48, 54

**Table 2-1** 802.11 Standards

You will notice in Table 2-1 that the 802.11g standard and the older 802.11b standard use the same frequency range and share the ability to use direct-sequence spread spectrum technology. This allows the older 802.11b radios to work on a newer 802.11g network. Since 802.11a devices are in a different frequency range, they cannot work with “b” or “g” radios. Also note that the data rates listed are discrete. That is, a client device jumps from a higher listed rate to a lower listed rate as it moves away from the access point. A “g” client will never use a data rate of 15 Mbps. It will jump down from 18 to 12 because 15 is not supported. This behavior is known as dynamic rate shifting.

802.11 access points are typically connected to Ethernet switches. Ethernet (802.3) uses a network access method known as CSMA/CD, which is described in detail later in this chapter. 802.11 uses a variation of this method known as CSMA/CA. While it is not important to understand the operation details of CSMA/CA for the Cisco CCNA exam, you should know that CSMA/CA provides far less rated bandwidth than CSMA/CD. This is primarily because every single wireless frame must be acknowledged by the receiver, creating substantial overhead.

## Wireless Network Components

802.11 can be used in two different modes. Wireless clients can connect and communicate directly with each other in **ad hoc mode**. In this mode, there is no access point, which is not typical. Commonly, wireless clients attach wirelessly to an access point in **infrastructure mode**. As previously stated, this mode involves the access point wired back into a switch so that the client has access to the LAN and WAN, not just the WLAN.

If a single access point is available in infrastructure mode, then the mode is said to be a **Basic Service Set (BSS)**. More typically, WLANs involve multiple access points connected to various switches in the network. This allows users to roam around the building and remain connected to the WLAN as well as the LAN and WAN. This type of infrastructure mode is known as an **Extended Service Set (ESS)**.

## Wireless Connectivity

So, how does a wireless client attach to the WLAN? Access points typically broadcast their network name. The network name is more commonly known as the **Service Set Identifier (SSID)**. When wireless clients are powered on, they begin scanning the airspace for available access points. They detect the broadcasted SSID of the various access points in the area and attempt to associate with the one that has the highest signal level and the lowest error rate. If the system is open (that is, if there is no authentication or encryption required), the client is accepted by the access point and begins communications. Sometimes, access points are configured not to broadcast their SSID. In this case, the wireless clients must already be configured with the correct SSID. This is a safety feature, although a very weak one. The client will send out a probe request with the configured SSID, and the access point with that SSID configured will allow the client to associate. In any case, if authentication and other security information are required, the wireless client will have to provide it or no data will be allowed to pass through the access point.

## Wireless Security Measures

Various levels of security are available for use on WLANs. To a large extent, the type of security used will be determined by the level of security necessary and by what is supportable on the access point. For example, many people use the inexpensive Linksys wireless routers in their home.

While security is always necessary in WLANs due to the broadcast nature of the medium, these devices are not designed to handle the most complex and highest levels of security. That is because it is unlikely that you have data on your home computer that is of value to a hacker. The most important reason to implement security on your WLAN at home is so others in your neighborhood do not use your bandwidth for free. In the workplace, where compromised data presents a major financial risk, home-level security is not an option. These situations call for security that not only requires the client device to authenticate, but that also prompts the device user to enter a username and password. In this implementation, 802.1x is used at the physical layer to block ports, and the **Extensible Authentication Protocol (EAP)** is used at layer 2 to transfer the authentication frames. Table 2-2 lists the various wireless security options along with the type of encryption and typical uses.

2

802.11 Security Option	Type of Encryption	Uses
WEP (Wired Equivalent Privacy)	Lower-level encryption: RC4 algorithm, static key	Home
WPA (Wi-Fi Protected Access)	Higher level encryption: TKIP algorithm, dynamic keys, user authentication also supported (802.1x)	Home and small office
WPA2 (Wi-Fi Protected Access version 2)	Highest level of encryption: AES algorithm, dynamic keys, user authentication also supported (802.1x)	Home and small office
802.11i (The IEEE standard based on WPA2)	Highest level of encryption: AES algorithm, dynamic keys, user authentication with 802.1x/EAP	Businesses

**Table 2-2** 802.11 Security

## Wireless Troubleshooting

Wireless systems are much more difficult to set up and troubleshoot than wired systems. The possibility of configuration mismatches and interference from other systems is high. In general, you should follow these steps when adding a WLAN to your LAN:

1. Make sure your wired LAN is working.
2. Complete a wireless site survey to determine access point placement.
3. Install the access point(s) with no security.
4. Attempt to associate to the access point with a laptop.
5. Configure security on both the access point and the client.
6. Verify connectivity at all layers.

The fact that users on a wireless network tend to come and go makes it even more crucial to monitor your WLAN. Remember, as the number of users on the WLAN increases, each user's

**32** Chapter 2 Network Devices

individual bandwidth will decrease. Other problems that are particular to 802.11 networks include the following:

1. Interference from too much overlap of one access point's cell range onto another. Some access point overlap is crucial for roaming, but adjacent access points on the same or adjacent communications channels will seriously degrade network performance.
2. User devices must be using an 802.11 standard that is compatible with the access point standards.
3. Access point antennas should be securely connected and in optimal position.
4. Watch for sources of interference such as large bodies of water, metal buildings or fences, other wireless devices using Bluetooth technology, older microwave ovens, some cordless phones, and baby monitors.

---

## Advantages and Disadvantages of Wireless Access Points

802.11 is everywhere, but it is not perfect. Familiarize yourself with the following advantages of using 802.11 on your network:

- Wireless devices provide the ability to work anywhere within range of your access points.
- Wireless extends the range of your network without running additional wires except the ones from the access points to the switch.

The disadvantages of using 802.11 include the following:

- Wireless introduces serious security concerns into the network environment.
- 802.11 provides much less bandwidth than wired devices.
- Many situations exist where 802.11 will not function well due to serious interference from various sources.

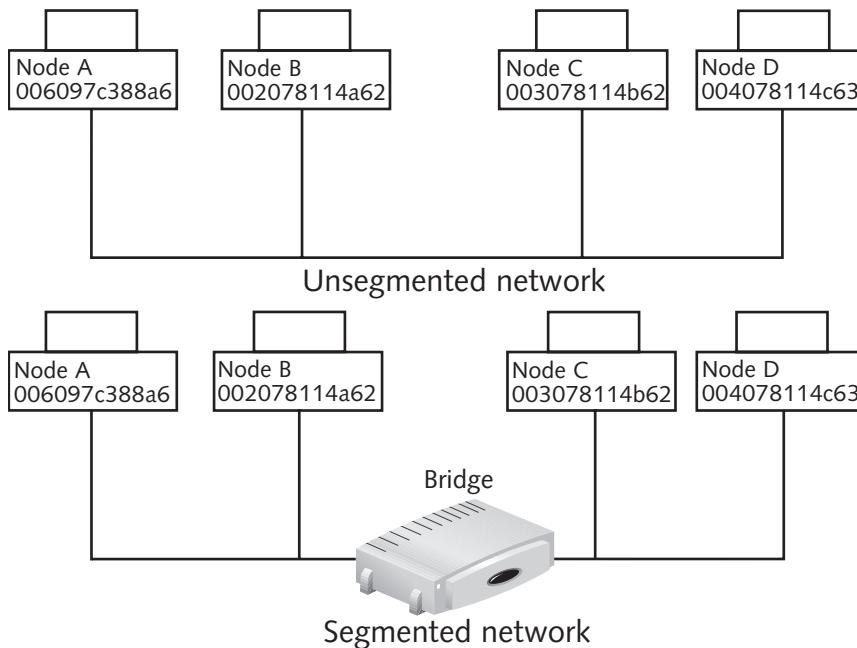
---

## Network Segmentation

Segmentation is an essential and fundamental networking concept. In particular, you must understand network segmentation using bridges, switches, and routers.

Network problems occur when network administrators place too many nodes on the same network **segment**. (A segment is a part of a network that is divided logically or physically from the rest of the network.) As the number of nodes increases, the amount of traffic on a segment increases, as does the chance that two nodes will transmit data at exactly the same time. This causes the number of collisions to increase. The result is a large amount of network bandwidth being used to retransmit frames that have been destroyed by collisions. Segmentation is the answer to this problem.

Segmentation is the breaking down of a single heavily populated network segment into smaller segments, or collision domains, populated by fewer nodes. Figure 2-5 shows an example of network segmentation.



**Figure 2-5** Network segmentation

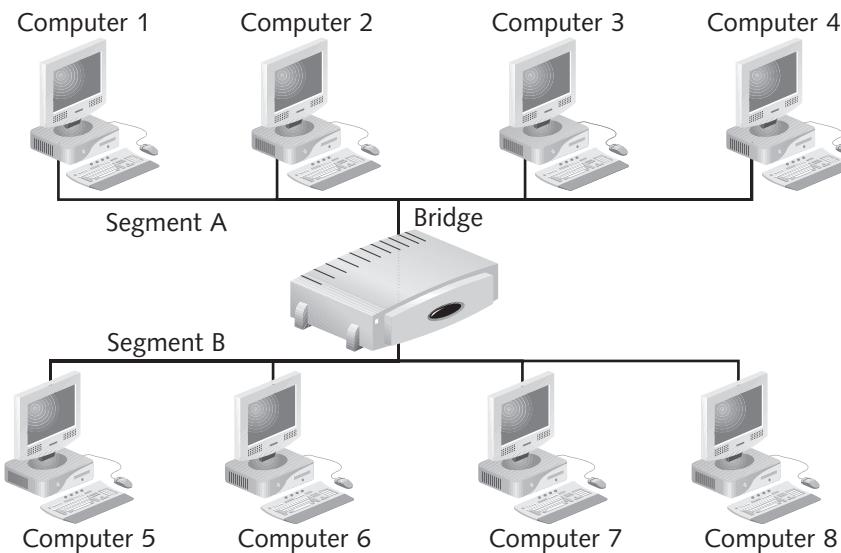
In Figure 2-5, the upper portion of the graphic depicts a network consisting of four nodes sharing a single segment—in other words, a single collision domain. In this unsegmented network, all computers would be affected by the traffic of other nodes. The lower portion of the graphic shows a bridge separating the four computers into two collision domains. This segmentation reduces the number of computers that must contend for use of the bandwidth. For example, on a 100-Mbps network, each collision domain shares its own 100 Mbps. In the upper graphic, four computers would share this 100 Mbps. In the lower graphic, only two computers would share the bandwidth. As a result, network collisions and retransmissions are reduced. A bridge is one networking device that can be used to segment networks.

## Bridges

Bridges operate at the Data Link layer of the OSI model. A bridge filters traffic between network segments by examining the destination MAC address. Based on this destination MAC address, the bridge either forwards or discards the frame. If the destination MAC address is located on a segment other than the originating segment, the bridge forwards it. If the frame was meant for the local segment, the bridge discards the frame. In this way, the bridge reduces network traffic by keeping local traffic on the local segment. However, when a client sends a broadcast frame, which is a frame destined for all computers on the network, the bridge will always forward the frame. In addition, if a bridge has no destination MAC address in its table, it will send the frame out to all interfaces except the one on which it entered.

The bridge functions like a repeater in that it listens to incoming frames and repeats them on other segments. The only real difference is that it actually reads the MAC address and chooses whether to repeat or discard a frame.

Consider the network shown in Figure 2-6. The bridge divides the network into two segments (Segment A and Segment B). Communications between computers on Segment A do not pass through to Segment B, and vice versa. However, communications between computers on Segment A and Segment B will be repeated through the bridge to the other segment. For example, when Computer 1 sends a message to Computer 4, the bridge discards the frame, and only Computers 2, 3, and 4 receive it. Computer 4 will accept the frame, while Computers 2 and 3 will discard it after determining that it was not destined for their MAC address. However, when Computer 2 sends a frame to Computer 5, all computers on Segment A and Segment B will examine the frame. Only Computer 5 will accept the frame, and the rest will discard it after determining that the MAC address on the frame does not match theirs.



**Figure 2-6** Bridge

Bridges can use two different methods to determine which segment includes a specific MAC address. One method is transparent bridging, and the other is source-route bridging.

### Transparent Bridges

Transparent bridges are also called learning bridges because they build a table of MAC addresses as they receive frames. This means that they “learn” which addresses are on which segments. When a bridge first receives power, its bridging table is empty. Over time, though, it learns which segments have which MAC addresses as frames are forwarded. The bridge uses the source MAC addresses to determine which addresses are on which segments. By determining a frame’s origin, the bridge knows where to send frames in the future. Ethernet networks mainly use transparent bridges. Token Ring networks usually employ source-routing bridges.

### Source-Routing Bridges

In Token Ring networks, source-routing bridges rely on the source of the frame transmission to provide the routing information. The source computer determines the best path by sending out explorer frames. When the destination computer receives the explorer frames, it determines

the best routes and sends that information back to the source. Then, the source includes the routing information returned by its explorer frames in the frame sent across the network. The bridge uses this information to build its table.

## Translation Bridges

2

Although bridges tend to connect similar networks, translation bridges can connect networks with different architectures, such as Ethernet and Token Ring. These bridges appear as transparent bridges to an Ethernet host and as source-routing bridges to a Token Ring host.

## Advantages and Disadvantages of Bridges

Bridges do more than repeaters because they evaluate frames; however, their additional capabilities bring both advantages and disadvantages. The advantages of using a bridge include the following:

- Bridges can extend a network by acting as a repeater.
- Bridges can reduce network traffic on a segment by subdividing network communications.
- Bridges increase the available bandwidth to individual nodes because fewer nodes share a collision domain.
- Bridges reduce collisions.
- Some bridges connect networks using different media types and architectures.

Because bridges regenerate the network signal when they pass it from segment to segment, they can extend the network's usable distance. Bridges selectively forward frames, which effectively reduces the number of messages circulating around the network. Because this also reduces the number of frames and broadcasting stations, the likelihood that two stations will broadcast at the same time on the same segment and cause a collision is reduced. Bridges also connect different media types, and some can connect different architectures. Bridges, however, do have some disadvantages:

- Because bridges do more than repeaters by viewing MAC addresses, the extra processing makes them slower than repeaters and hubs.
- Bridges forward broadcast frames indiscriminately, so they do not filter broadcast traffic.
- Bridges are more expensive than repeaters and hubs.

The fact that bridges forward broadcast traffic can be a major disadvantage on a network during a **broadcast storm**, which happens when two or more stations engage in the transmission of excessive broadcast traffic. While some broadcasting is normal on networks, excessive broadcasting due to errors or malfunctioning NICs can seriously erode network performance and even bring a network to a halt. Because bridges simply forward broadcast traffic, they do nothing to reduce the storm.

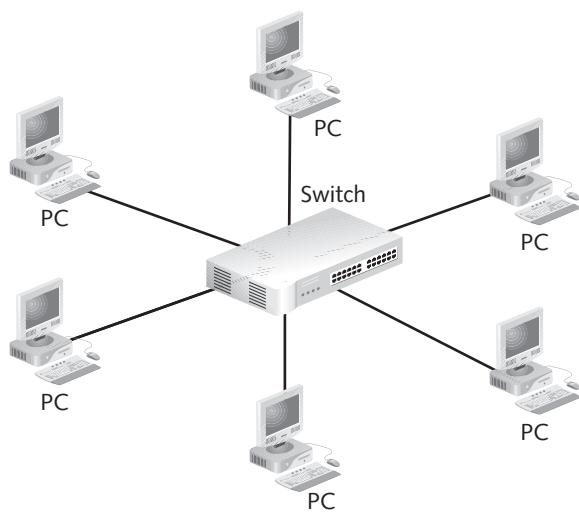
---

## Switches

Like bridges, switches operate at the Data Link layer of the OSI model. **Switches** increase network performance by reducing the number of frames transmitted to the rest of the network. In an Ethernet network, computers are usually connected directly to a switch. Unlike bridges,

a switch opens a **virtual circuit** between the source and the destination. This prevents communications between just two computers from being broadcast to every computer on the network or segment. This is called **microsegmentation** because the segment, or collision domain, is effectively just the sending and receiving nodes.

When two machines have a virtual circuit, they do not have to share the bandwidth with any other computers. Thus, if the total network transfer capacity is 100 Mbps, the two communicating machines get the full **bandwidth**, which is 100 Mbps in this case. Multiple virtual circuits can be in use at the same time, each with its own 100 Mbps. This is called “switched bandwidth.” Conversely, a hub will divide the 100 Mbps among each communicating node connected to its ports. This is called “shared bandwidth.” When machines must share a wire and compete for available bandwidth with other machines, they experience **contention**. A switch reduces contention by subdividing a network into virtual circuits. Figure 2-7 shows a star topology that uses a switch.



**Figure 2-7** Star topology using a switch

Switches filter based on MAC addresses and build tables in memory just like bridges, but the switching table will have a mapping of switch port number to MAC address instead of bridge segment number to MAC address. Switches can have an unlimited number of ports, which can be connected directly to workstations. Usually bridges have fewer than 10 ports, and so those ports are connected to hubs rather than directly to workstations. Bridges are software-based devices; switches are hardware-based.

## Advantages and Disadvantages of Switches

The advantages of switches include the following:

- Switches increase available network bandwidth.
- Switches reduce the workload on individual computers.
- Switches increase network performance.

- Networks that include switches experience fewer frame collisions because switches create collision domains for each connection (a process called microsegmentation).
- Switches connect directly to workstations.

Even though the benefits of switching are great, switching has its disadvantages. Here are a few to consider:

- Switches are significantly more expensive than bridges.
- Network connectivity problems can be difficult to trace through a switch.
- Broadcast traffic may be troublesome.

Switches usually cost more than bridges, but they do a lot more. Unfortunately, because switches are constantly creating and dropping virtual circuits, network problems may be difficult to trace. Broadcast traffic is also a problem for switches, because the hardware address indicates that all computers should receive a frame. The switch can either block or send these broadcasts. When a switch blocks the broadcasts, network performance improves, but applications that rely on broadcasts to keep track of resources are not able to communicate using broadcasts. However, if the switch sends the broadcasts, they will be transmitted by the switch to every machine on the network. In that case, virtual circuits provide no benefit. Of course, other types of network communications will still benefit from the use of switches. A switch is the device of choice for improving network performance, and many companies are replacing hubs and bridges with switches.



Switching is covered in greater detail in Chapters 12 and 13.

**NOTE**



This section discusses Ethernet switches (primarily used in LANs), but several implementations of switching for WAN configurations also exist. Public telecommunications carriers such as AT&T, Sprint, and MCI provide most of these switching services. The services include packet switching, switched-56, AT&T Switched Digital Services, and MCI Communications Virtual Private Data Network Services.

2

## Routers

As networks grow more complex, network administrators may need to use routers on their networks. **Routers** provide filtering and network traffic control on LANs and WANs. These devices can connect multiple segments and multiple networks. Networks connected by multiple routers are called **internetworks** because they create a larger network of interconnected, smaller networks.

Routers operate at the Network layer of the OSI model. Routers are similar to switches and bridges in that they segment a network and filter traffic. However, instead of filtering traffic based on the physical address of a frame (as do switches and bridges), routers use the logical address. Like bridges and switches, routers use a table to determine how to forward packets.



You will learn more about routing tables in Chapter 3.

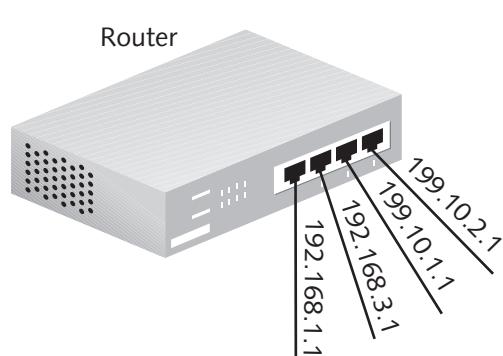
**NOTE**

When a router is introduced into a network, it creates more networks because every interface on a router represents a different network. Routers create collision domains; they also create **broadcast domains** because a router will not pass broadcast traffic. A broadcast domain is a group of network devices that will receive LAN broadcast traffic from each other.

### Physical vs. Logical Addresses

The NIC manufacturer burns the physical address or MAC address into the network card during the manufacturing process. The MAC address, which is found at the Data Link layer of the OSI model, is used by bridges and switches to make forwarding decisions within a network or **subnetwork**. On the other hand, the type of Network and Transport protocols used by the devices on a network dictate the format of the logical address. For example, the TCP/IP and IPX/SPX protocol suites span the Network layer and Transport layer of the OSI reference model. Both of these protocols are routable, which means that they can be used for communication between networks or subnetworks that are divided by a router or routers.

When TCP/IP is used on an internetwork, the logical address is known as an **IP address**. Routers use the IP address to route packets to the correct network segment. Software, not hardware, implements IP addresses. This means that routers use the logical Network layer software address to route packets to the appropriate network segment. Figure 2-8 illustrates a router connecting four different network segments. Notice that each **port** (connection) on the router has its own unique IP address and the addresses are on different networks.



**Figure 2-8** Router

### Advantages and Disadvantages of Routers

Although routers offer several advantages for the network, they have some inherent disadvantages. First, let us take a look at the advantages:

- Routers can connect different network architectures, such as Ethernet and Token Ring.
- Routers can choose the best path across an internetwork using dynamic routing techniques.



Dynamic routing techniques are described in Chapters 7 and 8.

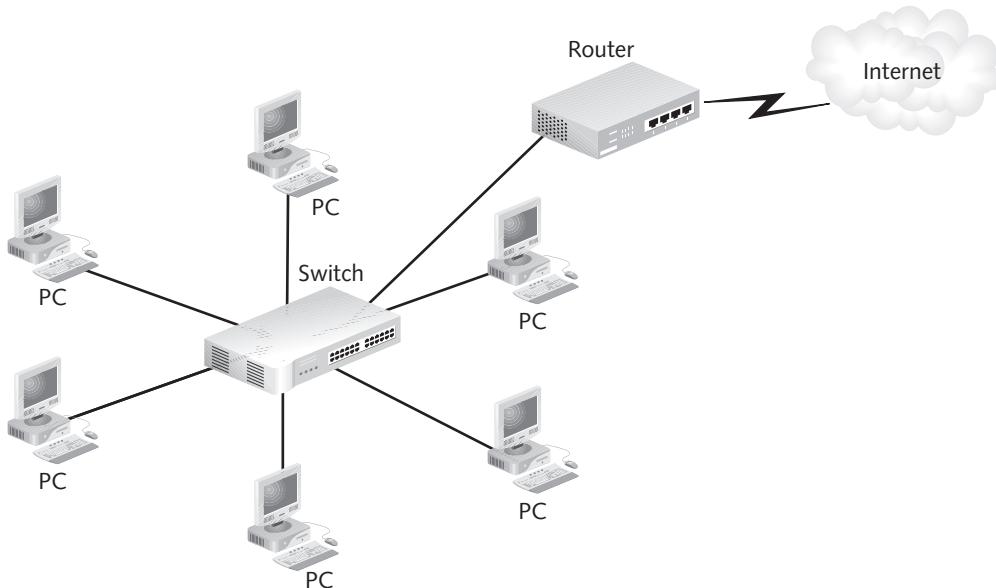
- Routers reduce network traffic by creating collision domains.
- Routers reduce network traffic by creating broadcast domains.

The disadvantages of using routers on the network include the following:

- Routers work only with routable network protocols; most but not all protocols are routable.
- Routers are more expensive than other devices.
- Dynamic router communications (inter-router communication) cause additional network overhead, which results in less bandwidth for user data.
- Routers are slower than other devices because they must analyze a data transmission from the Physical through the Network layer, whereas bridges and switches only read two layers of information: the Physical and Data Link.

2

Routers are commonly used to connect networks to the Internet. Figure 2-9 displays a network consisting of a switch that uses a physical star topology to connect computers to the Internet via a router.



**Figure 2-9** Router connecting network to the Internet

## Brouters

Several types of hybrid devices exist in the networking world. One such device is the **brouter**. A brouter functions as both a bridge for nonroutable protocols and a router for routable protocols.

A brouter provides the best attributes of both a bridge and a router. The brouter acts as a bridge when it receives a packet that contains a nonroutable protocol, such as NetBEUI. To accomplish its bridging task, the brouter uses the MAC address. In contrast, the brouter acts

as a router when it receives a packet that contains a routable protocol, such as IP or IPX. To accomplish its routing task, the brouter uses the network address. Routers operate at the Network layer of the OSI model; bridges operate at the Data Link layer. Because the brouter performs a dual role, it operates at both the Data Link and Network layers and can replace separate bridges and routers.

## Gateways

A gateway is usually a combination of hardware and software. Its purpose is to translate between different protocol suites. The packets must be rebuilt not just at the lower levels for conversion between, for example, Ethernet and Token Ring, but at the very upper levels so that the actual data content can be converted into a format the destination can process. Because gateways must rebuild the packets at the upper layers of the OSI model, they have the most negative effect on network performance. That is to say, gateways create the most latency of all the devices discussed in this chapter. One example of a common gateway would be Services for Macintosh. This is software installed on a Windows 2003 server so that Macintosh computers, which use the AppleTalk protocol, can communicate with the server (most likely using the TCP/IP protocol) and share file and printer resources.

## Ethernet Operations

Ethernet is a network access method (or media access method) originated by the University of Hawaii, later adopted by Xerox Corporation, and standardized as IEEE 802.3 in the early 1980s. Today, Ethernet is the most commonly implemented media access method in new LANs. Many companies and individuals are continually working to improve the performance and increase the capabilities of Ethernet technology.

### CSMA/CD

Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to prevent data packets from colliding on the network. CSMA/CD allows any station connected to a network to transmit anytime there is not already a transmission on the wire. After each transmitted signal, each station must wait a minimum of 9.6 microseconds before transmitting another frame. This is called the **interframe gap (IFG)**, or **interpacket gap (IPG)**, which provides sufficient spacing between frames so that network interfaces have time to process a packet before receiving another.

**Collisions** Even though stations must listen to the wire before sending a transmission, two stations could listen to the wire simultaneously and not sense a **carrier signal**. In such a case, both stations might begin to transmit their data simultaneously. Shortly after the simultaneous transmissions, a collision would occur on the network wire. The stations would detect the collision as their transmitted signals collided with one another.

Once a collision is detected, the first station to detect the collision transmits a 32-bit **jam signal** that tells all other stations not to transmit for a brief period (9.6 microseconds or slightly more). The jam signal is used to ensure that all stations are aware that a collision has occurred. After the first station to detect the collision transmits the jam signal, the two stations that caused the collision use an algorithm to enter a **backoff period**, which causes them not to transmit for a random interval. The backoff period is an attempt to ensure that the two stations do not immediately cause another collision.

**Collision Domain** A collision domain is the physical area in which a frame collision might occur. The concept of collision domains is crucial to understanding network segmentation, which is essentially the practice of dividing a network into collision domains. As noted earlier in this chapter, repeaters and hubs do not segment the network and therefore do not divide collision domains. Routers, switches, bridges, and gateways do segment networks and thus create separate collision domains.

If a station transmits at the same time as another station in the same collision domain, there will be a collision. The 32-bit jam signal that is transmitted when the collision is discovered prevents all stations on that collision domain from transmitting. If the network is segmented, the collision domain is also divided, and the jam signal will only affect those stations that operate within that collision domain. Stations that operate within remote segments (other collision domains) are not subject to the collisions or frame errors that occur on the local segment.

## Fast Ethernet

When a 10BaseT network is experiencing congestion, upgrading to **Fast Ethernet** (100BaseT) can reduce congestion considerably. Fast Ethernet uses the same network access method (CSMA/CD) as common 10BaseT Ethernet, but provides 10 times the data transmission rate—100 Mbps. This means that frames can be transmitted in 90 percent less time with Fast Ethernet than with standard Ethernet.

When you upgrade from 10BaseT to Fast Ethernet, all the network cards, hubs, and other connectivity devices that are now expected to operate at 100 Mbps must be upgraded. If the 10BaseT network is using Category 5 or higher cable, the cable can still be used for Fast Ethernet operations. Also, a 10-Mbps Ethernet NIC can function on a Fast Ethernet network because the Fast Ethernet hub or switch to which the 10-Mbps device attaches will automatically negotiate a 10-Mbps connection. The Fast Ethernet hub will continue to operate at 100 Mbps with the other Fast Ethernet devices. Most modern NICs can operate at either 10 or 100 Mbps. Finally, Fast Ethernet devices are also capable of full-duplex operation, which allows them to obtain a transmission rate of 100 Mbps in each direction.

Fast Ethernet is defined under the **IEEE 802.3u** standard and includes 100 BaseTX and 100BaseT4 over unshielded twisted pair (UTP), and 100BaseFX over multimode fiber optic cable.

## Gigabit Ethernet

**Gigabit Ethernet** (1000BaseX) is the next iteration of Ethernet, increasing the speed to 1000 Mbps. IEEE 802.3z includes 1000BaseSX over multimode fiber, 1000BaseLX over single-mode fiber, and 1000BaseCX over balanced-copper cabling. The **IEEE 802.3ab** standard defines the more common 1000BaseT configuration over all four pairs of UTP. Although Gigabit Ethernet can work in half-duplex mode through hubs, this is not typical. Almost all applications of the standard are full-duplexed through switches. 10 Gigabit Ethernet (10GBaseX, 10GbE or 10GigE) is the fastest of the Ethernet standards. This relatively new standard is ten times faster than Gigabit Ethernet. 10 Gigabit Ethernet is full-duplex only, through switches. Half- and full-duplex communications are discussed in the next section.

## Half- and Full-Duplex Communications

In **half-duplex** communications, devices can send and receive signals, but not at the same time. In **full-duplex** communications, devices can send and receive signals simultaneously. As an analogy of these communication types, consider the walkie-talkie and the telephone. When two

**42** Chapter 2 Network Devices

people use walkie-talkies, one person must finish speaking before the other can transmit. This is half-duplex communication. When two people communicate over the telephone, both people can speak simultaneously, and both transmissions will be heard at the opposite ends. This is full-duplex communication. Full-duplex is also known just as duplex.

Most Ethernet networks can use equipment that supports half- and full-duplex communications. Hubs can only support half-duplex communications; switches and routers typically have ports that can support full-duplex. In half-duplex Ethernet communications, when a twisted-pair NIC sends a transmission, the card loops the transmission back from its transmit wire pair onto its receive pair. The card stores the looped-back frame. The transmission is also sent out of the card. The card then compares the looped-back frame with the original frame. If the frame is the same, then no collision occurs. If the looped-back frame is different from the original frame, then a collision is recorded.

The transmitted frame travels along the network through the hub to all other stations on the collision domain. Half-duplex NICs cannot transmit and receive simultaneously, so all stations on the collision domain (including the transmitting station) listen to the transmission before sending another.

Full-duplex Ethernet components can send and receive signals at the same time. Full-duplex communications use one set of wires to send and a separate set to receive. Because full-duplex network devices conduct the transmit and receive functions on different wire pairs and do not loop back transmissions as they are sent, collisions cannot occur. Furthermore, full-duplex Ethernet increases the throughput capability between devices because there are two separate communication paths. This means that 100BaseT full-duplex network cards are capable of transferring data at a rate of 100 Mbps in each direction, as compared with half-duplex 100BaseT cards. The benefits of using full-duplex are:

- Time is not wasted retransmitting frames, because there are no collisions.
- The full bandwidth is available in both directions because the send and receive functions are separate.
- Stations do not have to wait until other stations complete their transmissions.

---

## Chapter Summary

- Network administrators use devices to control and extend the usable size of a network. These devices include repeaters, hubs, bridges, switches, routers, brouters, and gateways.
- Repeaters work against attenuation by cleaning and repeating signals that they receive on a network. Repeaters work at the Physical layer of the OSI model. They cannot connect different network architectures. Repeaters do not reduce network traffic or segment the network.
- A hub ties several networking cables together to create a link between different stations on a network in a star configuration. An active hub has its own electrical power and acts as a repeater, whereas a passive hub provides no signal regeneration. Hubs operate at the Physical layer of the OSI model and do not segment the network.
- Network segmentation is the process of isolating hosts onto smaller segments to reduce the possibility of collisions. Bridges and switches are two devices commonly used to segment networks.

- Bridges provide network segmentation by examining the MAC address that is sent in the data frame. Bridges can use transparent bridging or source-route bridging to determine which segment includes a specific physical address. Bridges operate at the Data Link layer of the OSI model.
- Switches increase network performance by reducing the number of frames transmitted to the rest of a network. They do this by opening a virtual circuit between the source and the destination. Switches operate at the Data Link layer of the OSI model.
- Routers operate at the Network layer of the OSI model and provide filtering and network-traffic control on LANs and WANs. They can connect multiple segments and networks. On a TCP/IP network, routers use IP addresses to route packets to the correct network segment. Routers use information from routing tables to move packets from one network to another.
- A brouter is a hybrid device that functions both as a bridge for nonroutable protocols and as a router for routable protocols. Brouters operate at both the Data Link and Network layers.
- Gateways are usually a combination of hardware and software and are used to translate between different protocols. They usually operate at layer 4 and above in the OSI model.
- Ethernet is the most commonly used LAN technology because it is the most efficient choice for most LANs. CSMA/CD is used for Ethernet operations and involves a mechanism to handle collisions.
- Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps) are faster implementations of the Ethernet technology.
- Most Ethernet networks can support either half- or full-duplex communications. Half-duplex allows for two-way communications, but not at the same time (like walkie-talkies). Full-duplex communications allows for two-way communications at the same time (like a telephone).

---

## Key Terms

**100BaseFX** A Fast Ethernet implementation over multimode fiber-optic cabling. The maximum segment length is 412 meters.

**100BaseT4** A 100-Mbps Fast Ethernet implementation that uses four pairs of either Category 3, 4, or 5 UTP cable. The maximum segment length is 100 meters.

**100BaseTX** A Fast Ethernet implementation that uses two pairs of either Category 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP). 100Base-TX operates at 100 Mbps with a maximum segment distance of 100 meters.

**1000BaseCX** An IEEE 802.3z Gigabit Ethernet implementation that uses balanced copper cabling to achieve 1000 Mbps.

**1000BaseLX** An IEEE 802.3z Gigabit Ethernet implementation that uses single-mode fiber to achieve 1000 Mbps.

**1000BaseSX** An IEEE 802.3z Gigabit Ethernet implementation that uses multimode fiber to achieve 1000 Mbps.

**1000BaseT** An IEEE 802.3ab Gigabit Ethernet implementation that uses all four pairs of Category 5 or better UTP cable to achieve 1000 Mbps.

**44** Chapter 2 Network Devices

**active hub** A device that connects multiple nodes and/or networks, is connected to external power, and repeats and regenerates signals on a network.

**ad hoc mode** A wireless mode where client devices connect directly to each other without an access point.

**amplifier** A device used to boost analog signals on a broadband network.

**analog** A method of signal transmission on broadband networks.

**attenuation** The natural degradation of a transmitted signal over distance.

**backoff period** A random time interval used after a collision has been detected on an Ethernet network. Use of a backoff period minimizes the likelihood of another collision.

**bandwidth** The available capacity of the network. The greater the network bandwidth, the greater the speed in data transfer.

**Basic Service Set (BSS)** A wireless network with only one access point connected to a switch.

**bridge** A device that operates at the Data Link layer, used to filter traffic between network segments by evaluating the MAC address of packets that are sent to it.

**broadcast** A frame meant for the entire network.

**broadcast domain** A group of network devices that will receive LAN broadcast traffic from each other.

**broadcast storm** Excessive broadcast messages to every host on the network, launched by multiple computers; usually triggered by some error condition on the network.

**brouter** A device that functions as a bridge for nonroutable protocols and a router for routable protocols. The brouter operates at both the Data Link and Network layers.

**Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** An access method specified by the IEEE Ethernet 802.3 standard. In this method, a node will listen to see if the line is clear and then, if the line is clear, send data. Two nodes may still send at the same time and cause a collision, in which case the two nodes will then perform the backoff algorithm.

**carrier signal** A transmitted electromagnetic pulse or wave on the network wire that indicates a transmission is in progress.

**collision domain** In Ethernet networking, a single segment on a network. Any station on the same physical segment or separated by a repeater is in the same collision domain. Bridges, routers, and switches (depending on how they are configured) can separate collision domains.

**contention** The condition that occurs when computers on a network must share the available capacity of the network wire with other computers.

**Ethernet** See Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

**Fast Ethernet** Defined in IEEE 802.3u, and includes any of the following 100-Mbps Ethernet LAN technologies: 100Base-T4, 100Base-TX, 100Base-FX.

**Extended Service Set (ESS)** A wireless network with multiple access points connected to switches. The access points are typically configured with the same network name (SSID) to facilitate roaming.

**Extensible Authentication Protocol (EAP)** Works with 802.1x to carry the authentication information between the user, the access point, and the security server.

**full-duplex** A connection that allows communication in two directions at once; common telephone connections are typically full-duplex because people can talk and listen at the same time.

**gateway** A combination of hardware and software that translates between different protocols on a network.

**Gigabit Ethernet** Includes IEEE 802.3z and IEEE 802.3ab, which allow for speeds up to 1000 Mbps.

**10 Gigabit Ethernet (10GbE or 10 Gige)** A standard ten times faster than gigabit Ethernet that is always implemented as full duplex.

**half-duplex** A connection that allows communication in two directions, but not simultaneously; the circuit can be used for sending or receiving bits in only one direction at a time.

**hub** An active or passive device that connects network segments. Passive hubs are connection points; active hubs repeat and regenerate signals.

**IEEE 802.1x** The IEEE standard that defines port switching designed to shut down a switch port to all frames unless they are authentication frames.

**IEEE 802.11** The IEEE standard that defines wireless networking in the unlicensed frequency bands 2.4 GHz and 5 GHz.

**IEEE 802.11i** The most robust wireless security standard in use today. It is based on Wi-Fi Protected Access version 2 (WPA2) which uses AES encryption, dynamic keys, and user authentication via 802.1x and EAP.

**IEEE 802.3ab** The IEEE standard that defines the Gigabit Ethernet implementation 1000BaseT.

**IEEE 802.3u** The IEEE standard that defines Fast Ethernet implementations, including 100Base-T4, 100Base-TX, and 100Base-FX.

**IEEE 802.3z** The IEEE standard that defines Gigabit Ethernet implementations including 1000BaseCX, 1000BaseLX, and 1000BaseSX.

**infrastructure mode** A wireless mode in which the access point is wired back into a switch so that the client has access to the LAN and WAN, not just the WLAN.

**interframe gap (IFG)** The time required between the transmission of data frames on the network: 9.6 microseconds.

**interpacket gap (IPG)** *See* interframe gap.

**internetwork** A large network comprised of smaller interconnected networks.

**IP address** A 32-bit binary address used on TCP/IP networks; consists of a host portion and a network portion.

**jam signal** A 32-bit signal that is sent by the first station to detect a collision on an Ethernet network; ensures that all other stations are aware of the collision.

**latency** A delay on a network caused by a variety of factors, including the addition of devices.

**media access method** *See* network access method.

**microsegmentation** The type of segmentation that occurs through the use of virtual circuits between switches and nodes. Each connection enjoys the total bandwidth. Bandwidth is not shared as it is through hubs.

**network access method** The process by which network interface cards and devices communicate data on a network; an example is CSMA/CD. Also known as media access method.

**node** A connection point or junction on the network. A node can be a terminal or computer connected to the network.

**optical repeater** A network device that uses LEDs or diode lasers to amplify optical signals.

**passive hub** A device that connects network segments but does not perform signal regeneration.

**port** A connection point, usually for network cable, on a device such as a hub, bridge, switch, or router.

**repeater** A device that repeats and cleans signals on the network and extends the usable distance of the network.

**router** A device that connects multiple segments, subdivides a network, filters broadcast traffic, and maintains a routing table. A router uses the logical address to move data packets from point to point.

**segment (noun)** A section of a network that has been subdivided by routers, switches, or bridges.

**segment (verb)** To subdivide a network with a networking device, such as a bridge, switch, or router.

**segmentation** The process of breaking a network into smaller broadcast or collision domains.

**Service Set Identifier (SSID)** The network name configured on both the access point and the client so that they can communicate.

**subnetwork** A portion of the network created by manipulating a network address and breaking it down into smaller parts.

**switch** A device used between nodes on a network or between networks to create virtual circuits between two points. A switch increases bandwidth by isolating traffic between two points.

**Token Ring** A networking method developed by IBM that organizes the network into a physical or logical ring. The token is a logical device, and because stations may only broadcast on the network when they have the token, traffic does not collide.

**topology** The physical layout of network components. The topology can take the form of a ring, star, or bus.

**virtual circuit** A private connection between two points created by a switch that allows the two points to use the entire available bandwidth between them without contention.

**WEP (Wired Equivalent Privacy)** The initial wireless security standard that uses the RC4 algorithm with static key. This is now considered weak encryption.

**WPA (Wi-Fi Protected Access)** The improvement to WEP. It provides better encryption with the TKIP algorithm and dynamic keys.

**WPA2 (Wi-Fi Protected Access version 2)** The upgrade to WPA that provides the more robust AES algorithm for encryption as well as dynamic keys. Both WPA and WPA2 can be configured to use 802.1x/EAP.

**wireless access point** A network device that contains a radio transceiver, which allows wireless clients to connect to a WLAN.

**wireless local area network (WLAN)** A local area network consisting either entirely of wireless clients or a traditional LAN that contains wireless access points.

## Review Questions

1. Routers operate at which layer of the OSI model?
  - a. Data Link
  - b. Presentation
  - c. Session
  - d. Network

2. Bridges operate at which layer of the OSI model?
- Network
  - Data Link
  - Session
  - Transport
3. What is an advantage of using a switch rather than a bridge?
- lower cost
  - microsegmentation
  - use of the MAC address for filtering
  - There is no advantage to using a switch rather than a bridge.
4. Which of the following is an appropriate description of a broadcast storm?
- noise on the network
  - a large amount of traffic that passes directly through routers
  - an electrical condition caused by the sun
  - an error condition in which many broadcasts are sent simultaneously across the entire network
5. Which of the following best describes a network segment?
- a section of the network that has been separated from other segments by a router, bridge, or switch
  - a piece of broken twisted-pair cable
  - a piece of broken coaxial cable
  - a portion of the network that has been isolated with a repeater
6. A router that has eight ports will require how many IP addresses?
- four
  - six
  - eight
  - nine
  - ten
7. If a bridge receives a frame that has a destination MAC address located on the same segment from which it came, what will happen to the frame at the bridge?
- It will be forwarded.
  - It will be dropped.
  - The source signal will be repeated on all segments.
  - The destination address will be repeated on all segments.
8. Which of the following is *not* true about bridges?
- Bridges do not forward broadcast traffic.
  - Bridges segment the network.

**48** Chapter 2 Network Devices

- c. Bridges reduce the likelihood of a collision.
  - d. Bridges operate at the Data Link layer.
9. Which of the following is *not* true about routers?
- a. Routers operate at the Network layer.
  - b. Routers segment the network.
  - c. Routers reduce broadcast traffic.
  - d. Routers are faster than repeaters.
10. Which of the following is *not* true about switches?
- a. Switches operate at the Data Link layer.
  - b. Switches create virtual network segments.
  - c. Switches do not segment the network.
  - d. Switches create private connections between two points.
11. Which type of addresses do routers use?
- a. Logical
  - b. Physical
  - c. MAC
  - d. Data Link
12. A \_\_\_\_\_ can reduce broadcast traffic.
- a. bridge
  - b. router
  - c. repeater
  - d. connector
13. Which of the following is the correct name for a device that operates at both the Data Link and Network layers of the OSI reference model?
- a. router
  - b. bridge
  - c. switch
  - d. brouter
  - e. hub
14. When two stations broadcast at the same time on a single segment of an Ethernet network, what happens?
- a. contention
  - b. crash
  - c. collision
  - d. interruption

15. Which type of addresses do bridges use?
- logical
  - physical
  - IP
  - TCP
16. Which of the following is an implementation of Gigabit Ethernet?
- 1000BaseT
  - 1000BaseFX
  - 1000Base3
  - All of the above
17. Which of the following OSI layers contains media access control information?
- Physical
  - Data Link
  - Transport
  - Presentation
  - Session
  - Network
18. A switch divides network communications at which layer of the OSI model?
- Presentation
  - Network
  - Transport
  - Data Link
19. Which of the following devices translates between different protocols?
- bridge
  - switch
  - router
  - gateway
20. Rank the following devices from lowest to highest latency.
- hub
  - switch
  - gateway
  - router
21. Typically, which is the best device for increasing performance on your LAN?
- hub
  - bridge
  - switch
  - router

**50** Chapter 2 Network Devices

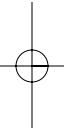
22. What kind of bridges do Ethernet networks use?
  - a. translation
  - b. source-routing
  - c. transparent
  - d. Brooklyn
23. What kind of bridges will connect an Ethernet network to a Token Ring network?
  - a. translation
  - b. source-routing
  - c. transparent
  - d. Brooklyn
24. Why don't repeaters and hubs segment the network?
  - a. They only work at the Physical layer where there is nothing to filter.
  - b. They are not considered devices.
  - c. They operate at the Network layer where segmentation can not occur.
  - d. They do segment the network.
25. Another name for IP address is \_\_\_\_\_ address, and another name for a MAC address is \_\_\_\_\_ address.
  - a. Ethernet, logical
  - b. physical, Ethernet
  - c. logical, physical
  - d. NIC, software
26. What device provides functions similar to a hub in wireless networks?
  - a. wireless local area network
  - b. optical repeater
  - c. virtual local area network
  - d. wireless access point
27. Which of the following represents the highest level of 802.11 security?
  - a. WPA2
  - b. WPA
  - c. 802.11i
  - d. WEP
28. Which of the following does not operate in the 2.4 GHz frequency range?
  - a. 802.11
  - b. 802.11a
  - c. 802.11b
  - d. 802.11g

## Case Projects



2

1. Winslow Networks wants to increase the performance of Sampson's network. As senior network administrator for Winslow, you assign Lisa to the job. That afternoon, while preparing to work on a lab assignment from her Cisco CCNA class, Lisa mentions that she would use a router to increase the performance of Sampson's network because routers are better than bridges. Explain to Lisa when and where a router would be the best choice. Under what circumstances would a router not be the best choice?
2. Another Winslow technician, Jennifer, overhears the discussion as she sits down to examine the lab materials spread out on Lisa's desk. Jennifer thinks Winslow should use a bridge to solve the problem. She reminds you that Sampson has a relatively small network and that a router would be more equipment than necessary. The Sampson network is running non-routable protocols. What do you tell Jennifer?
3. Moe works at Winslow too. As a graduate of the Cisco CCNA course, he thinks that a brouter would be the best choice. He has read that a brouter performs as both a router and a bridge, but he is not sure how this works. Explain to Moe how a brouter works. Is a brouter the best choice for Sampson? Are other devices worth consideration?
4. Moe and Lisa want you to settle an argument. Moe says a repeater is not the same as a hub. Lisa says it is. Moe argues that if you say a hub is a repeater, you might as well say that a bridge is a repeater too. Give Moe and Lisa your opinion and defend it.
5. Your boss is considering adding an 802.11 wireless network to your current LAN and buying wireless laptops for all the employees. In addition to the laptops, what else will he need to purchase and how will they be installed? Explain to your boss the pros and cons of using 802.11.





# 3

chapter

## TCP/IP

**After reading this chapter and completing the exercises, you will be able to:**

- Discuss the origins of TCP/IP
- Identify and discuss the different layer functions of TCP/IP
- Describe the functions performed by protocols in the TCP/IP protocol suite, including ICMP, UDP, TCP, ARP, and RARP
- Use Ping and Trace and describe their functions
- Explain how packets are transmitted
- Describe the Cisco three-layer hierarchical model

**TCP/IP stands for Transmission Control Protocol/Internet Protocol. However,**

TCP/IP is actually a protocol suite that contains a variable number of protocols, depending on the specific type of network. This chapter covers the aspects of the protocols that make up the TCP/IP protocol stack and are commonly used in data transmissions.

---

## Origins of TCP/IP

The invention and evolution of the **Transmission Control Protocol/Internet Protocol (TCP/IP)** protocol suite resulted from a coordinated effort by the U.S. Department of Defense (DOD). In the late 1960s, the DOD's research branch, named the **Advanced Research Projects Agency (ARPA)**, was charged with creating a wide area network (WAN). One of the results of the initial research was the TCP/IP protocol suite.

After completing the initial research and development, ARPA chose four universities to help establish the initial network: the University of California at Santa Barbara (UCSB), the University of California at Los Angeles (UCLA), the Stanford Research Institute (SRI), and the University of Utah. Initially, the network was formed by connecting sites with 50-Kbps leased lines. The resulting network was originally called the **Advanced Research Projects Agency Network**, or **ARPANET**.



ARPA is now known as the Defense Advanced Research Projects Agency, although the address for the agency's Web site is [www.arpa.mil](http://www.arpa.mil).

**NOTE**

Although the research was conducted for military purposes, academic researchers found the network to be a great way to communicate with one another. Because the U.S. government never classified or restricted the technology used to create the network, researchers at other organizations used the information gained from the project to create their own TCP/IP networks. This furthered the development of the protocol stack as various groups developed more protocols for the TCP/IP suite.

To further increase the popularity of TCP/IP, the DOD funded two projects. The first was the adaptation of TCP/IP to work with the UNIX operating system. The second was the inclusion of the TCP/IP protocol with Berkeley UNIX (Berkeley Software Distribution UNIX, or BSD UNIX). At the time, 90% of the university science departments in the United States used BSD UNIX, so TCP/IP quickly increased in popularity and use.

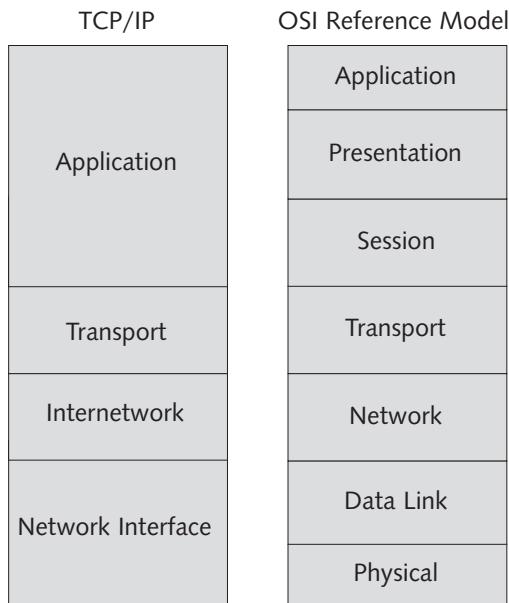
Eventually, this network interconnected so many different organizations and sites that it became known as the Internet. Because taxpayer money funded the project and the government did not classify it, it was considered to be in the public domain. This opened the Internet to everyone, organizations and individuals alike.

---

## Overview of the TCP/IP Protocol Suite

The TCP/IP model explains how the protocol suite works to provide communications. This model has four layers: Application, Transport, Internetwork, and Network Interface. A series of documents called **Requests for Comments (RFCs)** define, describe, and standardize the implementation and configuration of the TCP/IP protocol suite.

Figure 3-1 compares the TCP/IP protocol suite to the OSI reference model. Notice that the Application layer and the Network Interface layer of the TCP/IP model support multiple functions that require five different layers in the OSI model.



3

**Figure 3-1** Protocol architecture comparison

- *Application layer*—The **Application layer** in the TCP/IP model maps to the OSI Application, Presentation, and Session layers. This layer defines the functionality of the upper layers, including support for data formatting, conversion, and encryption. Also, the layer provides an application interface while providing session establishment and control services.
- *Transport layer*—The **Transport layer** in both models determines the connectionless or connection-oriented services. Two main protocols—TCP and UDP (**User Datagram Protocol**)—operate at this layer.
- *Internetwork layer*—The **Internetwork layer** in the TCP/IP model is a direct equivalent to the Network layer in the OSI reference model. Logical addressing information, such as the IP address, occurs here.
- *Network Interface layer*—The **Network Interface layer** of the TCP/IP model maps to both the Data Link and Physical layers of the OSI reference model. Network functions at this level include hardware addressing, media access control, physical topology, and electrical and mechanical specifications.

## Application Layer

The TCP/IP Application layer includes protocols for e-mail, remote logins, file transfers, Web browsing, network management, and name management. Specific protocols that exist at the TCP/IP Application layer include the following:

- **FTP**—The **File Transfer Protocol (FTP)** sends data over a reliable connection. This protocol can be used to send, delete, and move files to and from an FTP server and client.
- **TFTP**—The **Trivial File Transfer Protocol (TFTP)** sends data using an unreliable connection. This protocol functions similarly to FTP, but is faster and less reliable. A file transferred with TFTP is more likely to be corrupted than if it were transferred with FTP.

- **NFS**—The **Network File System (NFS)** is a distributed file system developed by Sun Microsystems that allows data to be shared across a network, regardless of the type of computer, operating system, network architecture, or protocol. This standard UNIX file system allows remote files to be manipulated as if they resided on the local computer.
- **SMTP**—The **Simple Mail Transfer Protocol (SMTP)** is the messaging or e-mail transfer protocol. This connection-oriented protocol allows mail to be transferred on TCP/IP networks and the Internet between e-mail servers.
- **Telnet**—A telnet client can use the **terminal emulation protocol (telnet)** to log on to a remote machine or telnet server. The telnet user can then run programs on the remote computer, using the remote computer's processor. Telnet is usually the first utility used when troubleshooting routers.
- **rlogin**—The **remote login application (rlogin)** allows you to gain access to TCP/IP hosts that support rlogin. This command-line utility allows you to navigate and manipulate a remote computer's directory structure.
- **SNMP**—You can install the **Simple Network Management Protocol (SNMP)** on TCP/IP hosts, including routers and other devices that support TCP/IP. SNMP is a connectionless protocol that permits remote tracking and management of TCP/IP hosts. For example, SNMP clients can report information such as hard drive space, network statistics, and various performance data. The SNMP manager can remotely monitor and control the SNMP clients.
- **DNS**—The **Domain Name System (DNS)** service provides TCP/IP host name to IP address resolution. For example, when you type *www.cisco.com* into a Web browser while connected to the Internet, the name must be resolved to an IP address before the communication can traverse the Internet. DNS servers on the Internet provide this name resolution so that you can establish a connection to the Cisco Web server.
- **HTTP**—The World Wide Web uses the **Hypertext Transfer Protocol (HTTP)**. This connection-oriented protocol allows you to connect your computer to other computers on the Internet and view Web page content.

## Transport Layer

The TCP/IP Transport layer performs several functions, the most notable being end-to-end packet delivery, reliability, and flow control. Two protocols, TCP and UDP, reside in the Transport layer of the TCP/IP model. TCP provides reliable, connection-oriented communications between two hosts. UDP provides connectionless datagram services between two hosts. Of the two protocols, TCP requires more network overhead because data is acknowledged as it is received. UDP is faster, but is also less reliable, because the recipient does not acknowledge data as it is received. Applications and utilities are written (programmed) to use either UDP or TCP. With UDP, communication reliability is left to the Application layer.

**Ports** Both TCP and UDP use port numbers for communications between hosts. Port numbers are similar to phone numbers in that Transport layer services can be “called” by their port number. For example, if you want to order a pizza to be delivered, you can look up the number

of a pizza place and dial the correct digits on your phone to request delivery. A similar event happens when a computer wants service from the TCP/IP Transport layer. When a computer wants to transfer a file over FTP, it uses TCP port 21 to establish and control the connection and TCP port 20 to transfer the data. TCP ports 20 and 21 are called **Well Known Port numbers** because applications expect to find FTP services on TCP port 21 and to transfer their data on TCP port 20.

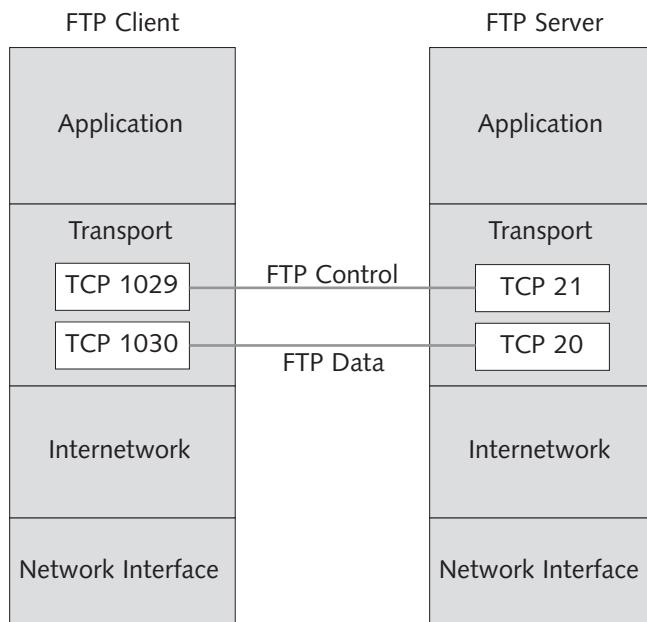
You should be familiar with the following Well Known TCP and UDP Port numbers from RFC 1700:

- TCP port 20—FTP data transfer
- TCP port 21—FTP control port
- TCP port 23—Telnet
- TCP port 25—SMTP
- TCP & UDP port 53—DNS (also known as Domain Name Server)
- UDP port 67 & 68—Dynamic Host Configuration Protocol (DHCP)
- TCP port 80—HTTP Web services
- TCP & UDP port 123—Network Time Protocol (NTP)
- TCP port 110—Post Office Protocol version 3 (POP3)
- TCP port 119—Network News Transfer Protocol (NNTP)
- UDP port 69—TFTP
- UDP port 161—SNMP

Each IP transport protocol has its own port numbers. This means that TCP has 65,535 ports available and UDP has another 65,535 ports available. Sometimes a service will exist on the same port number on both protocols. For example, DNS can use TCP port 53 or UDP port 53. Even if a Well Known Port number exists for a certain service, you do not have to use it for that service. For example, if you wanted to hide a Web server on the Internet, you might set its HTTP service port number to TCP 1055 (a randomly chosen number). Then, your Web clients would have to know the port number in order to contact your Web services. The port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic/Private Ports.

- Well Known Ports are those from 1 through 1,023.
- Registered Ports are those from 1,024 through 49,151.
- Dynamic/Private Ports are those from 49,152 through 65,535.

Figure 3-2 illustrates the use of ports in network communications. The FTP client calls the FTP server on TCP port 21 to establish communication. Then the FTP server responds to the client. The client computer dynamically configures the client software to use a port above TCP 1023; in the figure, that TCP port is 1029. Then, the FTP data transfer port is established. Again, the client calls the server on the Well Known Port of TCP 20. After the necessary acknowledgments, the client computer sets the FTP client software to use a port above TCP 1023 (port 1030 in the figure) to conduct the actual data transfer.



**Figure 3-2** TCP port usage in FTP communications

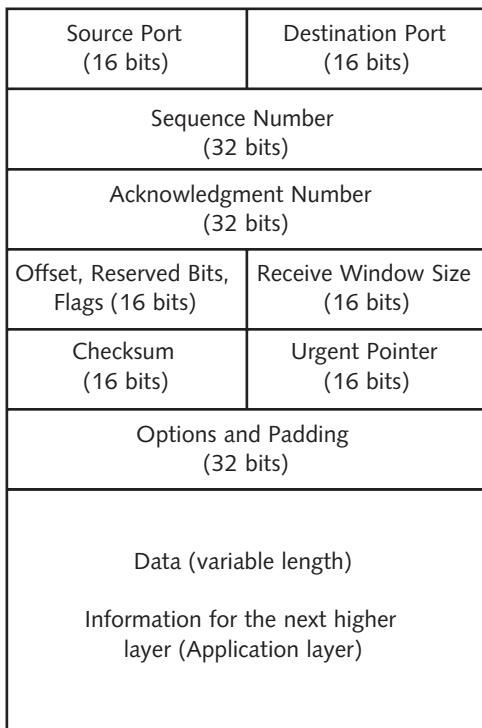
**TCP Three-Way Handshake** To establish a reliable connection between two points, TCP uses a **three-way handshake**. To do this, TCP transmits three packets before the actual data transfer occurs between two hosts. In order to transfer data reliably, the hosts must synchronize their communications to ensure that no packets are missed during communication.

As an analogy for the three-way handshake process, consider the following example: Assume that two pilots want to communicate with one another during a mission. The first pilot uses the call sign “Maverick” and the other pilot uses the call sign “Iceman.” A call from Maverick to Iceman might be similar to the following:

Maverick: “Iceman, this is Maverick. Do you copy?”  
 Iceman: “This is Iceman. I copy you, Maverick.”  
 Maverick: “Roger, Iceman.”

After this initial interaction, Maverick would begin sending information to Iceman. The major difference between the human interactions in the preceding example and how computers communicate via TCP is that the computers will use data packets with sequence numbers. Each host computer must acknowledge the sequence number of the sender and include its own sequence number in the following packet. This allows the computers to keep track of each packet and to ensure that none are lost during transmission. If a given packet does not arrive within a given time interval, the source computer will retransmit it. If the destination computer receives packets out of order, it can use the sequence numbers to reassemble those packets into the correct order.

Before investigating the three-way handshake process further, look at Figure 3-3, which is a conceptual drawing of the TCP packet header structure. In the following text, you will be concerned with the sequence number field and the acknowledgment number field.



3

**Figure 3-3** TCP packet header



TCP is defined in RFC 793 ([www.faqs.org/rfcs/rfc793.html](http://www.faqs.org/rfcs/rfc793.html)). The RFC describes all of the data fields in the TCP packet structure as well as the other TCP concepts discussed in this chapter.

NOTE

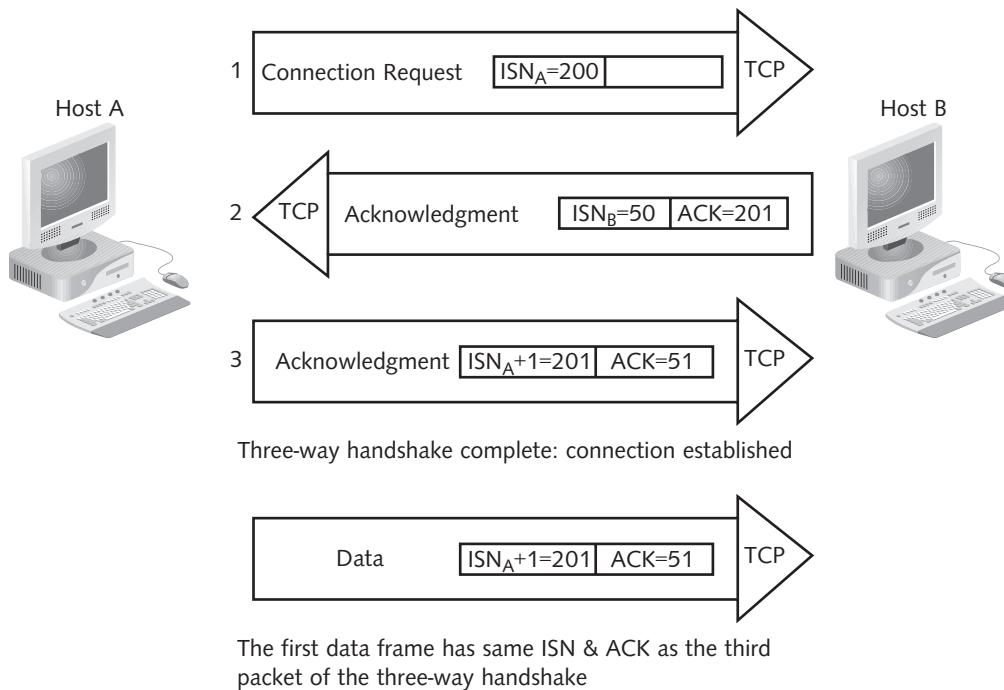
Before two computers can communicate over TCP, they must synchronize their **initial sequence numbers (ISN)**. These sequence numbers ensure that the communications are assembled in the proper order and that no missing packets exist. The synchronization process occurs when each host sends its own ISN and receives a confirmation and an ISN from the other host. When a synchronization request is sent, it is abbreviated as SYN. When an acknowledgment is sent, the abbreviation is ACK. This process has four steps:

1. Host A sends a SYN packet to Host B, which indicates a sequence number represented here as  $ISN_A$ . The ACK field contains a zero in this first packet.
2. Host B composes an ACK packet for Host A, which acknowledges A's sequence number by adding one to the sequence number that Host A submitted ( $ISN_A + 1$ ). This is called an **expectational acknowledgment**.

## 60 Chapter 3 TCP/IP

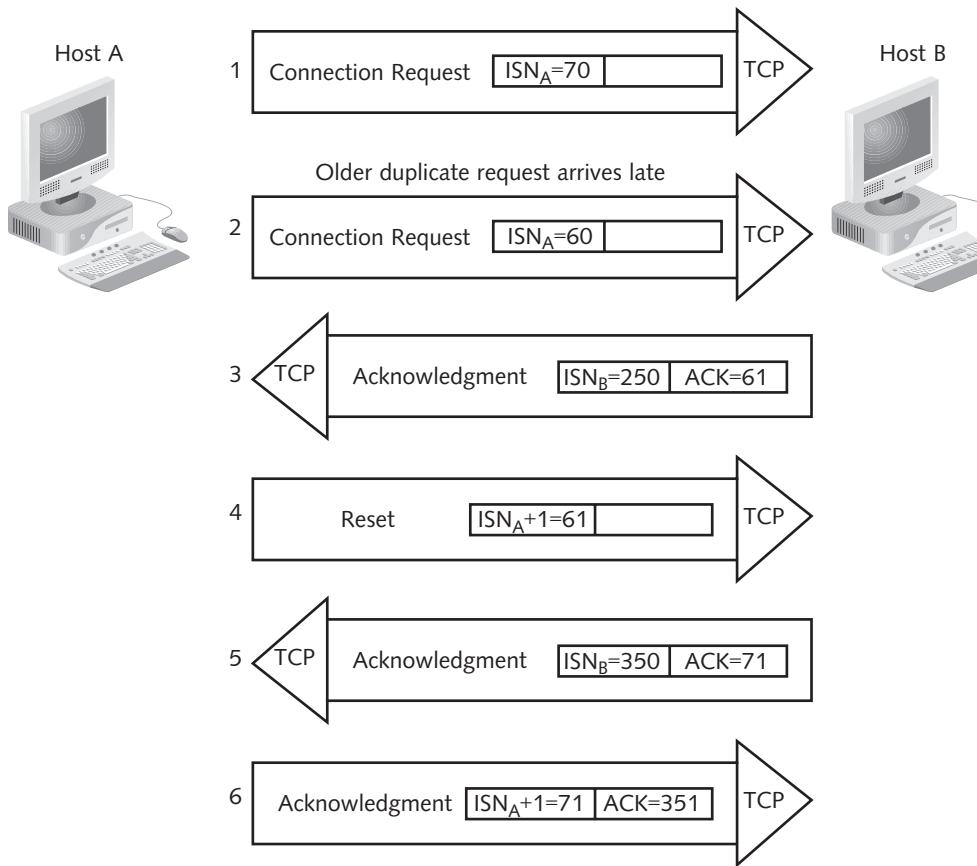
3. Host B adds its SYN data for Host A, which indicates its sequence number  $ISN_B$ , and sends that information to Host A in the ACK packet composed in Step 2.
4. Host A submits an ACK packet to Host B. The packet includes a sequence number of  $ISN_A+1$  (expected by Host B) and an acknowledgment number of  $ISN_B+1$ , which indicates that Host A received the last packet and now expects a sequence of  $ISN_B+1$  from Host B.

Even with four steps, only three packets need to be exchanged because the SYN packet from Host B also serves as the acknowledgment to the SYN packet from Host A. This process is called the TCP three-way handshake because only three packets travel the network to negotiate and synchronize the TCP connection, as shown in Figure 3-4.



**Figure 3-4** TCP three-way handshake

Notice in Figure 3-4 that the ACK number in the TCP packet from Host B is one number higher than the SYN number sent by Host A. This process shows that Host B expects to see ISN number 201 next ( $ISN_A+1$ ). The process is considered expectational (and not necessarily sequential because packets can get out of sequence). This allows hosts to detect and recover from failures or problems with TCP communications. RFC 793 states: “The principal reason for the three-way handshake is to prevent old duplicate connection initiations from causing confusion.” A number of possible error conditions are described in the RFC. One example of how TCP recovers from old duplicate connections is illustrated in Figure 3-5.



**Figure 3-5** TCP connection recovery

In the example, the packets are numbered to help you follow what is happening. Packet 1 is a connection request that arrives before a previous connection request (shown as packet 2). Host B acknowledges the connection request with the lower sequence number first (packet 3). Host A realizes that Host B is acknowledging an old connection request and sends a reset packet (packet 4). A **reset packet (RST)** indicates that a TCP connection is to be terminated without further interaction. Host B then acknowledges the newer connection request from Host A with packet 5 (ACK=71, which is one higher than the ISN in packet 1). Host A then completes the three-way handshake with Host B by sending data packet 6 with ISN=71 and ACK=351 (which is one higher than packet 5). In this example, TCP packets 1, 5, and 6 complete the three-way handshake.

**TCP Sliding Windows** Once the three-way handshake is complete and data transfer begins, TCP sliding windows control the flow and efficiency of communication. **Sliding windows**, also known as windowing, is a method of controlling packet flow between hosts. Windowing allows multiple packets to be sent and affirmed with a single acknowledgment packet.

The size of the TCP window determines the number of acknowledgments sent for a given data transfer because it constrains the amount of data that will be received before an acknowledgment is sent to the transmitting host. Essentially, once the window fills with data, the destination host sends an acknowledgment for all the packets received in that window. Then, the window slides over to accept new packets. It is important to note that the sender controls the window's size.

Networks that perform large data transfers should use large window sizes. During a connection for a large data transfer on a network with few collisions, a large TCP window would work well. Large window sizes can cause problems, however, on a network with high traffic volume or on one that does small data transfers. The large window may force the sending host to wait for an acknowledgment. If the sending host waits too long, it will retransmit data. Then, that sending host may receive an acknowledgment of both the original and the retransmitted data.

A small TCP window size produces frequent acknowledgments. Networks that transfer small amounts of data should use small window sizes; however, if the receiving computer is forced to acknowledge every data packet because of a small TCP sliding window, the increase in network traffic and the additional load placed on the hosts would be inefficient. Fortunately, TCP window sizes can adjust dynamically during the life of a connection, so that the window can be expanded or contracted as needed to make the communications more efficient.

TCP sliding windows is one of three methods used to control the flow of packets on a network; the other methods are **buffering** and **congestion avoidance**. Most networks can and do use buffering to keep up when packets are flowing in too quickly for the network to process. The **buffer** is a portion of memory where the device stores incoming packets until they can be processed. Congestion avoidance is a communication method for network devices that is designed to reduce the flow of packets from their source. Devices implement congestion avoidance by sending a “slow down the transmission rate” request to the device that is sending packets too rapidly. The ICMP Source Quench (covered in the next section) is a type of congestion avoidance.

## Internetwork Layer

The Internetwork layer in the TCP/IP model handles software, or logical, addressing. Four main protocols function at this layer:

- **IP**—The Internet Protocol (IP) provides a connectionless delivery service. The IP moves packets around the network, including through routers. IP is covered in greater detail later in Chapter 4.
- **ICMP**—The Internet Control Message Protocol (ICMP) controls and manages IP communications. This protocol, defined in RFC 792 ([www.faqs.org/rfcs/rfc792.html](http://www.faqs.org/rfcs/rfc792.html)), provides message control and error-reporting services between two TCP/IP hosts or between a host server and a gateway to the Internet. ICMP uses eight different message types to manage 11 different aspects of IP communications. The eight types of ICMP messages are **destination unreachable**, **time exceeded**, **parameter problem**, **source quench**, **redirect**, **echo request/reply**, **timestamp request/reply**, and **information request/reply**.

- **ARP**—The **Address Resolution Protocol (ARP)** resolves IP addresses to MAC addresses for source hosts that know the IP address of the destination host but not the MAC address. The source host issues an ARP broadcast requesting the MAC address for the corresponding IP address. Every station on the local network receives the ARP broadcast, but only the destination host responds.
- **RARP**—The **Reverse Address Resolution Protocol (RARP)** provides IP address to MAC address resolution in a manner similar to that of ARP, but does so under different circumstances. In the case of a **diskless workstation**, a source host will know its MAC address (because it is burned into the NIC) but not its IP address, because the IP address is implemented in software and a diskless workstation cannot store information locally. This host will get its IP address by issuing a RARP request to a RARP server. RARP has been largely replaced with DHCP because RARP requires that each MAC be manually configured on a central server and only the IP address can be assigned. DHCP conveys much more information and is easier to implement since it assigns the information irrespective of MAC address. DHCP is discussed in detail in Chapter 9.

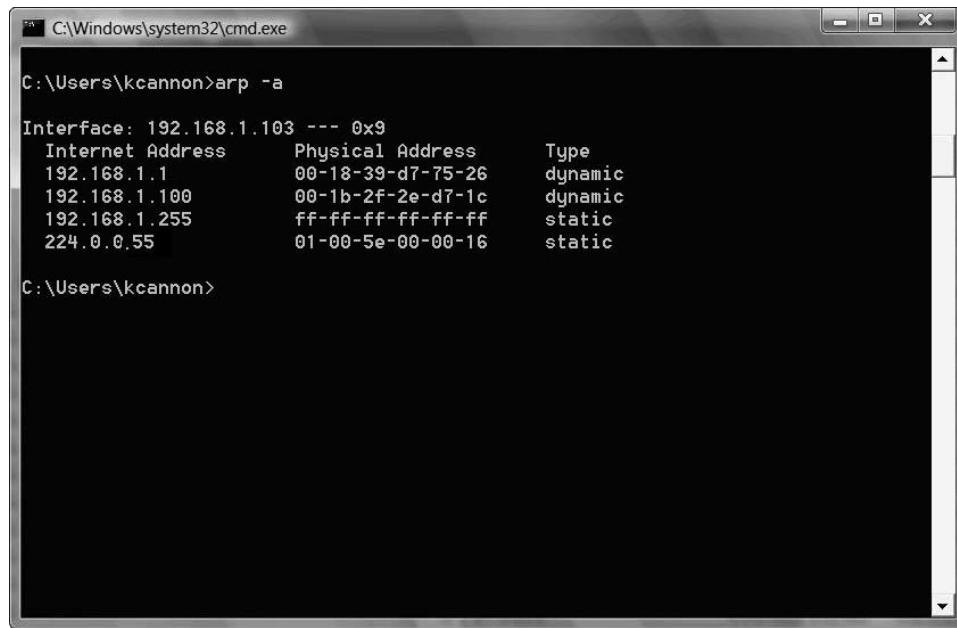
3

**ARP** IP, ARP, and RARP are all protocols associated with TCP/IP. IP is a **routed protocol**, which means that it contains enough information in its header to be routed through an internetwork. In order for data to be routed on an IP network, the packet must contain a source and destination IP address and a source and destination MAC address. ARP maps IP addresses to MAC addresses. In essence, the source of the network packet sends the information to the destination. Unique MAC addresses reference the endpoints in the exchange.

Many network devices maintain tables of the MAC and IP addresses of other devices on the network. These tables are called **ARP tables** and are maintained in volatile Random Access Memory (RAM). Many devices allow the network administrators to modify the ARP table (also known as ARP cache), but this is not a typical activity. Normally, devices automatically obtain and update their own ARP tables.

When a computer transmits a frame to a destination on the local network, it checks the ARP cache for an IP to MAC address mapping for the destination node. If the computer finds an appropriate IP to MAC address mapping, the source computer uses the IP and MAC addresses to encapsulate the data that it is ready to transmit. The source computer then sends the frame directly to the destination computer.

Figure 3-6 illustrates the ARP table of a Windows Vista host attached to the Internet. Notice that the IP address is listed first, the MAC address next, followed by information about whether the entry is static or dynamic. Most entries are dynamic, which means that the system performed IP to MAC resolution as needed. Static entries, which are rarely used, provide semi-permanent IP to MAC address mappings that an administrator entered manually. Administrators make these manual mappings to reduce ARP traffic on the network only when they know that a specific hardware address and IP address combination will remain constant.



```
C:\Windows\system32\cmd.exe
C:\Users\kcannon>arp -a

Interface: 192.168.1.103 --- 0x9
  Internet Address      Physical Address      Type
  192.168.1.1           00-18-39-d7-75-26    dynamic
  192.168.1.100          00-1b-2f-2e-d7-1c    dynamic
  192.168.1.255          ff-ff-ff-ff-ff-ff    static
  224.0.0.55             01-00-5e-00-00-16    static

C:\Users\kcannon>
```

**Figure 3-6** IP host's ARP table

**ARP Request** If a source computer cannot locate an IP to MAC address mapping in its ARP table, it must obtain the correct mapping because both an IP and MAC address for the source and destination are required to send data. To do this, the device initiates an **ARP request** to gain the destination's MAC address.



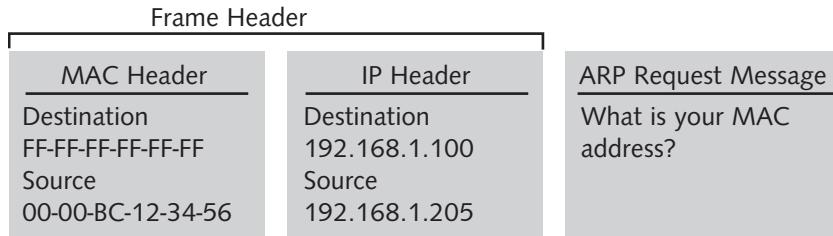
This section focuses on obtaining the MAC address for a specific IP address and assumes that the device already knows the destination's IP address. If the source computer has only the destination computer's host name, the source must first obtain the IP address, which is beyond the scope of the address resolution discussed here.

A source computer broadcasts an ARP request to all hosts on the local segment. Each device determines whether the frame is destined for its IP address. The one device that discovers that the ARP request broadcast frame is destined for its IP address responds to the ARP request.



Because it is a broadcast mechanism, ARP is only used on the local segment of a network. Routers will not pass ARP broadcasts. If the destination host is not on the same network segment as the source host, the source will send the packet to the **default gateway** (router) and will not ARP.

**ARP Request Frame** As you have learned, the lower layers in the protocol configuration encapsulate data frames. With ARP, the computer is seeking an IP to MAC address resolution, so the ARP frame includes both the MAC and IP addresses. The frame header includes the MAC header and the IP header, followed by the ARP message. The MAC header contains the destination and source MAC addresses, and the IP header contains the destination and source IP addresses. Figure 3-7 represents the ARP request frame configuration.



**Figure 3-7** ARP request packet

The packets shown in the figure are simplified to illustrate a specific point. Actual packets have 28 octets (28 sets of eight binary digits), which identify hardware types, protocol types, and message lengths. Because these components are not significant to the current discussion, they are not shown in the figure. RFC 826 ([www.faqs.org/rfcs/rfc826.html](http://www.faqs.org/rfcs/rfc826.html)) contains a detailed discussion of ARP.

Because the source host does not know the MAC address of the destination, the ARP request frame is a broadcast to all MAC addresses (FF-FF-FF-FF-FF-FF), and all devices on the local segment will investigate the frame to determine whether their IP addresses match that of the destination. The device that discovers its own IP address in the IP header reads the rest of the packet and returns an ARP reply. The rest of the devices on the segment discard the packet.

The ARP reply supplies the MAC address of the destination host in a unicast packet. When the computer that sent the ARP request receives the ARP reply from the host, it has the information necessary to properly address the data it wants to send to the destination computer. The source computer extracts the MAC address from the ARP reply and updates its ARP table. Then, the source computer creates and properly addresses its data packet and sends it with the MAC address of the destination computer.



Devices on the network that receive and eventually discard an ARP request use the source information to update their own ARP tables. Recipients enter the source computer's IP and MAC addresses from the ARP request packet into their local ARP tables.

**ARP Cache Life** Because the source checks its local ARP cache prior to sending packets on the local network, the ARP cache must contain current information. If the ARP cache contains stale information, data frames could be sent to the wrong host. Because the ARP table directs data packets to a specific network card based on the mapping, it is important that the mappings are correct. Host IP addresses can change, so old ARP table mappings can cause misdirected frames. To ensure that old ARP table entries do not become a serious problem, network devices place a timer on ARP entries. For example, Microsoft operating systems use

a two- to ten-minute timer for their ARP cache, and initial mappings through ARP have a two-minute timer. Any entry that is used twice within those first two minutes is automatically given a life of 10 minutes. After the 10 minutes, the ARP entry is removed from the ARP table.

By using timers, an operating system ensures that an ARP cache is never outdated for more than 10 minutes. The process of removing ARP entries from an ARP table is known as aging out the ARP table. In addition to aging out, devices on a network also replace ARP entries whenever new information is received. For example, if a computer receives a packet from a host that contains an IP and MAC address that are different from what it has listed in the ARP table, the computer updates its ARP table.

Even though the ARP tables are revised frequently, and their entries have short lives, they reduce network traffic. Without an ARP table, a device would have to perform an ARP for each frame, which could significantly increase network traffic on the local segment. As discussed earlier, increased traffic usually results in increased collisions and network delays.

**RARP** The Reverse Address Resolution Protocol (RARP) is similar to ARP in that computers use it to bind MAC addresses to IP addresses. However, RARP is used primarily by diskless workstations, which have MAC addresses burned into their network cards but no IP addresses. Because these workstations have no disks, they have no hard drives to hold IP configuration information. Therefore, they must obtain their IP configuration information each time they boot on the network.

To do this, a client's IP configuration must be stored on a RARP server. The RARP server maintains a table of IP to MAC address mappings for RARP clients. During the boot process, RARP clients call the RARP server to obtain their IP configuration information.

**RARP Request Frame** As mentioned earlier, a RARP frame has the same structure as an ARP frame. However, it contains different pieces of information. Figure 3-8 illustrates a RARP request frame.

### RARP

Frame Header		
MAC Header	IP Header	RARP Request Message
Destination FF-FF-FF-FF-FF-FF	Destination 255.255.255.255	What is my IP address?
Source 00-00-8C-12-34-56	Source 0.0.0.0	

### ARP

Frame Header		
MAC Header	IP Header	ARP Request Message
Destination FF-FF-FF-FF-FF-FF	Destination 192.168.1.100	What is your MAC address?
Source 00-00-8C-12-34-56	Source 192.168.1.205	

**Figure 3-8** RARP request frame

Notice that the IP header does not have a specific destination or source IP address in the RARP frame. The source does not know which device is the RARP server, so it must broadcast to all devices on the segment.

**RARP Client** Once a RARP client receives a RARP reply, it configures its IP networking components by copying its IP address configuration information into its local RAM. After the client receives the configuration settings, it can use the MAC and IP address to send frames on the network to other clients.

When the diskless workstation reboots or is shut down, the respective IP configuration information is lost. Consequently, each time the diskless workstation boots, it must obtain its IP configuration settings from a RARP server.

3

**ARP and RARP Compared** The RARP process and the ARP process are both concerned with IP to MAC address mapping. In addition, they use the same frame format and use broadcast addresses to accomplish their tasks. Although they share similarities, they have certain differences as well:

- ARP is concerned with obtaining the MAC address of other clients by using an IP address, but RARP obtains the IP address of the local host by using the local host's MAC address. Computers broadcast ARP frames on the local network by using the broadcast MAC address, but RARP uses the broadcast IP address (255.255.255.255) as well as the broadcast MAC address.
- The local host maintains the ARP table. A RARP server maintains the RARP table.
- The local host uses an ARP reply to update its ARP table and to send frames to the destination. The RARP reply is used to configure the IP protocol on the local host.

BOOTP and DHCP are two other protocols that provide the same basic functionality as RARP. Although DHCP is the most advanced of the three, all of the protocols provide IP configuration information to clients on bootup.

**Routers and ARP** As you have learned, routers segment networks. Segmenting a network reduces network traffic because routers do not forward broadcast traffic from one segment (subnet) to another by default. (Although you can configure most routers to forward broadcasts, such an action would increase network traffic unnecessarily.)

Because hosts rely on ARP requests to determine MAC addresses, and ARP requests use broadcasts, hosts must create broadcast traffic to determine the MAC address of other hosts. However, routers filter broadcast traffic, which means that ARP requests can go no further than the local segment (subnet). What happens when the source computer needs to send a message to a host on a remote segment? In such a case, the source must forward the frame to the router. This section explains how routers use their routing tables and ARP to correctly route packets across a network.

**ARP Tables** Like other network devices, routers maintain ARP tables to assist in transmitting frames from one network to another. If the destination IP address of a frame is on a segment to which a router is attached, the router will forward the frame directly to the destination. To do this, the router must obtain the MAC address for that destination. If the router has the MAC to IP mapping in its ARP table, the router can forward the frame directly. However, if the router does not have that mapping in its ARP table, it must issue an ARP request.

A router uses ARP just as other hosts use ARP. However, the router is bound to have a larger ARP table because it typically deals with more hosts. A router connects to multiple networks;

a typical TCP/IP host only connects to and receives ARP mappings for its local segment. Of course, the actual number of ARP table entries depends on the amount of traffic sent between and within the various segments. Routers have multiple network interfaces and therefore also include the port numbers of their NICs in the ARP table. Thus, routers can make routing decisions for incoming frames quickly by forwarding the frames to the appropriate interface.

**The Ping Utility** Network administrators and support personnel commonly use the **Packet Internet Groper (Ping)** utility to verify connectivity between two points. The Ping utility uses ICMP echo request/reply messages to verify connectivity at the Internetwork layer of the TCP/IP model, which is one reason that ICMP echo request/reply messages are the most commonly used ICMP message. When you issue the ping command, the source node sends out ICMP echo request packets to the specified destination node. The destination node, if it is up and running correctly, replies with ICMP echo reply packets. A simple Ping request can be issued by typing the ping [ip address] command. Figure 3-9 shows the output of the ping command on a Cisco router.

```
RouterB>ping 172.22.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.22.5.1, timeout is 2 seconds:
!!!!! ←
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/70/76 ms
RouterB>
```

Five exclamation points represent five successful ping replies

**Figure 3-9** Ping example

The reply of five exclamation points means that all five echo request packets were responded to with echo reply packets. Table 3-1 shows a list of possible replies:

Ping Replies	Meaning of Reply
!	Echo request successfully replied to with echo reply
.	Time-out (no response from destination)
U	Destination unreachable
?	Unknown packet type
&	Time-to-live exceeded
C	Packet experienced congestion

**Table 3-1** Ping responses

Cisco routers include two ping commands: standard ping and extended ping. Figure 3-10 shows the proper syntax for the extended ping command. The extended ping allows you to specify more echo request packets and larger packets. You can also use this command to ping IPX nodes with the IPX protocol. Overall, the standard and extended ping commands give you an excellent tool for determining the status of remote hosts on your network.

However, because Ping works at the Internetwork layer (OSI-Network layer), a successful ping does not mean that applications such as e-mail that use higher level protocols (SMTP) will work. All Ping does is verify network layer connectivity.

```

RouterB>en
Password:
RouterB#ping
Protocol [ip]: ip
Target IP address: 172.22.5.1
Repeat count [5]: 25
Datagram size [100]: 100
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 25, 100-byte ICMP Echoes to 172.22.5.1, timeout is 2 seconds:
!!!!!! Success rate is 100 percent (25/25), round-trip min/avg/max = 68/93/120 ms
RouterB#

```

**Figure 3-10** Extended ping commands

**The Trace Utility** The Trace utility also uses ICMP echo request/reply messages and can verify Internetwork layer (OSI-Network layer) connectivity. Trace shows the exact path a packet takes from the source to the destination. This is accomplished through the use of the time-to-live (TTL) counter. The packet is sent out first with a time-to-live of 1. Once it finds the first hop (router) on the path to the destination, the packet is returned with a destination unreachable message. The TTL is incremented to 2 and the packet is resent. This process continues until the packet reaches the destination or times out. The net effect is that you see the hops (transitions from one device to another) that a packet takes as it travels the network. Figure 3-11 shows a trace to a router port with IP address 172.22.5.1. You can use the Trace utility to determine where communications are breaking down along a particular path.

```

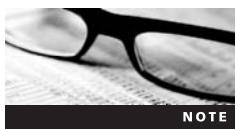
RouterB>trace ip 172.22.5.1
Type escape sequence to abort.
Tracing the route to 172.22.5.1
1 172.22.3.1 20 msec 20 msec 20 msec
2 172.22.4.2 36 msec 40 msec *
RouterB>

```

**Figure 3-11** Example of a trace command

Be aware that some routers can be configured to discard ICMP echo requests and therefore become invisible to the trace command. This feature is often used as a security measure because some network administrators do not want all of their network devices and IP addresses exposed to people who decide to run a trace. Several different malicious network

attacks have also been created using ICMP messages; one in particular is called an **ICMP flood**. An ICMP flood is caused by a malicious user or program that sends a large quantity of ICMP echo requests (pings) to a target device in an attempt to crash or greatly reduce the performance of the target device. This is another reason network administrators may choose to turn off ICMP support on key devices, such as routers.



Using Ping and Trace on a PC workstation is slightly different than on a Cisco router.

**NOTE**

## Network Interface Layer

The TCP/IP Network Interface layer plays the same role as the Data Link and Physical layers of the OSI model. The MAC address, network card drivers, and specific interfaces for the network card function at this level of the TCP/IP protocol stack. No specific IP functions exist at this layer because the layer's focus is on communication with the network card and other networking hardware such as cable, hubs, and repeaters.

---

## Understanding Frame Transmission

As frames travel a given network segment, each host on the segment evaluates the frame to determine whether the listed destination MAC address matches its own or is a broadcast to all hosts. The host makes a copy of the frame and sends the original along the network path. If the copy is for the local host's MAC address, a broadcast, or a multicast for which the local host is configured to receive, the frame continues up the protocol stack. If the frame is not for the local host, the copy is discarded.

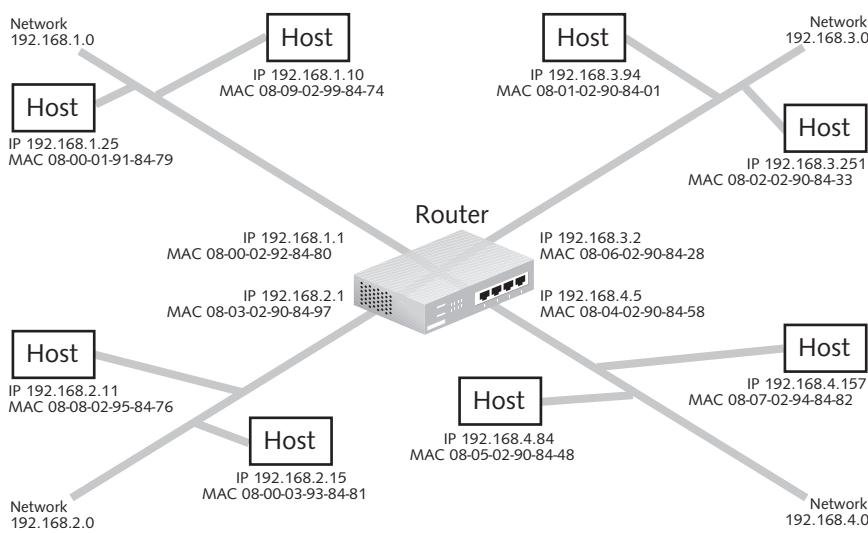
MAC address checking occurs at the Network Interface layer of the TCP/IP model or the Data Link layer (layer 2) of the OSI model. In the TCP/IP networking model, if the data is destined for the local host's MAC address or is a broadcast, the Network Interface layer information is removed. Next, the protocol stack passes the packet to the Internetwork layer. There, the destination IP address contained in the packet is compared to the local host's IP address. If the IP address listed in the data packet matches the local host address, or is a broadcast, the protocol stack strips off the Internetwork layer information and moves the packet up the protocol stack again.

As you learned previously, the Internetwork layer of the TCP/IP protocol stack is equivalent to the Network layer of the OSI model. The Network Interface layer and the Internetwork layer of the TCP/IP protocol stack ensure that data gets from one host to another on a TCP/IP network. The MAC address, at the Network Interface layer, uniquely identifies a specific device on any network. The IP address, at the Internetwork layer, identifies a specific host on a specific network. For a packet to be routed on a TCP/IP internetwork, an IP address and MAC address are required for both the source and destination hosts.

## Routers on the Network

Routers connect two or more network segments. In doing so, a router must have a separate identity for each network it is connecting. A router requires an IP address for every network

segment to which it is connected and a separate network interface or port for each network segment. For example, if a router connects four different network segments, it must have four different IP addresses and four different network interfaces. Figure 3-12 illustrates the configuration of a router that connects four segments.



**Figure 3-12** Configuration of a router with four segments

Notice that the router has an IP and MAC address for each of its ports that are valid for the network segments to which it is connected. Figure 3-12 also illustrates hosts configured on each network segment. Each device on the network has a unique IP address and MAC address.

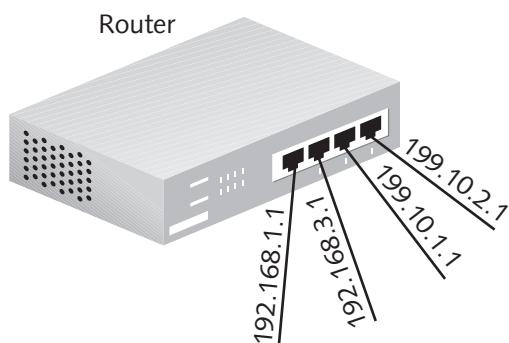


Serial interfaces—in other words, those attached to WAN links—typically do not have their own MAC addresses. The serial interfaces use MAC addresses assigned to LAN interfaces on the router.

When computers need to send frames to destinations not on their segment, they send them to the router (default gateway) instead. The router connected to the segment on which the frame originated recognizes that the destination host is on a different subnet. The router must determine which subnet should receive the frame. The router first removes the Network Interface information (OSI Data Link layer header), which contains the router's MAC address, because it is no longer necessary, now that the router is in possession of the packet. (The sending computer obtained the router's MAC address either from looking in its ARP cache or by sending an ARP request if the address was not in its table.) Then, the router analyzes the destination IP address in the Internetwork layer. The destination IP address will be the IP address of the final destination, not the IP address of the router. In fact, the source and destination IP addresses do not change throughout the journey of a frame from source to destination; only the MAC addresses change. The router references its **routing table** to determine which of its interfaces is connected to the destination network. Then the router rebuilds the Network Interface layer information with the appropriate format for the destination network and sends the frame out through the correct interface.

## Network to Network

Routers maintain routing tables that they use to route packets from one network to another. When a network uses TCP/IP, each port on a router requires an IP address; this allows the router to correctly forward the packet to the appropriate network segment. For example, consider the router connections shown in Figure 3-13. Assume the router port 192.168.1.1 connects to network segment 192.168.1.0. If a packet comes in for a host computer that connects to 192.168.1.0, the router knows to forward this packet to the 192.168.1.1 port because that port attaches to the correct network. The routing table tells the router that packets destined for 192.168.1.0 should be sent to the interface with IP address 192.168.1.1.



**Figure 3-13** Router

On a TCP/IP network, the logical addresses on a certain segment must be matched. For example, if the network segment is 192.168.1.0, all the hosts on that segment must have addresses that start with 192.168.1. They will also have unique identifiers for the last octet. This means that if you move a computer from one segment to another, the IP address will have to be changed to make it a member of the new segment.



You only need to ensure that the logical address, such as the IP address, matches the network because MAC addresses are a permanent part of the NIC and do not change when the computer is moved to a new network.

**NOTE**

## Dynamic or Static Tables

Routing tables match network addresses with the addresses of the routers that handle those networks. The tables can be built statically or dynamically. A static routing table requires manual configuration by the network administrator. Each route must be entered by hand, and the router always uses the same route to send packets to a specific network address, even if that route is not the most efficient.

Dynamic updates are provided through **routing protocols**. Routing protocols allow the routers to be updated automatically. Routers automatically build dynamic routing tables; a router capable of dynamic routing can choose from among the various routes on a network

without input from the administrator. The router communicates with other dynamic routers to determine the most efficient route from one point to another on the network. The routers can also track multiple paths to the same location so that alternate routes are available. Dynamic routers can use different methods to determine the best path across a network. One method is the distance-vector algorithm, which considers the number of hops between two points. A hop is a transition from one network segment to another. Each router along a network path is considered one hop. The packet takes the path with the smallest number of hops. A second method used in dynamic routing is the **link-state** algorithm. Using the link-state algorithm, the router takes into consideration network traffic, connection speed, and other factors.



Dynamic routing protocols are covered in more detail in Chapters 7 and 8.

**NOTE**

3

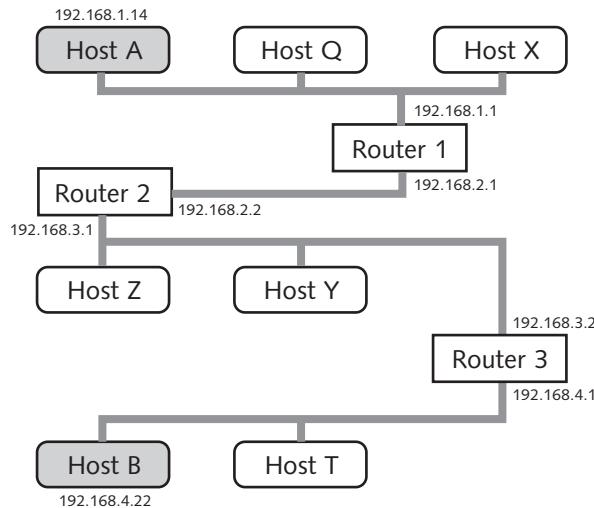
## Transmitting Packets to Remote Segments

When TCP/IP hosts transmit a packet to a remote segment, they cannot use ARP to obtain the correct MAC address because the router would filter the ARP request broadcast. In such a case, the TCP/IP host must use the services of the router. When TCP/IP hosts transmit packets to remote segments, they contact their default gateway, which is the network interface to which the client sends traffic that is destined for remote segments. The default gateway is usually a router connecting that local segment to other networks on the LAN or WAN. The TCP/IP host sends the data packet with the destination MAC address of the router. However, because the ultimate destination for the packet is a client on a remote network, the IP address listed as the destination is that of the remote host. When the router receives the packet, it pulls off the Network Interface information and analyzes the packet at the Internetwork layer.

The router checks its routing tables against the destination IP address to locate the appropriate network interface through which to forward the packet. If the router is directly connected to the network for which the packet is destined, it will re-address the frame at the Network Interface layer (OSI layer 2) with the MAC address of the destination host. It will get this MAC address from its ARP cache. If the information is not in its ARP table, the router will send an ARP request on the destination's segment and attempt to obtain the MAC address. If the router is not directly connected to the network in question, the router will send the packet to the next router in the path on the way to the destination. In this case, the destination IP address will stay the same but the destination MAC address will be that of the next router. The packet will be transferred around the internetwork until the destination is found or the TTL (hop count) reaches its maximum. Routers automatically discard packets that meet the packet's maximum hop count. This prevents packets from endlessly looping around the network or Internet. The process of moving a packet from one router to another in hopes of locating the correct IP address to MAC address mapping is known as indirect routing.

## Routing Packets

This section discusses the journey of a packet across a network, from Host A to Host B, as shown in Figure 3-14.



**Figure 3-14** Routing to a packet

Table 3-2 lists the IP address, network interface, and network identifier for each device.

Device IP	Address	Interface	Network
Host A	192.168.1.14		192.168.1.0
Router 1	192.168.1.1	Ethernet 0	192.168.1.0
Router 1	192.168.2.1	Ethernet 1	192.168.2.0
Router 2	192.168.2.2	Ethernet 0	192.168.2.0
Router 2	192.168.3.1	Ethernet 1	192.168.3.0
Router 3	192.168.3.2	Ethernet 0	192.168.3.0
Router 3	192.168.4.1	Ethernet 1	192.168.4.0
Host B	192.168.4.22		192.168.4.1

**Table 3-2** Information depicting the journey of a packet

**Host A** Host A composes its data at the Application layer and then encapsulates that data in the appropriate Transport layer protocol. The data is then passed to the Internetwork layer. At the Internetwork layer of the TCP/IP protocol stack, the IP address (192.168.4.22) for the destination host (Host B) is added as well as Host A's own IP address. Because Host A is communicating with a remote host, it uses the MAC address of its default gateway (Router 1; 192.168.1.1) as well as its own MAC address when encapsulating the data at the Network Interface layer.

Once Host A has properly composed, formatted, and addressed the packet, it transmits the packet on the network. The other hosts on the network (Q and X) receive and discard the packet because the MAC address does not match theirs. Router 1 accepts the packet because the MAC address does match.

**Router 1** Router 1 picks up the packet. After the router strips the Network Interface layer information off the packet, the router determines that the packet is destined for IP address 192.168.4.22. Router 1 then consults its routing table to determine to which router port the packet should be sent. Table 3-3 contains essential information from the routing table of Router 1. To make the example simple, the routing table shown here has only two pieces of information, the network and interface addresses. In reality, routing tables may contain several additional items, including subnet masks (or netmasks), default gateways, and cost metrics.

Network	Interface
192.168.1.0	192.168.1.1
192.168.2.0	192.168.2.1
192.168.3.0	192.168.2.2
192.168.4.0	192.168.2.2

**Table 3-3** Router 1 routing table

When Router 1 consults its routing table, it sees that packets destined for network 192.168.4.0 must be sent to 192.168.2.2, which is the interface on the next hop in the path, Router 2.

Router 1 repackages the Network Interface part of the data packet and transmits the packet out interface 192.168.2.1 using the MAC address of Router 2. The destination IP address, 192.168.4.22, remains unchanged.

**Router 2** Router 2 picks up the packet destined for its MAC address and strips off the Network Interface information. Router 2 analyzes the IP Header destination address and identifies that it is destined for network 192.168.4.0. Next, Router 2 checks its routing table, as shown in Table 3-4.

Network	Interface
192.168.1.0	192.168.2.1
192.168.2.0	192.168.2.2
192.168.3.0	192.168.3.1
192.168.4.0	192.168.3.2

**Table 3-4** Router 2 routing table

According to its routing table, Router 2 must send the packet destined for network 192.168.4.0 to the next router interface, which is 192.168.3.2 on Router 3. Therefore, Router 2 repackages the Network Interface layer of the packet, adding the MAC address for Router 3 to the packet. The destination IP address remains 192.168.4.22, and the data packet is sent to Router 3.

**Router 3** Router 3 receives the data packet destined for its MAC address and strips off the Network Interface layer information to reveal the IP address. Router 3 determines that the traffic is destined for network 192.168.4.0 and checks its routing table, as shown in Table 3-5.

Network	Interface
192.168.1.0	192.168.3.1
192.168.2.0	192.168.3.1
192.168.3.0	192.168.3.2
192.168.4.0	192.168.4.1

**Table 3-5** Router 3 routing table

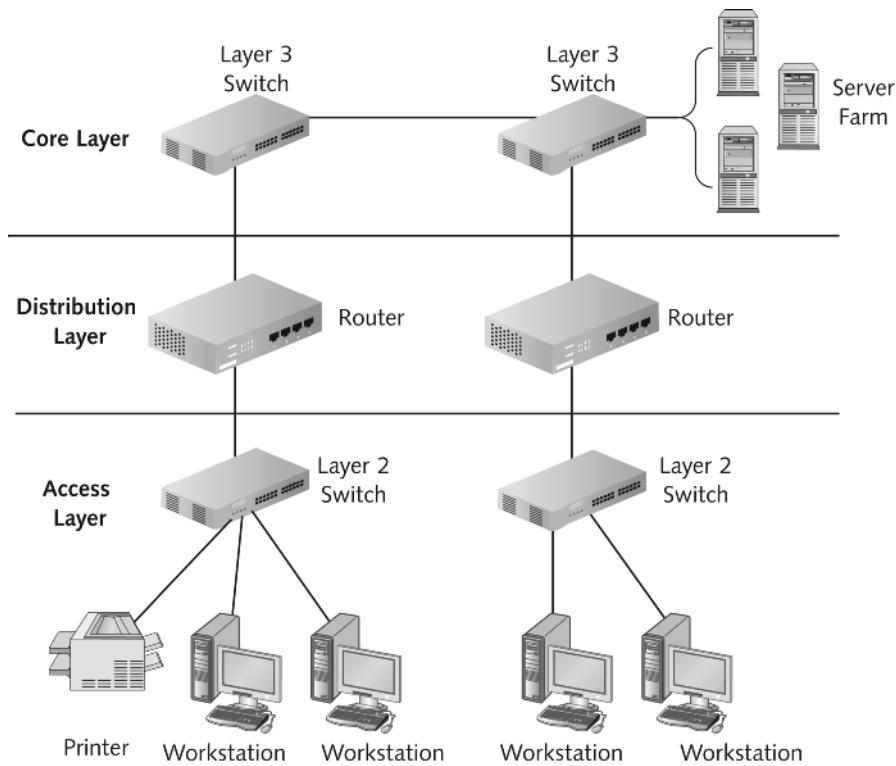
The routing table shows that one of Router 3's interfaces is directly connected to network 192.168.4.0. Because of this, Router 3 must then determine which host on the network has the IP address 192.168.4.22. Router 3 checks its ARP table to get a MAC address mapping for the client. If no mapping exists, Router 3 issues an ARP request on network 192.168.4.0 to get a mapping. Once the router has the correct MAC to IP mapping, it repackages the Network Interface layer using the MAC address of the destination. After the packet is properly addressed, Router 3 transmits it to Host B through interface 192.168.4.1.

**Host B** Both Host B and Host T receive the traffic forwarded by the router. However, Host T discards the packet because it is not addressed to its MAC address. Host B accepts the packet at the Network Interface layer and continues to process the data frame. At the Internetwork layer, Host B confirms that the packet is intended for its IP address. Then, it passes the data packet up the protocol stack for further processing.

## The Cisco Three-Layer Hierarchical Model

You have learned about the OSI model and the TCP/IP model. As a CCNA, you are also expected to understand a third model, the **Cisco Three-Layer Hierarchical model**. Unlike the OSI model and the TCP/IP model, the Cisco Three-Layer Hierarchical model does not describe how communications take place. Rather, it focuses on how best to design a network, especially a relatively large network or one that is expected to grow. In the past, networks have been flat for the most part that is, as the network grew, administrators would simply add devices such as routers and switches in a lateral and ad hoc fashion. The process provided for no structure or compartmentalization of functions. As a result, as networks became more complex and applications such as Voice-Over-IP, Video-Over-IP, and web applications demanded more bandwidth, the limitations of this flat design became more obvious.

Cisco's Three-Layer Hierarchical model was the response to this need for better functionality through design. Each layer of the model is involved in specific functions and is typically defined by a particular type of device. The three layers of the model from bottom up are Access, Distribution, and Core. These layers are explained in the following sections and illustrated in Figure 3-15.



3

**Figure 3-15** Cisco's Three-Layer Hierarchical Model

## Access Layer

The Access layer is the layer closest to the users, where they attach to the network. The Access layer device could be a router if the network is very small, but it is typically a hub or layer 2 switch. The Access layer is sometimes called the desktop layer because it deals with connecting workstations to the network. Frames are delivered to the users at this layer.

## Distribution Layer

The Distribution layer separates the Access layer from the Core layer, implements network policies, and provides many networking services such as Network Address Translation (NAT), firewall protection, and quality of service (QoS). IP addressing hierarchy is managed at this layer through routing policies, broadcast and multicast domains, and VLANs. (IP addressing is the process of assigning unique IP addresses to devices on the network.) This layer typically involves routers and includes all of the router functions. It provides almost all of the connectivity tasks required by the users, including Internet access.

## Core Layer

The Core layer is at the top of the model and is responsible for switching large amounts of data quickly and efficiently. To prevent slowing down the switching process, this layer should not be burdened with security or traffic control measures or any unnecessary additional equipment.

The primary device at this layer is a high-end layer 3 switch. This device is essentially the backbone of the network and typically connects the users to corporate resources, servers, gateways, and the Internet.

## Chapter Summary

- TCP/IP is not limited to transmission control and Internet protocols; it is an entire suite of protocols that provides data transportation, management, and diagnostic capabilities for networks that use it.
- TCP/IP was started by the Defense Advanced Research Projects Agency (DARPA), a group charged with developing a national communication system. Later, the DARPA-developed ARPANET was turned over to the public, particularly universities. From there, the Internet grew into what it is today—a worldwide commerce and communications network.
- TCP/IP maps to a four-layer network model: Application, Transport, Internetwork, and Network Interface. These layers map to equivalent functions in the OSI reference model.
- The Application layer in the TCP/IP model covers the Application, Presentation, and Session layers of the OSI reference model. The TCP/IP Transport layer maps directly to the OSI Transport layer. The Internetwork layer of the TCP/IP model maps directly to the Network layer of the OSI model. Finally, the Network Interface layer of the TCP/IP model is equivalent to the Data Link and Physical layers of the OSI model.
- The TCP and UDP protocols reside at the Transport layer of the TCP/IP networking model. UDP is an unreliable and connectionless communications protocol that does not guarantee packet delivery. TCP is a reliable and connection-oriented protocol that guarantees packet delivery. TCP uses a three-way handshake to establish a communications link between two points before data transfer. TCP also uses a sliding window to control the flow of packets and the number of acknowledgments between the two hosts.
- Both TCP and UDP use port numbers from 1 to 65,535 to establish their communications between two points. Ports with numbers 1023 and under are Well Known Port numbers, as defined in RFC 1700. These ports describe common Internet services that hosts can use to contact public servers for specific types of services such as Web, FTP, and telnet.
- The Internet Protocol (IP) resides at the Internetwork layer and provides the logical address that can be passed through a router.
- You can use the Ping utility with IP and ICMP to diagnose and troubleshoot network connections. Also, you can use the Trace utility with IP to determine all the hops that a packet makes along its path to a remote TCP/IP host.
- Address Resolution Protocol (ARP) and Reverse ARP (RARP) reside in the Internetwork layer. These protocols allow the TCP/IP host to map the IP address to a MAC address.
- The MAC address is the final leg of communication between hosts. Packets are transmitted via the MAC address to the destination host once the packets arrive at the destination network.

- Routing tables can be created manually and dynamically. Network administrators manually create static routing tables. A manual table requires more administrative overhead but gives the administrator greater control over the routing process. Dynamic updates are provided through routing protocols, which allow the routers to be updated automatically.
- Cisco developed the Three-Layer Hierarchical model to help network administrators design more efficient networks. The model outlines specific functions and devices at three layers. The bottom (or access)layer—gives users entry into the network, typically through a hub or switch. At the intermediate (or distribution) layer, traffic is managed and security is implemented via routers. At the highest (core) layer, traffic is switched quickly and reliably to other corporate resources, to the Internet, and other destinations.

3

---

## Key Terms

**Address Resolution Protocol (ARP)** A protocol that works at the Internetwork layer of the TCP/IP networking model; resolves a known IP address to an unknown MAC address, which is the final leg of communication between the source and destination.

**Advanced Research Projects Agency (ARPA)** The government organization operating in the Department of Defense (DOD) that was responsible for the creation and proliferation of the Internet and the TCP/IP protocol suite.

**Advanced Research Projects Agency Network (ARPANET)** The original name of the Internet.

**Application layer** The TCP/IP layer that corresponds to the Application, Presentation, and Session layers of the OSI model.

**ARP reply** A reply sent by the device that discovers its own IP address in the IP header of the ARP request frame and includes the requested MAC address.

**ARP request** A process used to obtain the correct mapping when a source computer cannot locate a destination MAC address for a known IP address in its ARP table.

**ARP table** A table used by a network device that contains MAC to IP address mappings.

**buffer** A portion of memory used to store information that is being sent or created too fast for a system to process.

**buffering** A method in which devices on a network handle packet flows that exceed their processing capabilities. Packets are stored in a buffer until the system can process them.

**Cisco Three-Layer Hierarchical model** A model that emphasizes good network design and involves the access layer at the bottom, the distribution layer in the middle, and the core layer at the top.

**congestion avoidance** A method by which a system on a network can reduce the flow of packets on the network by sending a message request to the sender to reduce the rate at which packets are being transmitted.

**default gateway** The address to which a host or IP device sends a packet when the destination host is not on its subnet. The default gateway is usually an interface on a router.

**destination unreachable** An ICMP message sent back to the source host when a gateway cannot deliver an IP datagram.

**Dynamic Host Configuration Protocol (DHCP)** A protocol used to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses from a server. DHCP has largely replaced RARP.

**diskless workstation** Workstations configured to download their operating systems from a central server. These workstations typically do not have a hard drive.

**Domain Name System (DNS)** A hierarchical naming service that is used on the Internet and IP networks to provide host name to IP address resolution.

**echo request/reply** The most commonly used ICMP message. ICMP echo request/reply messages are used to check the availability of a remote host and the devices along a network path (intermediate gateways), and to verify the installation of the TCP/IP protocol on the local source host.

**expectational acknowledgment** A TCP acknowledgment process in which the acknowledgment number refers to the next expected sequence number. If the expected sequence is not received within a specific time interval, a retransmission is requested.

**File Transfer Protocol (FTP)** A part of the TCP/IP protocol suite that provides reliable file transfers across the Internet or other TCP/IP networks. FTP uses TCP to transfer files.

**Hypertext Transfer Protocol (HTTP)** A protocol used for communications on the World Wide Web. Web servers are HTTP servers.

**ICMP flood** A large quantity of ICMP echo requests sent to a target device by a malicious person or program in an attempt to crash or greatly reduce the performance of the target device.

**information request/reply** ICMP messages that are typically used to determine the subnet mask used by the destination. This message allows a host to determine the number of the network on which it resides.

**initial sequence number (ISN)** Sequence numbers that allow communicating hosts to synchronize their communications in a TCP three-way handshake. When the communication is initiated, two hosts communicating over TCP will synchronize their initial sequence numbers.

**Internet Control Message Protocol (ICMP)** A protocol in the TCP/IP protocol suite at the Internetwork layer. ICMP messages control and manage IP protocol communications.

**Internet Protocol (IP)** The Network layer (Internetwork layer) protocol that is responsible for logical addressing. This allows data to be routed.

**Internetwork layer** The layer of TCP/IP that is equivalent to the Network layer of the OSI model.

**IP addressing** The process of assigning (unique) IP addresses to devices on the network either by typing them in statically or using a dynamic approach such as RARP or DHCP.

**link-state** A routing protocol that uses cost when calculating the best path between two points. It considers items such as network traffic, router congestion, bandwidth, reliability, and other factors that could affect network performance.

**Network File System (NFS)** A file system associated with the UNIX operating system that allows for network communications between hosts.

**Network Interface layer** In TCP/IP, the layer that is equivalent to the Physical and Data Link layers of the OSI model.

**Packet Internet Groper (Ping)** A troubleshooting utility that uses ICMP to verify that a remote host is currently running and accessible.

**parameter problem** An ICMP message sent whenever incorrect datagram header information is received. The message identifies the octet in the datagram that caused the problem.

**Post Office Protocol version 3 (POP3)** A protocol used by client machines that allows users to download e-mail from an e-mail server.

**redirect** An ICMP message sent to source hosts requesting that they change routes because the one they chose was not optimal. This packet is used to update a source host's internal routing table.

**remote login application (rlogin)** A utility that allows remote computers to connect to other computers or devices.

**Requests for Comments (RFC)** A group of Internet-related documents that specify Internet protocols and standards.

**reset packet (RST)** A packet indicating that the receiver should delete the TCP connection without further interaction.

**Reverse Address Resolution Protocol (RARP)** A protocol used to resolve the client's unknown IP address to the client's MAC address for the final leg of communication between an IP source and destination. RARP clients broadcast a request for their IP address. A RARP server has a table of IP to MAC mappings and responds to the client with a RARP reply.

**routed protocol** A protocol that contains enough OSI Network layer information that its packets can be routed from a source to a remote destination on an internetwork.

**routing protocols** Used to dynamically create routing tables so that routed protocols can route the data.

**routing table** A table used by a router to determine which of its interfaces is connected to the destination network.

**Simple Mail Transfer Protocol (SMTP)** The main protocol that transfers electronic mail on the Internet between e-mail servers.

**Simple Network Management Protocol (SNMP)** A protocol that provides network administrators the ability to centrally control and monitor the network.

**sliding windows** A feature of TCP used to control the flow of communications between two hosts. The size of the TCP sliding window regulates how often acknowledgments will be sent to the transmitting host from the receiving host.

**source quench** An ICMP message request to reduce the rate at which the sender is transmitting packets to the destination. This message is used for flow control, when packets arrive too fast (the receiving host runs out of buffer space for the message), or if the system is near capacity (network is congested).

**TCP/IP** See Transmission Control Protocol (TCP) and Internet Protocol (IP).

**terminal emulation protocol (telnet)** A connection-oriented, Application layer utility that allows TCP/IP clients to log in to a remote system and operate on that system as if the connection between the two were local.

**three-way handshake** The method used by TCP to negotiate a reliable connection between two hosts on a network. This process involves the exchange of three data packets before the communication process begins.

**time exceeded** An ICMP message sent whenever a packet's time-to-live (hop count) reaches zero and the datagram is dropped.

**time-to-live (TTL)** The number of hops (routers) that a packet can make before it is discarded. The router discards a packet when its TTL is zero, which prevents a packet from looping endlessly around the network. Routers normally decrement the packet TTL by 1 before passing the packet to the next router.

**timestamp request/reply** ICMP messages that are used to synchronize clocks by requesting the destination machine's current time of day value, which is given in milliseconds from midnight Universal Time.

**Trace** A utility that uses ICMP messages to determine the path between a source and destination host. Trace can discover all of the hops (routers) along the path between two points.

**Transmission Control Protocol (TCP)** The protocol that guarantees the delivery of a packet by sending an acknowledgment for each window of data received. This protocol operates at the Transport layer and sends its data encapsulated in the IP protocol. TCP communications are considered connection-oriented because TCP negotiates a communication path between hosts on the network.

**Transport layer** The TCP/IP layer that maps directly to the OSI model Transport layer.

**Trivial File Transfer Protocol (TFTP)** A file transfer utility used on the Internet. TFTP uses UDP to transfer files and is therefore less reliable than FTP, which uses TCP in transferring files.

**UDP (User Datagram Protocol)** The protocol that operates at the Transport layer and transports data unreliable over IP. This is sometimes known as connectionless communication because the messages are sent without expectation of acknowledgment. Unlike TCP, UDP has no connection negotiation process. The packets that are sent by UDP are also known as datagrams. Because UDP does not negotiate a connection, it is faster than TCP.

**Well Known Port numbers** TCP and UDP ports from 0 through 1023 on which client applications expect to find common Internet services.

---

## Review Questions

1. Which of the following is a reliable communications protocol?
  - a. UDP
  - b. TCP
  - c. IP
  - d. ICMP
2. Which of the following is used by the TFTP protocol?
  - a. UDP
  - b. TCP
  - c. ICMP
  - d. Telnet
3. Which of the following is a layer in the TCP/IP protocol stack? (Choose all that apply.)
  - a. Application
  - b. Presentation
  - c. Physical
  - d. Data Link
  - e. Internetwork

4. Which of the following is a TCP/IP Application layer protocol? (Choose all that apply.)
- a. DNS
  - b. FTP
  - c. UDP
  - d. IP
  - e. ICMP
5. Which of the following is a TCP/IP Internetwork layer protocol? (Choose all that apply.)
- a. ICMP
  - b. FTP
  - c. DNS
  - d. ARP
  - e. IP
6. Which of the following is a TCP/IP Transport layer protocol? (Choose all that apply.)
- a. ARP
  - b. RARP
  - c. IP
  - d. UDP
  - e. TCP
7. What are the Well Known Port numbers?
- a. 1024–49151
  - b. 49152–65535
  - c. 0–1021
  - d. 1–1023
8. What is the purpose of the three-way handshake?
- a. to establish a reliable connection between two points
  - b. to establish an unreliable connection between two points
  - c. to establish a relationship at the Application layer between two points
  - d. to establish a relationship at the Internetwork layer between two points
9. What is in an ARP table?
- a. destination and source MAC addresses
  - b. MAC and corresponding IP addresses
  - c. destination and source IP addresses
  - d. routes to networks
10. What do computers do with the information in an ARP request when they are not the destination IP?
- a. update their ARP caches with the destination information
  - b. update their ARP caches with the source information

**84** Chapter 3 TCP/IP

- c. update their routing tables with the ARP information
  - d. none of the above
11. Routers pass ARP broadcasts to find MAC addresses on other networks. True or False?
12. An ARP request is a \_\_\_\_\_.
- a. multicast
  - b. unicast
  - c. broadcast
  - d. anycast
13. An ARP reply is a \_\_\_\_\_.
- a. multicast
  - b. unicast
  - c. broadcast
  - d. anycast
14. RARP has largely been replaced by \_\_\_\_\_.
- a. BOOTP
  - b. ARP
  - c. DHCP
  - d. DNS
15. Ping and Trace both rely on what protocol?
- a. SMTP
  - b. DNS
  - c. ICMP
  - d. TFTP
16. When sending packets to remote segments, routers rely on information in \_\_\_\_\_.
- a. ARP tables
  - b. routing tables
  - c. switching tables
  - d. ROM
17. Distance-vector algorithms and link-state algorithms are used in \_\_\_\_\_.
- a. DHCP
  - b. ARP
  - c. static routing
  - d. dynamic routing
18. All computers on the local segment process an ARP request at layer four of the OSI model. True or False?
19. Each interface on a router represents an IP address on a different network. True or False?

20. The TCP acknowledgment process is \_\_\_\_\_.  
a. expectational  
b. sequential  
c. exceptional  
d. sesquicentennial
21. Which of the following are *not* ICMP message types?  
a. Echo & destination unreachable  
b. Source quench & redirect  
c. Relay & reroute  
d. Parameter problem & information  
e. Timestamp & time exceeded
22. Which layer of Cisco's Three-Layer Hierarchical model provides services such as traffic control and security to the network?  
a. Access layer  
b. Distribution layer  
c. Core layer  
d. All layers can provide these functions.  
e. Traffic control and security are not addressed by this model.

3

---

## Case Projects



1. Lisa has to give a presentation regarding the origins of TCP/IP. List five things you think her audience should know about this topic.
2. Moe wants to understand the concept of sliding windows. Explain their purpose to Moe. When should networks use large sliding windows? When should they use smaller sliding windows? What could happen if small data transfers occur in a large sliding window?
3. Moe and Jennifer want you to explain step by step what occurs when a host wants to send a message. Discuss where ARP fits in and how exactly ARP facilitates the communications.
4. Lisa does not understand the purpose of the RARP protocol or the RARP server. Explain to her how RARP works and why a computer might have a MAC address but no IP address.





# 4

chapter

## IP Addressing

**After reading this chapter and completing the exercises, you will be able to:**

- Explain the different classes of IP addresses
- Configure IP addresses
- Subdivide an IP network
- Discuss advanced routing concepts such as CIDR, summarization, and VLSM
- Convert between decimal, binary, and hexadecimal numbering systems
- Explain the differences between IPv4 and IPv6

## IP Addressing

An IP address has 32 bits divided into four octets (four sets of eight binary digits). To make the address easier to read, people use decimal numbers to represent the binary digits. For example, the IP address 192.168.1.1 is 11000000.10101000.00000001.00000001 when written in binary. Notice that 32 binary digits create the address. The lowest number of any octet is 00000000, or zero, and the highest number of any octet is 11111111, or 255. When binary IP addresses are written in decimal format, it is often called dotted decimal notation.

To understand how eight binary ones are equal to the decimal 255, you must look at the places for each of the binary values. Table 4-1 illustrates the places of the binary digits 128, 64, 32, 16, 8, 4, 2, and 1. Notice that the decimal number 192 is created when the first two binary digits are ones and the following six digits are zeros. To determine the decimal equivalent, you add the binary places that are identified by ones. In the first row of Table 4-1, the 128 and 64 places have ones, which creates the decimal number 192 (i.e.,  $128 + 64 = 192$ ).

	128	64	32	16	8	4	2	1
192	1	1	0	0	0	0	0	0
168	1	0	1	0	1	0	0	0
1	0	0	0	0	0	0	0	1
255	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0

**Table 4-1** Binary to decimal conversion

## MAC to IP Address Comparison

The MAC address identifies a specific NIC in a computer on a network, so each MAC address is unique. TCP/IP networks can use MAC addresses in communication. However, network devices could not efficiently route traffic on a large internetwork or on the Internet using MAC addresses; MAC addresses are not grouped logically, they cannot be modified, and they do not give information about physical or logical network configuration. Therefore, another addressing scheme called **IP addressing** was devised for use on large networks. Unlike MAC addresses, IP addresses have a hierarchical structure and do provide logical groupings. The structure of the IP address makes packet routing possible on large internetworks.

You can compare driver's license numbers to MAC addresses. The license allows you to drive a car, and it uniquely identifies you as a vehicle operator. However, when people want to talk with you, they do not call your driver's license number. Instead, they call your phone number, which identifies your location with an area code and other digits specific to you. Similarly, IP addresses identify your computer and the specific network on which it resides. For example, if your IP address is 192.168.1.3, your computer is host 3 on network 192.168.1.0.

Because the IP address identifies both a network and a host, you can route communications through large networks, including the Internet. Routers can send communications in a more efficient manner by using the hierarchical IP address. If the Internet used MAC addresses, huge tables would have to be maintained containing not only the MAC addresses of each and every computer, but also each device along the path to that computer. Clearly, that would be

unmanageable, especially given that network cards can malfunction. Every time someone replaced a network card, the giant MAC table would have to be updated!

## IP Classes

The **Internet Assigned Numbers Authority (IANA)** devised the hierarchical IP addressing structure, and the **American Registry of Internet Numbers (ARIN)** manages IP addresses in the United States. These organizations work in conjunction with the **Internet Corporation for Assigned Names and Numbers (ICANN)**, which is a global, government-independent entity with overall responsibility for the Internet. ICANN has effectively replaced IANA. Five different groups of IP addresses (labeled Class A through E) exist on the Internet. Classes A, B, and C are assigned to governments, companies, schools, and public entities for use on the Internet. Classes D and E are reserved for multicasting and experimentation. Therefore, you will mainly be concerned with managing Class A, B, and C addresses.

4

**Class A** ARIN reserves Class A IP addresses for governments and large corporations throughout the world. Class A addresses, when written in binary format, will always begin with a zero. You can tell what class an Internet address belongs to by looking at its first octet. For example, Class A addresses in decimal notation will have 1 to 126 as their first octet. Figure 4-1 displays the binary digits associated with these decimal numbers.

Binary Place Values								Decimal Equivalent	Description
128	64	32	16	8	4	2	1		
0	0	0	0	0	0	0	0	= 0	Subnet identifier
0	0	0	0	0	0	0	1	= 1	Bottom of Class A range
0	1	1	1	1	1	1	0	= 126	Top of Class A range
0	1	1	1	1	1	1	1	= 127	Loopback address

**Figure 4-1** Class A addresses begin with a number between 1 and 126

Notice that all zeros identify the subnet, which is not a usable IP address. The first Class A address that can be assigned is 1.0.0.0 (decimal) or 00000001.00000000.00000000.00000000 (binary). The last Class A address that can be assigned is 126.0.0.0 in decimal notation, which is 01111110.00000000.00000000.00000000 in binary format.

It seems that 127.0.0.1 (decimal) is the highest assignable Class A address, but that particular address range is reserved as the **loopback address**. The loopback address is widely known as 127.0.0.1, but all addresses with 127 as their first octet are part of the loopback range. You can use the loopback address range for diagnostics, such as ping. If you ping 127.0.0.1 or any other IP address on the 127.0.0.0 network, your internal IP configuration should respond. This response verifies a properly installed TCP/IP protocol suite. Because the entire 127 Class A address is reserved for diagnostics, the highest Class A address that can be assigned is 126. (It is important to note that a successful loopback test does not mean the device can communicate with other devices. You can get a successful loopback response from a computer with no network cable attached to the NIC card.)

Notice that you cannot create a decimal number higher than 127 with eight binary digits if the first digit must be zero. The IANA specified that the first binary digit in a class A address would be zero to separate it from the other four categories (B, C, D, and E).

**90** Chapter 4 IP Addressing

For Class A addresses, the ARIN only assigns the first octet. However, the same is not true for Class B and Class C addresses. Class B addresses are assigned with the first two octets set. Class C addresses are assigned with the first three octets set. This means that there is a difference between the number of hosts that you can assign based on the type of address you are assigned:

- Class A: Each Class A address supports 16,777,214 hosts.
- Class B: Each Class B address supports 65,534 hosts.
- Class C: Each Class C address supports 254 hosts.

Why is there a significant difference in the number of hosts supported? When you are assigned a Class A network, you can use the last three octets for your network hosts. When you use a Class B network, only the last two octets can be used. A Class C address only has a single octet for you to modify.

**Class B** Class B IP addresses are assigned to large- and medium-sized companies. The IANA specifies that Class B addresses will lead with 10 when written in binary format. This means that the range in decimal notation for the first octet of Class B addresses is 128 through 191. Figure 4-2 illustrates the binary to decimal calculations that specify this range.

Binary Place Values									Decimal Equivalent	Description
128	64	32	16	8	4	2	1			
1	0	0	0	0	0	0	0	= 128		First Class B address
1	0	1	1	1	1	1	1	= 191		Last Class B address

**Figure 4-2** Class B addresses begin with a number between 128 and 191

With the first two binary digits of the first octet in the Class B category defined, the address range is limited. When the last six configurable bits of the first octet are set to zero, the lowest configurable number is obtained (128). When those same six digits are set to one, the highest configurable number is set (191).

**Class C** Class C IP addresses are assigned to groups that do not meet the qualifications to obtain Class A or B addresses. The IANA specified that the first three binary digits of a Class C address must be 110, which means that Class C addresses can range from 192 through 223 in decimal notation. Figure 4-3 illustrates the binary to decimal equivalents for the Class C addresses.

Binary Place Values									Decimal Equivalent	Description
128	64	32	16	8	4	2	1			
1	1	0	0	0	0	0	0	= 192		First Class C address
1	1	0	1	1	1	1	1	= 223		Last Class C address

**Figure 4-3** Class C addresses begin with numbers between 192 and 223

In Class C addresses, the last five digits are configurable. The graphic shows that when the last five digits are set to all zeros, the decimal equivalent is 192. When those same five digits are set to binary ones, the decimal equivalent is 223.

**Class D** Class D addresses (also known as **multicast addresses**) are reserved for multicasting. **Multicasting** is the sending of a stream of data (usually audio and video) to multiple computers simultaneously. Compared to broadcasting, this saves bandwidth. Many routers forward multicasts, and computers configured to receive the multicast information accept the packets and can receive the data stream. Because Class D addresses must have 1110 as their first four binary digits, the range for Class D starts with decimal 224 and ends at 239 in the first octet. Figure 4-4 illustrates the binary and decimal range for Class D addresses.

4

Binary Place Values		Decimal Equivalent	Description						
128	64	32	16	8	4	2	1		
1	1	1	0	0	0	0	0	=	224
1	1	1	0	1	1	1	1	=	239
									First Class D address
									Last Class D address

**Figure 4-4** Class D addresses begin with a number between 224 and 239

**Class E** The IANA reserved Class E addresses for research, testing, and experimentation. The Class E range starts where Class D leaves off. Figure 4-5 illustrates the first address in the “experimental” range as 240. The top of the range is 255, which is the highest possible 8-bit number. Therefore, Class E defines 240 to 255 (decimal) as the first octet.

Binary Place Values		Decimal Equivalent	Description						
128	64	32	16	8	4	2	1		
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	1	1	1	=	255
									First Class E address
									Last Class E address

**Figure 4-5** Class E addresses begin with a number between 240 and 255

**Private IP Ranges** Many companies today use private IP addresses for their internal networks. This prevents the organizations from having to obtain official IP addresses from their ISP every time they add a host to the network. Class A, B, and C private address ranges have been defined by RFC1918 ([www.faqs.org/rfcs/rfc1918.html](http://www.faqs.org/rfcs/rfc1918.html)). Table 4-2 illustrates the private IP address ranges that network administrators can use. If these private ranges are used for an internal network, they will not be routable on the Internet. This is fine for most organizations because they have one or more gateway devices (such as routers, firewalls, or proxy servers) that provide connectivity to the Internet. These gateway devices have network interface connections to both the internal network and the Internet and route packets between them (thereby providing Internet connectivity to internal clients). The company will simply have to obtain one or more official IP addresses if it chooses to provide services (like an organizational Web site) to people using the Internet.

Class	Private Address Range
A	10.x.x.x
B	172.16.x.x – 172.31.x.x
C	192.168.x.x

**Table 4-2** The private IP ranges

## Network Addressing

As previously mentioned, IP addresses identify both the network and the host. However, the division between the two is not specific to a certain number of octets. In an earlier example, the IP address 192.168.1.3 was used to illustrate that 192.168.1.0 was the network and 3 was the host identifier on that network. This suggests that the first three octets comprise the network identifier and the last octet is the host identifier, but that is not always true. In fact, the network portion can be as small as the first octet or as large as 30 of the 32 binary digits of the IP address.

How do you determine how many digits are used for the network identifier? You must look at the **subnet mask**, which is a required component for all IP hosts. On every TCP/IP network, hosts must have both an IP address and a subnet mask. The subnet mask indicates how much of the IP address represents the network or **subnet** (short for subnetwork). Standard (default) subnet masks are as follows:

- Class A subnet mask is 255.0.0.0 or 11111111.00000000.00000000.00000000
- Class B subnet mask is 255.255.0.0 or 11111111.11111111.00000000.00000000
- Class C subnet mask is 255.255.255.0 or 11111111.11111111.11111111.00000000

Notice that Class A addresses come with the first octet masked, Class B addresses have the first two octets masked, and Class C addresses have the first three octets masked.

The mask is essentially a continuous string of binary one digits. TCP/IP hosts use the combination of the IP address and the subnet mask to determine if other addresses are local or remote. The binary AND operation is used to perform the calculation. The binary AND operation is simple—each of the 32 binary digits in the IP address is compared with the corresponding digit on the subnet mask to arrive at the ANDing result. One and one results in one, and all other combinations result in zero. When devices AND the IP address with the corresponding subnet mask, the network (or subnetwork) number is the result. Computers and routers use the AND computation to determine the subnet identifier for each IP address. If the subnet identifier for the local IP address is the same as that of the IP address to which it wants to communicate, then the packet is sent on the local subnet (ARP is used, as necessary, to locate the destination MAC address on the local subnet). However, if the subnet identifiers are different, then the packet is sent to the default gateway (usually the local router) to be routed to the remote subnet. Figure 4-6 illustrates ANDing.

In the figure, the first comparison uses the subnet mask 255.255.255.0, which defines the first three octets as the network identifier. A quick look will tell you that these hosts are on

Source IP:	64.168.1.1	01000000.10101000.00000001.00000001
Subnet mask:	255.255.255.0	11111111.11111111.11111111.00000000
ANDing result:	64.168.1.0	01000000.10101000.00000001.00000000
Destination IP:	64.168.5.7	01000000.10101000.00000101.00000111
Subnet mask	255.255.255.0	11111111.11111111.11111111.00000000
ANDing result:	64.168.5.0	01000000.10101000.00000101.00000000
When the mask 255.255.255.0 is used the hosts are remote.		
Source IP:	64.168.1.1	01000000.10101000.00000001.00000001
Subnet mask:	255.255.0.0	11111111.11111111.00000000.00000000
ANDing result:	64.168.1.0	01000000.10101000.00000000.00000000
Destination IP:	64.168.5.7	01000000.10101000.00000101.00000111
Subnet mask	255.255.0.0	11111111.11111111.00000000.00000000
ANDing result:	64.168.5.0	01000000.10101000.00000000.00000000
When the mask 255.255.0.0 is used the hosts are local.		

4

**Figure 4-6** ANDing operations

two different subnets. Notice that the first three octets from the ANDing result of the source host are 64.168.1, while those of the destination host are 64.168.5. This means that the source is on subnetwork 64.168.1.0 and the destination is on subnet 64.168.5.0. The source host will have to send communications for 64.168.5.7 through its default gateway.

Now consider the calculations shown on the bottom half of Figure 4-6. The subnet mask has been changed to 255.255.0.0. Given this configuration, the two hosts are on the same subnet because the network identifier in this case is 64.168.0.0 for both. This means that the source host would use ARP, if necessary, to determine the MAC address of host 64.168.5.7 and then transmit its data to that MAC address. Notice that in both of these examples, the default mask is not used. The 64 in the first octet identifies this as a Class A address, which would have a default subnet mask of 255.0.0.0. This means the network administrator has manipulated the mask to get more network numbers. This is called **subnetting** and is discussed later in this chapter.

**Subnet Address** If you look at the preceding network and host number divisions, you will notice that the network is identified by the first, or first few, octets. Notice that after the masked portion of the subnet mask, the network identifier changes to zero(s). For example, the network identifier of a host that has IP address 192.168.23.45 with subnet mask 255.255.255.0 is 192.168.23.0.

One of the IP networking rules stipulates that a TCP/IP host must have a nonzero host identifier. From this information, you can determine that on a subnet using mask 255.255.255.0, the IP address 222.12.150.4 is a valid host IP address. However, the address 222.12.150.0 is not a host address, but a network identifier. In other words, you could not assign 222.12.150.0 to a computer.



NOTE

Do not expect all subnetwork identifiers to end in a decimal zero. It is true that subnetworks are identified by all the binary digits in the host portion being zero, but this does not mean that the entire last octet will be zero. For example, 199.192.65.32 could be a subnetwork identifier using subnet mask 255.255.255.224. In this case, the host identifier will be the last five binary digits of the last octet. Because 32 is 00100000 in binary, the final five digits are all zero, which indicates the subnetwork. This concept is described in greater detail as the chapter progresses.

**Broadcast Address** IP addressing has another rule that you must commit to memory. On any subnet, when the entire host portion of an IP address is all binary ones, it is a broadcast to all of the computers on that segment. For example, on subnet 192.168.1.0, the IP address 192.168.1.255 is a broadcast. This also can apply to larger subnetworks such as 190.55.0.0; the IP address 190.55.255.255 is a broadcast on that network.

Converting these addresses into binary digits can quickly show if an IP address is a broadcast. If all the binary digits in the host identifier are ones, the address is a broadcast. Figure 4-7 illustrates a broadcast address for a subnet.

Subnet ID:	199.192.65.0	11000111.11000000.01000001.00000000
Subnet mask:	255.255.255.0	11111111.11111111.11111111.00000000
Broadcast Address:	199.192.65.255	11000111.11000000.01000001.11111111

**Figure 4-7** Broadcast addresses

By looking at Figure 4-7, you can quickly determine the broadcast address (199.192.65.255) because the decimal 255 represents eight binary ones. The binary calculation is not necessary if you know that all bits in the octet that represents the host portion are ones. However, the determination is not so easy when an octet is partially masked, as shown in Figure 4-8.

Subnet ID:	199.192.65.32	11000111.11000000.01000001.00100000
Subnet mask:	255.255.255.224	11111111.11111111.11111111.11100000
Broadcast Address:	199.192.65.63	11000111.11000000.01000001.00111111

**Figure 4-8** Broadcasts on partially masked octets

In Figure 4-8, you can see that subnetwork identifiers do not always end in a zero decimal value. In this case, the last octet has been partially masked (three binary places), leaving the last five binary digits of the last octet to represent the host identifier. In decimal format, it may be difficult to determine that 199.192.65.63 is a broadcast address for the subnet 199.192.65.32, but in binary format, it is much easier. You can see that the last five binary digits are all ones, which indicates a broadcast on the local subnet.

Notice how important the subnet mask is in determining the logical subdivision of the network. For example, if the subnet mask in Figure 4-8 were 255.255.255.0 instead of 255.255.255.224, the broadcast address would not be 199.192.65.63. Instead, 199.192.65.255 would be the correct broadcast address.

## Broadcast Types

The two different types of broadcasts are flooded and directed. **Flooded broadcasts** are broadcasts for any subnet and use the IP address 255.255.255.255. A router does not propagate flooded broadcasts because they are considered local. When a host sends a packet to the IP address 255.255.255.255, the packet remains on the local subnet.

On the other hand, **directed broadcasts** are for a specific subnet. Routers can forward directed broadcasts. For example, a packet sent to the Class B address 129.30.255.255 would be a broadcast for network 129.30.0.0. The router would forward that packet to the identified network. For security purposes, directed broadcasting is often disabled on a router.

4

## Subdividing IP Classes

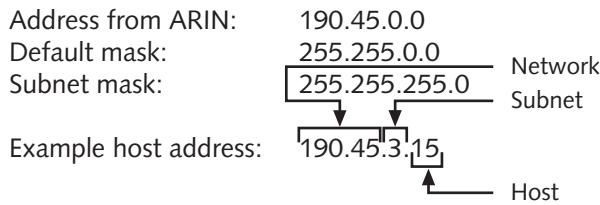
By now, you know that ARIN assigns Class A, B, and C addresses. You have also seen how these address groups can be further subdivided into subnetworks. Organizations that are not connected to the Internet can define their own subnets in any way they desire. In this section, we will look closer at how networks can be logically segmented using IP subnets.

When a private organization decides to subnet its network identifier, the outside world does not see a difference in the organization; only the internal structure of the organization's network changes. An organization may decide to subnet for various reasons:

- To match the physical layout of the organization—A group may want to configure the network to mirror the organizational structure. For example, if the company occupies a six-storey building with 30 hosts per floor, the network administrator may create six different subnets, one for each floor.
- To match the administrative structure of the organization—Some organizations may choose to divide their network by administrative structure. For example, the administrator might subdivide the network by department. Each department could have its own subnetwork.
- To plan for future growth—A network administrator who foresees and plans for organizational growth may decide to subnet the network based on that expectation.
- To reduce network traffic—This is one of the most common reasons to divide an IP network into smaller subnetworks. Because routers are required for each network division, the number of routers on the network must increase when subnetting occurs. Typically, routers do not forward broadcast traffic, which means that there will be less broadcast traffic on the network. Routers, as their name implies, also route packets along a path instead of broadcasting them to all hosts on a segment. Overall, this equates to a more efficient use of the network and a corresponding reduction in network traffic.

As an example, assume that a private organization had the Class B address 190.45.0.0; the network manager of this organization might decide to subnet the Class B address to mirror the internal administrative structure of the organization. This decision would not affect the external network (Internet); it would only influence the structure of the network inside the private organization. The organization's internal routers would be responsible for handling inbound communications for that Class B address.

You can divide the 190.45.0.0 address by adding 255 to the third octet of the subnet mask. By default, the subnet mask for a Class B address is 255.255.0.0, but the network administrator might decide to use 255.255.255.0. Figure 4-9 illustrates what the subnetting does to the Class B address.

**96** Chapter 4 IP Addressing**Figure 4-9** Dividing a Class B network

The example address in the figure shows how the different octets can be broken out. Notice that the third octet now defines the subnet. By masking the third octet, the administrator can create 254 different subnetworks, each of which can contain 254 hosts.

## Subnet Masking

When network administrators create subnets, they borrow bits from the original host field to make a set of subnetworks. The number of borrowed bits determines how many subnetworks and hosts will be available. Whenever you subnet a network address, you lose some of the host addresses that you could have had without the subnetting. For instance, in the example from the previous section, the network administrator divided the Class B address 190.45.0.0 by masking the third octet. You know from the previous section that Class B addresses support 65,534 hosts. However, masking the third octet allows room for only 254 subnetworks, each containing 254 hosts. This means that the number of addresses is reduced to 64,516 ( $254 \times 254$ ). Table 4-3 illustrates the types of subnet masks that can be used and how these masks affect the number of hosts available per subnet.

Subnet Mask	Subnets on Network	Hosts per Subnet
255.255.128.0	2	32,766
255.255.192.0	4	16,382
255.255.224.0	8	8,190
255.255.240.0	16	4,094
255.255.248.0	32	2,046
255.255.252.0	64	1,022
255.255.254.0	128	510
255.255.255.0	256	254
255.255.255.128	512	126
255.255.255.192	1,024	62
255.255.255.224	2,048	30
255.255.255.240	4,096	14
255.255.255.248	8,192	6
255.255.255.252	16,384	2

**Table 4-3** Class B subnet masks



When the host portion of an IP address is all binary zeros, that address is the subnetwork identifier. When the host portion of an IP address is all binary ones, that address is a broadcast address.



The network administrator can use up to 14 bits to subnet a Class B address. Two bits must be left for host numbers.



Class C addresses also can be subdivided, but not as many options or available masks exist because only the last octet can be manipulated with this class. Table 4-4 illustrates the six available subnet masking options for Class C addresses.

Subnet Mask	Subnets on Network	Hosts per Subnet
255.255.255.128	2	126
255.255.255.192	4	62
255.255.255.224	8	30
255.255.255.240	16	14
255.255.255.248	32	6
255.255.255.252	64	2

**Table 4-4** Class C subnet masks



The network administrator can use up to six bits of the last octet to subnet the Class C address. Two bits must be left for host numbers.

Each example in Table 4-4 follows a pattern in the last octet. If you refer to Table 4-3, you will see the same numbers in the last masking octet in those examples. This pattern exists because subnet masks must have continuous binary one digits from the left side. Figure 4-10 illustrates the possible binary combinations that can be used as subnet masks.

Binary Place Values →

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

Binary Digits ↓

Decimal Equivalents ↓

- =128
- =192
- =224
- =240
- =248
- =252
- =254
- =255

**Figure 4-10** Subnet mask values

The subnet masks have a clear binary pattern. They must have a continuous string of ones from the left side of the octet. Such a table would be easy to re-create, if you remember the binary places at the top. Then, you need only to add up the binary places to get their decimal equivalents. For example, the mask 11000000 can be calculated by adding binary places 128 and 64 ( $128 + 64 = 192$ ).

## Learning to Subnet

The best way to learn to subnet a network is to use a Class C address. A Class C address only allows the administrator to subnet the last octet. Also, as Table 4-4 shows, you can use only six different numeric masks on the last octet of a Class C address.

Suppose you had a network with five different segments and somewhere between 15 and 20 TCP/IP hosts on each network segment. You just received your Class C address from ARIN (199.1.10.0). Refer to Table 4-4 to decide which subnet mask you will use. Notice that only one subnet mask can handle your network configuration: 255.255.255.224. This subnet mask will allow you to create eight subnetworks and to place up to 30 hosts per network. The other subnet masks will give you either too few subnetworks or too few hosts.

Deciding on the subnet mask is fairly straightforward. You just select the mask that meets your needs. Your next task is to assign the addresses to your network. You must find the IP address of each subnet identifier and a valid range of IP addresses for each subnet. A quick way to determine the subnet identifiers (IP addresses) is to write the last masking octet as a binary number. Then, you can determine the binary place of the last masking digit, as shown in Figure 4-11.

Class C Address: 199.1.10.0  
 Standard Mask: 255.255.255.0  
 Selected Mask: 255.255.255.224

	128	64	32	16	8	4	2	1
224	1	1	1	0	0	0	0	0

**Figure 4-11** Subnet masking example

Notice that the last masking digit in this example occupies the binary place of 32. To calculate the subnets, begin with the major network number (subnet zero) and increment by 32. Stop counting when you reach the value of the mask (224):

- 0 (binary 00000000)
- 32 (binary 00100000)
- 64 (binary 01000000)
- 96 (binary 01100000)
- 128 (binary 10000000)
- 160 (binary 10100000)
- 192 (binary 11000000)
- 224 (binary 11100000)

Next, you must determine the valid ranges for your hosts on each subnet. These are IP addresses that can be configured on the computers on your network. For this operation, you need only take the ranges between each subnet identifier. In doing this, you must remember to remove the broadcast address for each subnet from the list of valid ranges. Each subnet has a broadcast address; it is the last number before the start of each new subnet, because the last number is equivalent to placing all binary ones in the host portion of the IP address. Table 4-5 illustrates the subnet identifier, valid host range, and broadcast address for each subnet.

4

Subnet Identifier	Valid Host Range	Broadcast Address for Subnet
199.1.10.0	199.1.10.1 – 199.1.10.30	199.1.10.31
199.1.10.32	199.1.10.33 – 199.1.10.62	199.1.10.63
199.1.10.64	199.1.10.65 – 199.1.10.94	199.1.10.95
199.1.10.96	199.1.10.97 – 199.1.10.126	199.1.10.127
199.1.10.128	199.1.10.129 – 199.1.10.158	199.1.10.159
199.1.10.160	199.1.10.161 – 199.1.10.190	199.1.10.191
199.1.10.192	199.1.10.193 – 199.1.10.222	199.1.10.223
199.1.10.224	199.1.10.225 – 199.1.10.254	199.1.10.255

**Table 4-5** Class C address 199.1.10.0 masking 255.255.255.224

As first described in Table 4-4 and shown in Table 4-5, there are eight available networks with 30 available hosts per network. One address on each subnet is the subnetwork identifier, and one is the broadcast address for that subnet. Notice that the masking digits in the last octet cover the first three binary digits, as shown in Figure 4-12. Each valid subnet in the list has a different combination of the first three binary digits.

Binary				Binary			
Decimal Mask	0 224	000 00000 111 00000		Decimal Mask	32 224	001 00000 111 00000	
Decimal Mask	64 224	010 00000 111 00000		Decimal Mask	96 224	011 00000 111 00000	
Decimal Mask	128 224	100 00000 111 00000		Decimal Mask	160 224	101 00000 111 00000	
Decimal Mask	192 224	110 00000 111 00000		Decimal Mask	224 224	111 00000 111 00000	

**Figure 4-12** A binary look at the mask



Automated subnet calculators on the Internet are quite useful for determining the number of subnets versus the number of hosts. One example is the IP Subnet Calculator from WildPackets ([www.wildpackets.com](http://www.wildpackets.com)).

NOTE

## Subnetting Formulas

If you take an exam on IP subnetting, you probably will not be permitted to use a subnet calculator. Although you can write the numbers out in binary format and create tables to determine the subnet identifiers and ranges, you can also use formulas to solve these problems. Consider memorizing the following two formulas:

- $2^y = \# \text{ of usable subnets}$  (where  $y$  is the number of bits borrowed)
- $2^x - 2 = \# \text{ of usable hosts per subnet}$  (where  $x$  is the number of bits remaining in the host field after borrowing)



Most router internetworking operating systems (IOS) in use today support the use of the first and last subnet. This is referred to as "supporting subnet zero." If you are using an older IOS, you must subtract 2 when calculating the number of usable subnets.

NOTE

To demonstrate how these formulas can be used, assume that you have the subnet mask 255.255.255.240 on your Class C network address of 199.4.10.0. To determine the number of subnets, you would figure out how many masked bits (borrowed bits) exist in the final octet, as shown in Figure 4-13.

C Address	199.4.10.0	11000111.11000000.01000001.00000000
Standard mask	255.255.255.0	11111111.11111111.11111111.00000000
Mask	255.255.255.240	11111111.11111111.11111111.11110000
		y = 4 (borrowed bits)
		x = 4 (bits left in host field after borrowing)
<b>Formulas:</b>		
$2^y = \# \text{ of usable subnets}$		
$2^x - 2 = \# \text{ of usable hosts per subnet}$		
$2^4 = 16 \text{ usable subnets}$		
$2^4 - 2 = 14 \text{ usable hosts per subnet}$		

**Figure 4-13** Sample calculation using formulas

Figure 4-14 illustrates the subnets created when the Class C address 199.4.10.0 is used with the subnet mask 255.255.255.240. Notice that the last octet of the subnet increments by the decimal value of the right-most significant binary digit in the mask, which in this case is 16.



Refer back to Figure 4-6 for an illustration of ANDing.

NOTE

Below is a list of the last octets for the 16 subnets created from network number 199.4.10.0 with the subnet mask 255.255.255.240

0	128
16	144
32	160
48	176
64	192
80	208
96	224
112	240

Subnetwork numbers will increment by 16, as it is the decimal equivalent of the right-most significant digit in the mask

4

**Figure 4-14** 255.255.255.240 subnet mask

## CIDR

**Classless Inter-Domain Routing (CIDR)** was developed to slow the exhaustion of IP addresses. It is based on assigning IP addresses on criteria other than octet boundaries. It became apparent in the mid-1990s that this address space was becoming depleted, mostly because IP addresses were being wasted. For example, a Class C address provides 254 host addresses, which is clearly not enough for many large businesses. On the other hand, an unsubnetted Class B address provides over 65,000 IP addresses, which is usually far more than necessary on any one network, so the unused addresses are wasted. The CIDR addressing method allows the use of a **prefix** to designate the number of network bits in the mask. The prefixes allow a more flexible assignment of IP network numbers. For example, a company may be assigned the IP network of 200.16.1.48 /25. The prefix of 25 means that the first 25 bits in the mask are network bits, in other words, “1s.” In binary, the mask is 11111111.11111111.11111111.10000000. In decimal, the mask is 255.255.255.128. It is much easier to express the mask as a prefix, which is the CIDR notation. CIDR notation is also known as bit-count notation because the number of “1s” in the mask are counted and displayed. The prefix can be longer than the default subnet mask (subnetting) or it can be shorter than the default mask (**supernetting**).

The allocation of network numbers based on CIDR has helped slow the depletion of addresses. CIDR is now used by all backbone routers and most ISPs. However, knowledge of the original class system is essential to understand subnetting and CIDR.

## Summarization

**Summarization** is also known as route aggregation. It is also sometimes called supernetting. This is because the network/node boundary in the subnet mask moves to the left with supernetting, rather than to the right as with subnetting. The purpose of summarization is to allow many IP subnets to be advertised as one. This reduces the number of entries in the router’s routing table. Large routing tables are a concern because they negatively affect router performance. Deciding how to summarize a group of subnets is relatively straightforward.

You simply count the number of bits that are common to all of the networks you want to advertise, and then you use the prefix that identifies the number of common bits. For example, Table 4-6 shows four subnets in both decimal and binary that can be summarized.

Decimal	Binary Equivalent
213.64.132.0 /24	11010101.01000000.10000100.00000000
213.64.133.0 /24	11010101.01000000.10000101.00000000
213.64.134.0 /24	11010101.01000000.10000110.00000000
213.64.135.0 /24	11010101.01000000.10000111.00000000

**Table 4-6** Example summarization

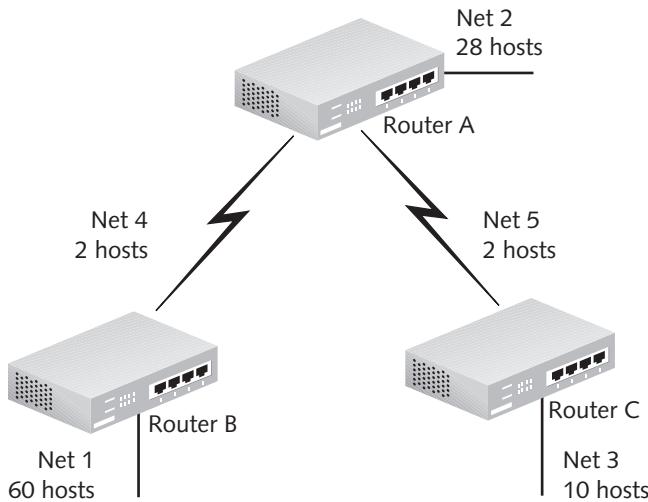
Rather than advertising the Class C addresses as four separate networks, the router on the edge of this internetwork could be configured to advertise network 213.64.132.0 with a shorter prefix that includes all four networks. Notice that the first 22 bits of the four network addresses are the same. This means all four of these networks can be advertised in the summary route 213.64.132.0 /22. Configuration of summary routes is considered an advanced routing concept, but it may be covered on the CCNA exam.

## Variable Length Subnet Masks

Subnet masks tell the computer or router which part of an IP address is the network portion and which part is the host portion. Manipulating the mask via subnetting is a big improvement over using the traditional fixed-length mask because it allows a single major network number to be subdivided into smaller subnetworks. The problem with basic subnetting is that once the new mask is formulated, that same mask must be used on every one of the subnets—it is a “one-size-fits-all” design. For example, if you subnet to accommodate 254 hosts on each subnet, you will waste 252 of those IP addresses on a point-to-point WAN link where you only need two addresses.

**Variable length subnet masking (VLSM)** solves this problem by allowing different masks on the subnets. Essentially, this is done by subnetting the subnets. Basic routing protocols such as RIP version 1 and IGRP do not support VLSM because they do not carry subnet mask information in their routing table updates. More advanced routing protocols such as RIP version 2, OSPF, and EIGRP support VLSM because they do carry subnet mask information inside their routing table updates.

Figure 4-15 shows an internetwork that would benefit from VLSM because of large variations in the number of host IP addresses necessary on each of the different subnetworks.



**Figure 4-15** Example internetwork for VLSM

In this example we see that, assuming no growth, five subnetworks are necessary. The network requiring the most IP addresses is Net 1, with 60 hosts. On RIP version 1 and IGRP networks, which are **classful**, the major network number 192.168.59.0 is sized for 60 hosts, but there are problems. Although we have enough host bits to cover the maximum number of hosts on any of our subnetworks, there are not enough bits to create the five subnetworks. Recall that the formula to calculate the number of subnets is  $2^y$ , where  $y$  equals the number of bits borrowed. The four subnet numbers ( $2^2=4$ ) will be 192.168.59.0, 192.168.59.64, 192.168.59.128, and 192.168.59.192 /26. Obviously, we are one subnet short. In addition, on the networks other than Net 1, far fewer IP addresses are necessary, thus many of the 62 available IP addresses per subnet will be wasted. This is especially true on Nets 4 and 5, which are point-to-point links. Only two host addresses per subnet are needed on these two networks, so the other 60 IP addresses on each of these subnets will be wasted.

The problems are solved if a **classless** routing protocol, such as RIP version 2, OSPF, or EIGRP, is used instead of RIP version 1 or IGRP. In a classless world, the routing updates carry subnet mask information and allow different masks to be used on different subnets. Using VLSM with classless routing protocols will allow us to subnet our subnets. This will not only provide many more usable subnets, it will also enable us to more efficiently allocate the IP addresses.

We begin as we did previously by sizing for the subnet with the largest number of hosts—Net 1. The formula to calculate the number of hosts per subnet is  $2^x-2$ , where  $x$  represents the number of host bits left in the host portion after bit borrowing has taken place. Two host IP addresses still must be reserved; one for the subnet number itself, and one for the broadcast address. So,  $x$  equals 6 and  $y$ , which is the number of bits borrowed, equals 2. The subnet numbers we create by borrowing two host bits for subnetting are 192.168.59.0, 192.168.59.64, 192.168.59.128, and 192.168.59.192 /26, and they will each support 62 hosts. After you figure the subnetting scheme for the maximum number of hosts, you can then take the remaining subnets and further subnet them to provide a subnet that supports the correct number of hosts.



The use of subnet zero is on by default in all versions of Cisco IOS 12.0 or later. On routers with earlier IOS versions, support for using subnet zero can be enabled with the `ip subnet-zero` command.

NOTE

Using VLSM, we assign the first subnet, 192.168.59.0, to Net 1, which needs almost all of the 62 available IP addresses. Next, the second available subnet will be further subnetted to accommodate Net 2 with 28 hosts and Net 3 with 10 hosts. The second subnet is 192.168.59.64. Net 2 must accommodate 28 hosts so  $2^x - 2$  must equal at least 28. In this case, substituting 5 for  $x$  will produce  $2^5 - 2 = 30$  hosts on a subnet. Presently, there are six bits in the host portion from the first round of subnetting; now we need only five bits, so we can give up one more bit for subnets—in other words,  $y=1$ . Therefore, we can create  $2^1 = 2$  new subnets from this second original subnet. The first new subnet will have the same starting value as the original, 192.168.59.64, and end at 192.168.59.95, but it will have a different mask, /27. Remember, originally two bits were borrowed, extending the mask from the default of /24 to /26. Now, we borrow one more bit, so the mask moves one more to the right to /27. This means our new second network will increment by 32 and not 64. The second subnet number is 192.168.59.96 /27. Each of these subnets provides 30 hosts, which is enough for Net 2 with 28 hosts and Net 3 with 10 hosts. So, Nets 1, 2, and 3 are taken care of and we have two of the original subnets left (192.168.59.128 and 192.168.59.192 /26). It would be more efficient to further subnet 192.168.59.128 /26 and assign the new subnets to Net 4 and Net 5. This will not only conserve IP addresses, it will leave the last original subnet (192.168.59.192 /26) unassigned so it can be used at a later date for growth if necessary.

So, we begin with the third original subnet, 192.168.59.128 /26. We need only two host addresses on each of the last two subnets (Net 4 and Net 5), so  $2^x - 2 = 2$ , meaning  $x=2$ . Because only two bits are required in the host portion, we can move our mask to the right by four more bits, making it /30. Now,  $y=4$  and we get  $2^4 = 16$  more subnets, each with only two host IP addresses available.



The /30 mask is preferred on WAN links and is often referred to as the “serial mask.”

NOTE

The first new subnet will be the same as the original 192.168.59.128 but with a different mask, /30. The new subnets will increment by four, as that is the value of the last bit borrowed. The new subnets are shown in Table 4-7.

192.168.59.128 /30	192.168.59.160 /30
192.168.59.132 /30	192.168.59.164 /30
192.168.59.136 /30	192.168.59.168 /30
192.168.59.140 /30	192.168.59.172 /30
192.168.59.144 /30	192.168.59.176 /30
192.168.59.148 /30	192.168.59.180 /30
192.168.59.152 /30	192.168.59.184 /30
192.168.59.156 /30	192.168.59.188 /30

**Table 4-7** VLSM subnets created from 192.168.59.128 /26

Table 4-8 displays the entire IP scheme for Figure 4-15. It is important to note that the VLSM IP scheme presented in this example is just one of many ways VLSM could have been implemented to solve the problem presented by classful routing.



Classless routing protocols that support VLSM such as OSPF and EIGRP are explained in greater detail in Chapter 8.

**NOTE**

4

Major Network	Original Subnets	Subnetted Subnets Using VLSM	Subnet Assignments
192.168.59.0 /24	192.168.59.0 /26		Net 1
	192.168.59.64 /26	192.168.59.64 /27	Net 2
		192.168.59.96 /27	Net 3
	192.168.59.128 /26	192.168.59.128 /30	Net 4
		192.168.59.132 /30	Net 5
		192.168.59.136 through 192.168.59.188	Reserved
	192.168.59.192 /26		Reserved

**Table 4-8** VLSM IP scheme for 192.168.59.0

## Working with Hexadecimal Numbers

The decimal number 192 expressed in binary is 11000000. It takes eight binary digits to express the three-digit decimal number 192. The reason is that decimal numbers can be expressed with up to 10 numerals (0–9), while binary numbers can only be expressed with two (0 and 1). The higher the quantity of numerals in a numbering system, the fewer digits it takes to express any given number. Decimal number systems have 10 numerals, which is why decimal is referred to as base 10. Binary number systems have two numerals, and binary is referred to as base 2.

The hexadecimal numbering system is base 16; in other words, 16 numerals are used to express any given number. These numerals include 0 through 9 as well as A through F. Because more numerals are available in hexadecimal, it is logical that any given number can be expressed with fewer hexadecimal numerals than with either binary or decimal. For example, the decimal number 192 is C0 in hexadecimal.

Why should you be concerned with hexadecimal numbering? Often you will come across hexadecimal numbers when working with computers and networking. For example, the MAC address is a 12-digit hexadecimal number. Another example is the color displayed on your TV and computer monitors. The colors are coded using two-digit hexadecimal numbers. Another common use of hexadecimal numbering occurs in packet sniffing. Sniffers placed on the network to capture packets usually display much of the capture information in hexadecimal. In addition, memory addresses are displayed in hexadecimal. Most importantly, computers typically process information in 8-bit chunks (bytes). It is easier to express those eight bits with two hex digits.

## 106 Chapter 4 IP Addressing

You have already learned how to convert binary numbers to decimal numbers and vice-versa. Now you will learn how to convert between hexadecimal and the other systems. The easiest way to convert a decimal number into a hexadecimal number is to convert the decimal number to binary first. This is because each group of four binary digits equals one hex digit; that hex digit will be between 1, which is 0001 in binary, and 15, which is 1111 in binary. Table 4-9 lists the 16 hexadecimal numerals and their binary and decimal equivalents.



Four bits, which is half of a byte, is also called a **nibble**.

**NOTE**

Binary	Hexadecimal	Decimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

**Table 4-9** Binary to hex to decimal conversion

Let us look at a few conversion examples. As stated earlier, the decimal number 192 is equal to 11000000 in binary. We know that there are four binary digits for each hex digit, so let us group the eight binary digits above into two sets of four digits and write it as 1100 0000, two nibbles. Now all we have to do is treat each set of four binary digits as its own separate hex number. The first set of four binary digits equals 12 ( $8+4$ ) and the second set of four digits equals 0. Table 4-9 indicates that a binary 1100, which is the same as a decimal 12, is equal to a hexadecimal C. A zero in binary is a zero in decimal as well as hexadecimal. We simply put the C and the 0 together to get C0, which is the hexadecimal equivalent of 192.

What if you are given a binary number for conversion that cannot be grouped by four digits (for example the binary number 100011, which has only six digits)? In this instance, you should add enough leading zeroes to the binary number to make even groups of four digits. Thus, you would express 100011 as 00100011. (The value of any number does not change when you add leading zeroes.) Next, you can split the binary number into two groups of four digits: 0010 0011. The first four digits are equivalent to a hex 2, and the second four digits are equivalent to a hex 3. Therefore, the binary number 100011 is equal to the hex number 23. How do you know that the expressed number 23 is not a decimal number instead of a hex number? Often hex numbers are displayed with a small letter “h” after the number for clarity. Another way to explicitly indicate that a number is a hex number is to place a “0x” before the hex number. So the hex number 23 would be expressed as either 23h or 0x23.

4

When converting from hexadecimal to binary, we simply pull the hex digits apart and use four binary digits to represent each hexadecimal digit. For example, 3E9 is equivalent to 0011 1110 1001 in binary. To go directly from hexadecimal to decimal, recall that the hexadecimal numbering system is base 16. This means that each place value is a factor of 16. This means that 3E9 is equal to  $3 \times 16^2 + 14 \times 16^1 + 9 \times 16^0$ , which equals  $3 \times 256 + 14 \times 16 + 9 \times 1$ . That is equal to a decimal 1,001.

It has been said that humans use decimal, computers use binary, and humans use hexadecimal to understand binary. Although the base 16 numbering system seems foreign at first glance, largely due to the addition of letters, it really is an efficient way to express large numbers such as MAC and IPv6 addresses.

## IPv4 versus IPv6

IP version 4 (**IPv4**), described earlier in this chapter, is the version of IP currently deployed on most systems today. The next generation of IP, known as IP version 6 (**IPv6**), is being deployed more frequently. This new version was originally designed to address the eventual depletion of IPv4 addresses.

As previously discussed, CIDR has slowed the exhaustion of IPv4 address space and made the move to IPv6 less urgent; however, CIDR is destined to become obsolete because it is based on IPv4. IPv6 makes CIDR techniques unnecessary due to the very large address space available. In addition, security and performance enhancements offer additional reasons to upgrade to IPv6.

Network address translation (**NAT**) was another technique developed in part to slow the depletion of IPv4 addresses. NAT allows a single IP address to provide connectivity for many hosts and is widely used on networks of all sizes. It does, however, present problems. NAT is CPU intensive and expensive. In addition, some protocols do not work well with NAT, such as the IP Security Protocol (**IPSec**), which is currently the most important layer 3 security protocol. However, NAT is completely unnecessary on IPv6 networks. (NAT is explained in more detail in chapter 9.)

Security measures have had to be built around IPv4 because the protocol does not provide security in itself. This has led to security issues with DNS and ARP. Security concerns were factored into the design of IPv6, so fewer security issues are expected in its deployment.

IPv4 networks rely on broadcasting, which is inefficient because many hosts unnecessarily see and partially process traffic not ultimately destined for them. Multicasting is far more efficient but was really not fully utilized in IPv4. IPv6 does away completely with broadcasting and replaces it with multicasting.

IPv6 addresses are 128 bits compared with IPv4's 32-bit structure. This means there are approximately  $2^{128}$  available addresses in IPv6, versus  $2^{32}$  addresses in IPv4. Because of this

significant increase in length, IPv6 addresses are expressed as hexadecimal numbers. An example of an IPv6 address is 3FFE:0501:0008:0000:0260:97FF:FE40:EFAB. That is 32 hexadecimal digits rather than the 32 binary digits in an IPv4 address. Each group of four hexadecimal digits represents 16 bits. Since leading zeroes can be omitted, the above address could also be expressed as 3FFE:501:8:0:260:97FF:FE40:EFAB.

Similar to IPv4, IPv6 can be subnetted; CIDR notation is also used with IPv6. For example, 2001:702:21:: /48 is an IPv6 address with a prefix of 48. Specifically, it is a network address. The CIDR notation tells us that the first 48 bits identify the network. The double colon indicates that all bits remaining after 2001:702:21 are zeroes. A host portion consisting of all binary zeroes indicates a network address just as in IPv4. Note that, because of the lack of broadcasting in IPv6, a host portion consisting of all binary ones does not indicate a broadcast address as in an IPv4 address. In other words, an IPv6 address with a host portion consisting of all binary ones is a valid IP address.

Organizations requesting an IPv6 address may be assigned a /64 prefix. This is the minimum subnet and has space for over a billion hosts. If it seems clear that an organization will need to subnet, a /48, /56, or /60 prefix will typically be assigned instead. A /48 prefix allows for 16 network bits to be subnetted ( $64 - 48 = 16$ ). The 16 bits translate to over 65,000 subnets, which should be more than enough.

## Transitioning to IPv6

According to the U.S. Office of Management and Budget, the federal government will transition to IPv6 by June 2008. At the time of this writing, there is concern that not all federal agencies will be completely prepared for the transition. The problem is that some firewalls and network intrusion-detection systems are unable to monitor IPv6 traffic. If these devices are not reconfigured properly or if they do not support IPv6, a serious security breach is possible. The private sector, which is free to follow its own schedule, should benefit from transition mechanisms that are built into IPv6, and that should make the upgrade relatively easy. These transition mechanisms will allow vendors and networkers to begin integrating IPv6 hardware and software on their own schedules. The two most common transition methods are **dual stack** and **tunneling**.

**Dual Stack** The dual stack method involves enabling IPv6 on all routers, switches, and end nodes but not disabling IPv4—so both version 4 and version 6 stacks run at the same time. Usually, this strategy is implemented in an incremental fashion. When both IPv4 and IPv6 are running, IPv6 will be used for communications if it is preferred by the application. This is the most popular strategy because you get to see if everything is able to run in dual stack mode first before risking a full migration and losing your IPv4 connectivity. Currently, not all systems can work in IPv6-only mode but most can work in dual stack mode. Over time, the IPv4 stack should be able to be removed from your systems, which is the ultimate goal.

**Tunneling** Tunneling is a transition method that encapsulates IPv6 traffic inside IPv4 packets. This is done when portions of a network are running IPv6 and other network areas have not been upgraded yet. Put simply, the tunnels are used to get IPv6 traffic across an IPv4 area to another IPv6 area. The greatest concern with tunneling involves security. If you manually configure the tunnels at each end, there will be less of a security issue because you will be able to monitor the traffic at the endpoints. However, the preferred tunneling technique is to use dynamic tunnels, which are automatically created based on destination address and routing parameters. The problem is that dynamic tunneling does not create interfaces that can be monitored. This makes malicious, injected traffic more likely. Because of this security issue, it is recommended that organizations use the dual stack transition method if possible.



NOTE

Currently, the default setting for IPv6 in Cisco systems is "disabled," however it can be enabled with a few simple commands. First, you enable IPv6 traffic and then you assign IPv6 addresses to individual interfaces in the router.

## Chapter Summary

- The Internet Corporation for Assigned Names and Numbers (ICANN) and the American Registry of Internet Numbers (ARIN) work together to subdivide and issue addresses for Internet clients. Three classes of addresses (A, B, and C) are available to organizations. Class A addresses are for governments worldwide. Class B addresses are assigned to medium-to-large companies and universities. Class C addresses are assigned to organizations and people who require an IP address but do not meet the criteria to have a Class A or B address. Addresses are now largely assigned without regard to classful boundaries using a system known as CIDR.
- The two additional address categories are Class D and Class E. Class D addresses are used for multicasting information. Multicasting allows anyone with the correct setup to broadcast a simultaneous transmission to multiple computers. Class E addresses are used for experimentation and research.
- You can subdivide assigned addresses. This process is called subnetting. The subnet mask divides the network portion of the IP address from the host portion of the address. The network or subnetwork IP address must always have zeros for the host identifier portion. IP addresses that identify TCP/IP hosts must be nonzero in the host portion. When the host portion of an IP address is all binary ones, the address is a broadcast address.
- Routing tables can be created manually and dynamically. Network administrators manually create static routing tables. A manual table requires more administrative overhead but gives the administrator greater control over the routing process. Dynamic updates are provided through routing protocols. The routing protocols allow the routers to be updated automatically.
- Advanced routing protocols such as RIP version 2, OSPF, and EIGRP support variable length subnet masking (VLSM). VLSM allows network administrators to better allocate their IP address space by using different subnet masks on their subnetworks. Classful routing protocols such as RIP version 1 and IGRP do not support VLSM. They require the same subnet mask on every subnet.
- The hexadecimal numbering system is also known as base 16 because it has 16 available numerals. The numerals include all of the numbers 0–9 as well as the letters A–F. For example, the letter A represents the decimal number 10 and the letter F represents the decimal number 15. Hexadecimal numbers are found in MAC addresses and IPv6 addresses, and are often used in computer and networking applications.
- IPv6 is the latest version of IP addressing. Unlike the 32-bit IPv4 addresses that are in use today on most networks, IPv6 addresses are 128 bits long and are expressed in hexadecimal. The U.S. federal government has been mandated to upgrade to IPv6 by June of 2008. It is expected that private entities will convert to IPv6 in the next several years.

## Key Terms

**American Registry of Internet Numbers (ARIN)** An organization that manages IP address allocation in the United States.

**classful** A routing process that involves using subnet masks with traditional octet boundaries.

**classless** A routing process that allows subnet masks to partition the network and the node portions on any bit boundary.

**Classless Inter-Domain Routing (CIDR)** A system of allocating IP network numbers based on arbitrary subnet mask boundaries. CIDR notation uses a prefix to designate the network portion of the subnet mask.

**directed broadcasts** Broadcasts sent to specific segments. For example, a broadcast on segment 192.168.1.0 would be 192.168.1.255.

**dual stack** An IPv6 transition method that allows for both IPv4 and IPv6 stacks to be run on the network at the same time.

**flooded broadcasts** A broadcast for any subnet that uses the IP address 255.255.255.255. Routers do not pass flooded broadcasts.

**hexadecimal** A base 16 numbering system that uses numerals 0 through 9 and the letters A through F to represent numbers. MAC addresses and IPv6 addresses are displayed in hexadecimal.

**Internet Assigned Numbers Authority (IANA)** The regulatory agency originally responsible for subdividing and administering the address hierarchy used on the Internet. IANA has been replaced by ICANN.

**Internet Corporation for Assigned Names and Numbers (ICANN)** The global, government-independent entity responsible for the Internet.

**IP addressing** The act of assigning (unique) IP addresses to devices on the network.

**IP Security Protocol (IPSec)** A suite of protocols that provide authentication and encryption at layer 3.

**IPv4** The currently deployed system of IP addressing involving 32-bit numbers expressed as decimal numbers in four octets.

**IPv6** The newest version of IP addressing that involves 128-bit addresses expressed as hexadecimal numbers.

**loopback** The TCP/IP Class A address 127.x.x.x that is reserved for diagnostic purposes. Any address on this network allows you to check if TCP/IP has been properly installed on the system. (Specifically, the IP address 127.0.0.1 is the address usually given as the loopback.)

**multicast address** A special subdivision of IP categories reserved for data streaming. Multicast addresses are used to send information to groups of computers. The range for multicasting addresses is 224.0.0.0 to 239.255.255.255.

**multicasting** The sending of a stream of data to multiple computers simultaneously.

**Network Address Translation (NAT)** A standard that allows inside IP addresses to be translated to different outside IP address(es). NAT maps inside IP addresses to different outside IP addresses or just one outside address. NAT is used to slow the exhaustion of IPv4 addresses as well as to hide a company's internal IP scheme.

**nibble** Four bits. There is one hexadecimal digit in a nibble.

**prefix** A way of designating the subnet mask that involves a forward slash followed by the number of binary ones in the mask; in other words, the network portion.

**subnet** A portion of a network that has been separated from the main network by using a different subnet mask.

**subnet mask** A required component for all IP hosts used in combination with an IP address to determine to which subnet the local host belongs. The local host uses this information to determine if the destination is local or remote to the source. Based on this information, the source will either broadcast information on the local network or send its packet to the default gateway for delivery to a remote network.

4

**subnetting** The act of subdividing a network logically with subnet masks.

**summarization** The advertisement of many routes as a single route to reduce the total number of route table entries on a router.

**supernetting** Also known as summarization or route aggregation. Done by moving the network/node boundary in the subnet mask to the left to include more than one network in an advertisement.

**tunneling** An IPv6 transition strategy that involves encapsulating IPv6 packets inside of IPv4 packets so they can traverse the non-IPv6 portion of the network.

**variable length subnet masking (VLSM)** The use of different masks on different subnets, which allows for more efficient IP address allocation. Supported by advanced routing protocols such as RIP version 2, OSPF, and EIGRP.

---

## Review Questions

1. If your Class C address has a three-bit subnet mask, which of the following would be a subnetwork identifier?
  - a. 203.16.34.33
  - b. 203.16.34.135
  - c. 203.16.34.32
  - d. 203.16.34.240
2. Which of the following would be a broadcast address for a Class C network?
  - a. 190.15.23.255
  - b. 190.42.25.255
  - c. 221.21.23.255
  - d. 129.21.15.255
3. Which of the following Class C IP addresses is a broadcast (assuming the subnet mask is 255.255.255.224)?
  - a. 219.129.32.5
  - b. 219.129.32.63
  - c. 219.129.32.97
  - d. 219.129.32.161

**112** Chapter 4 IP Addressing

4. For a Class B broadcast, which octets will be completely binary ones?
  - a. 2nd
  - b. 2nd and 3rd
  - c. 1st and 2nd
  - d. 3rd and 4th
5. Which of the following is a Class A broadcast?
  - a. 11.255.255.255
  - b. 127.75.255.255
  - c. 193.255.255.255
  - d. 14.25.255.255
6. What is the purpose of the reserved numbers in a Class D address?
  - a. unicast
  - b. experimental
  - c. broadcast
  - d. multicast
7. What is the purpose of the reserved numbers in a Class E address?
  - a. unicast
  - b. broadcast
  - c. multicast
  - d. experimental
8. In a Class C address, which octets identify the network?
  - a. all of them
  - b. the first octet only
  - c. the first and second octet
  - d. the last octet
  - e. the first three octets
9. Class B addresses allow you to configure how many octets on your network for host IP addresses?
  - a. one
  - b. two
  - c. three
  - d. four
10. Which of the following are valid network identifiers for Class A addresses?
  - a. 1-127
  - b. 1-126
  - c. 192-223
  - d. 224-240
  - e. 128-191

11. What would the value of the first octet of the subnet mask be if the CIDR notation for an address is 192.168.1.16/27?
- 224
  - 254
  - 255
  - 265
12. What would the value of the last octet of the subnet mask be if the CIDR notation for an address is 192.168.1.16/28? **4**
- 192
  - 224
  - 240
  - 248
  - 252
13. Assuming that the address 165.24.3.6 uses the correct default mask, what is the host identifier?
- 165.24
  - 24.3.6
  - 3
  - 3.6
14. How many bits (maximum) can be used from the last octet of a Class C address to subnet your network?
- 2
  - 4
  - 6
  - 8
15. Which of the following address classes allows you to borrow a maximum of 14 bits to create a subnet mask?
- Class A
  - Class B
  - Class C
  - None of the above
16. A subnet mask of 255.255.252.0 on a Class B network indicates that bits have been borrowed from the host portion to subnet the network.
- 2
  - 4
  - 6
  - 8
  - 10

**114** Chapter 4 IP Addressing

17. Given the following CIDR address and mask, which of the following is a broadcast on its subnet 162.17.12.125/24?
  - a. 162.17.15.255
  - b. 162.17.12.255
  - c. 162.17.255.255
  - d. 255.255.255.255
  - e. None of the above
18. Given the address 190.14.20.255/20, which of the following statements is true?
  - a. This is a broadcast address.
  - b. This is a network address.
  - c. This is a host address.
  - d. This address is on network 190.14.20.0.
  - e. This address is on network 190.14.16.0.
19. Given the address 190.14.20.0/22, which of the following statements is true?
  - a. This is a broadcast address.
  - b. This is a network address.
  - c. This is a host address.
  - d. This address is on network 190.14.20.0.
  - e. This address is on network 190.14.16.0.
20. How does CIDR conserve IP addresses?
  - a. by charging more for IP address assignments
  - b. by allocating IP network numbers on criteria other than traditional bit boundaries
  - c. by using traditional octet boundary subnet masks
  - d. by aggregating routes
21. Which of the following routing protocols support VLSM? (Choose all that apply.)
  - a. RIP version 1
  - b. IGRP
  - c. OSPF
  - d. EIGRP
22. What is the purpose of summarization?
  - a. to reduce the number of routing table entries
  - b. to prevent route flapping
  - c. to conserve IP addresses
  - d. to reduce the cost of acquiring IP addresses

23. What is true regarding IPv6? (Choose all the apply.)
- a. Addresses are expressed in binary.
  - b. Addresses are expressed in hexadecimal.
  - c. It is difficult to transition to IPv6.
  - d. IPv6 addresses are 64 bits rather than 32 bits like IPv4 addresses.
  - e. Most Cisco systems support IPv6.
24. What are some reasons to switch to IPv6? (Choose all that apply.)
- a. The equipment costs less.
  - b. IPv6 is inherently more secure.
  - c. There is more address space available with IPv6.
  - d. IPv6 will handle your NAT configurations automatically.
  - e. Broadcasting will be replaced with multicasting.

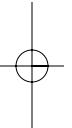


---

## Case Projects



1. Moe is having a difficult time with IP subnetting. He knows the basics but has some specific questions. He wants to know why certain numbers are unavailable for use. For example, he was told that he cannot use 10 or 127 or any numbers over 223 in the first octet. Why are these numbers off limits? Explain your answer to Moe.
2. Moe now wants to know why there are two invalid IP addresses on each subnet. Explain to him what the two addresses are and why they cannot be used.
3. CIDR, summarization, and VLSM all involve moving the network/node line to the right or to the left. Explain which of the three moves the line to the left and how each method is used.





5  
chapter

## Router and IOS Basics

**After reading this chapter and completing the exercises, you will be able to:**

- Describe the benefits of network segmentation with routers
- Understand the elements of the Cisco router user interface
- Configure the HyperTerminal program to interface with the Cisco router
- Describe the various router configuration modes
- Describe the various router passwords
- Understand the enhanced editing features of the Cisco IOS
- Compare router components to typical PC components

**This chapter delves deeper into the benefits of routing. You will learn** about the elements of the Cisco user interface, including the system configuration dialog, various configuration modes, and the many Cisco router passwords. You will also configure the Windows program HyperTerminal for use with the router. In addition, you will explore the enhanced editing features of the Cisco IOS and router components.

## Benefits of Routing

As you learned in preceding chapters, network administrators use routers in large networks to provide packet filtering, connections between local networks, traffic control, and wide area network (WAN) connections. Routers operate at the Network layer of the OSI reference model and because of Network layer addressing, routers can direct packets to both local and remote segments.

One of the main benefits of using a router is that it filters traffic. When a device sends a packet on the local segment, all other devices on that segment must receive or discard the packet. Bridges can segment the network at the Data Link layer, but broadcast traffic from one segment to another must still pass through the bridge because the bridge cannot distinguish addresses above layer 2. In a large network composed of one large segment, this broadcast traffic could seriously affect performance. Routers solve the problem by filtering traffic and forwarding only packets that are addressed to hosts on other networks. In this way, routers reduce traffic by segmenting the network and filtering broadcasts. Said another way, routers create collision domains as well as broadcast domains.

When network administrators add routers to a network, they must configure them to operate within the network. To perform routine maintenance and troubleshooting, network operators and administrators must be able to check the status of the router and its components. This necessary interaction with the router requires an interface through which the routers can be configured.

## Cisco Router User Interface

Network administrators commonly configure and interact with a Cisco router via the **Cisco Internetwork Operating System (IOS)**. The Cisco IOS provides a command-line interface (CLI), which allows network operators to check the status of the router and network administrators to manage and configure the router. The software that interprets the commands is called the **command executive**, or **EXEC**.

You can access a router in several different ways; each method involves access through one of three lines. Network administrators typically access the router directly through the **console port** (also known as the **console**) located on the back of the router. The console port connects directly to a PC through an **RJ-45 to RJ-45 rollover cable** with an **RJ-45 to DB-9 connector** included with the router. The second line used to access the router is through the **auxiliary port (AUX)**, which is also on the back of the router. The auxiliary port allows a remote administrator to dial into the router through an external modem, which gets attached to the auxiliary port. The remote PC must also have a modem to use this method.

Figure 5-1 shows a laptop connected to a Cisco 2600 series router via the console port using the RJ-45 to RJ-45 rollover cable and RJ-45 to DB-9 connector. The DB-9 is attached to the COM1 port of the laptop in the picture.

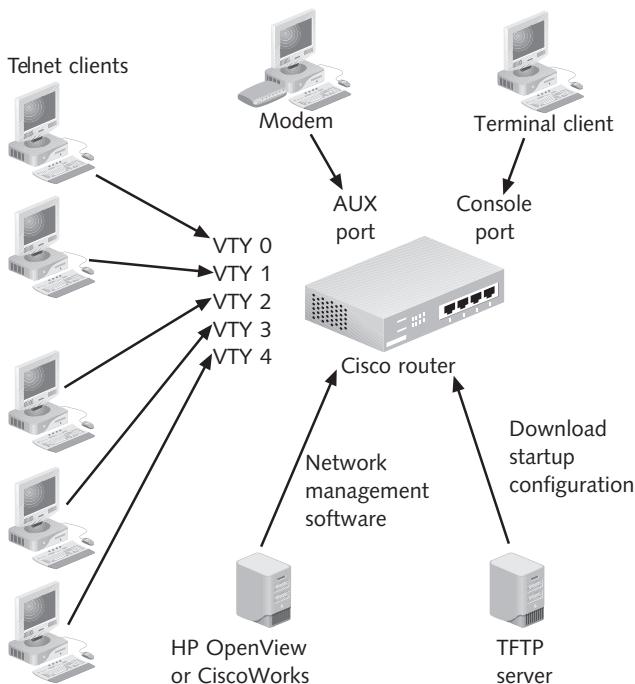
In addition to the AUX and the console ports, you can use five **virtual terminals (VTY)** to configure the router. When you access the router through VTY lines, you are using telnet. The virtual terminals are numbered from zero to four. You can reference the virtual terminals by their abbreviation and numeric indicators: VTY 0, VTY 1, VTY 2, VTY 3, and VTY 4. Network administrators access the virtual terminals through a telnet session.



5

**Figure 5-1** Connecting a PC to the console

In addition to configuration through access via the AUX, console, or virtual terminals, the router can obtain configuration information from a **Trivial File Transfer Protocol (TFTP)** server. You can store the router configuration information as a file on a TFTP server and download it to configure the router. (The process is described in chapter 6.) Also, network administrators can use network management software such as HP OpenView or CiscoWorks to manage Cisco routers. Figure 5-2 illustrates different methods for accessing a router for configuration purposes.



**Figure 5-2** Methods for configuring a Cisco router

## Connecting via Terminal Programs

When configuring the router through the console or AUX ports, you must first make the physical connection. Then, you can access the router through a terminal program. Many different terminal programs are available for this purpose, including HyperTerminal, MicroPhone Pro, ProComm Plus, Telix, Teraterm, and Terminal on Microsoft DOS and Windows systems; Kermit and Tip on Sun Workstations; Z-terminal on Apple Macintosh computers; and Minicom on Linux systems. For example, if the connection from the router to the PC attaches at the COM1 port on the PC, you would configure your terminal program to use COM1. HyperTerminal is available in most Windows operating systems but not with Windows Vista. If you are using Vista, you can download a free personal edition of HyperTerminal from [www.hilgraeve.com/htpe/download.html](http://www.hilgraeve.com/htpe/download.html).

You can use the following steps to configure HyperTerminal:

1. Open the HyperTerminal application. You may be prompted to make HyperTerminal your default telnet program. Click **Yes**. In Microsoft Windows XP and Windows 2000, you should find HyperTerminal in the All Programs/Accessories/Communications group in the Start menu. If you cannot find HyperTerminal, you may have to install additional Accessories programs from the Add/Remove Programs icon in the Control Panel of your Microsoft Windows system. In Microsoft Windows XP, click **Start** and navigate to **All Programs, Accessories, Communications**, and **HyperTerminal**.
2. You may be prompted for location information. In this case you are not using a phone or modem connection, so click **Cancel**, then click **Yes**, and then click **OK**. If the New Connection Wizard does not appear automatically, click **File** on the menu bar, and then click **New Connection**.
3. Enter a name for the connection. The name is for user reference only, so you can use any name that describes the connection. Click **OK** to continue.
4. You must then configure how you will connect to the router via the Connect To dialog box (you may be prompted to install a modem). You will see a field to enter a phone number. If you are connecting to the router through the AUX port, you would provide the router phone number here. If connecting to the router through the console port, click the “Connect using” list box and choose the COM port to which the RJ-45 to DB-9 connector is attached. Click **OK** to continue.
5. Configure the following settings for the COM port: Bits per second, **9600**; Data bits, **8**; Parity, **None**; Stop bits, **1**; Flow control, **None**. Click **OK** to complete the configuration. Click **File** on the menu bar, and then click **Properties**. Under Settings, make sure the keys are set to act as “Terminal” keys.

When the HyperTerminal configuration is complete, the program will attempt to connect to the router. At this point, you would turn on the router. On the screen, you should then see the router boot routine. Sometimes it is necessary to press Enter a few times to get a response from the router.



If you see a series of miscellaneous characters after you turn on the router, you probably have incorrectly set the bits per second (also known as baud rate). Click **File** on the menu bar, click **Properties**, and reconfigure your connection as described previously.

**NOTE**

When the router boots, it should eventually show a prompt, such as **router>**, or you may be prompted to enter the **system configuration dialog** (also known as the initial configuration dialog), an automated setup routine described in the next section.

## System Configuration Dialog

If the router has not been configured previously, or if the startup file has been erased, the Cisco IOS will prompt you to run the initial configuration dialog after the router boots. You can also access the system configuration dialog by typing the `setup` command at the privileged EXEC prompt. The system configuration dialog presents a series of prompts that guide you through the initial configuration for the router. Each question is followed by a default option in brackets. If you decide to accept the default option, you can press the Enter key. Beginning with version 12.0 of the IOS, setup is available in two different levels: basic management setup and extended setup. Basic management setup only configures enough connectivity for management of the system. Extended setup prompts you for configuration of all interfaces and provides enough configuration information to make the router operational.

The first question you are asked by the system configuration dialog is whether you want to enter the initial configuration dialog. If you type “y”, you will begin the router configuration process. The next question is, “Would you like to enter basic management setup?” If you type “y” you will enter basic management setup. If you answer “n” you will enter extended setup mode. Figure 5-3 illustrates use of the `setup` command.

```
lab-a#setup

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: y

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]: y
Configuring global parameters:

Enter host name [lab-a]:
```

**Figure 5-3** Output from the `setup` command

After the system configuration dialog program completes, the router will run through its typical startup process (which is described in greater detail later in this chapter). After this initialization process, you can begin to view and configure the router settings.

## User Interface

When the router completes its initialization process, you must press the Enter key to reach the prompt. The initial prompt consists of two parts: the host name of the router followed by the greater than symbol (>). By default, the router’s host name is `router`, so the default prompt is `router>`.

## 122 Chapter 5 Router and IOS Basics

When the prompt displayed is the greater than symbol, the router is in **user EXEC mode** (or **user mode**). In this mode the network operator can check router status to see if the interfaces are operational, and review several of the router settings. From any prompt, you can see a list of possible commands at that prompt by typing a question mark (?), as shown in Figure 5-4. You do not need to press Enter after typing the question mark.

```

RouterB(config)#? ←
Configure commands:
aaa                               Authentication, Authorization and Accounting.
access-list                      Add an access list entry
alias                            Create command alias
arp                               Set a static ARP entry
async-bootp                      Modify system bootp parameters
banner                           Define a login banner
boot                             Modify system boot parameters
bridge                           Bridging Group.
buffers                          Adjust system buffer pool parameters
busy-message                     Display message when connection to host fails
cdp                             Global CDP configuration subcommands
chat-script                      Define a modem chat script
clock                            Configure time-of-day clock
config-register                  Define the configuration register
default-value                    Default character-bits values
dialer-list                      Create a dialer list entry
dnsix-dmdp                       Provide DMDP service for DNSIX
dnsix-nat                        Provide DNSIX service for audit trails
downward-compatible-config      Generate a configuration compatible with older
                                software
enable                           Modify enable password parameters
end                             Exit from configure mode
exit                            Exit from configure mode
frame-relay                      global frame relay configuration commands
help                            Description of the interactive help system
hostname                         Set system's network name
interface                        Select an interface to configure
ip                               Global IP configuration subcommands
ipx                             Novell/IPX global configuration commands
key                            Key management
line                            Configure a terminal line
logging                          Modify message logging facilities
login-string                     Define a host-specific login string
map-class                        Configure static map class
map-list                         Configure static map list
menu                            Define a user-interface menu
modemcap                        Modem Capabilities database
netbios                         NETBIOS access control filtering
no                              Negate a command or set its defaults
ntp                             Configure NTP
partition                       Partition device
priority-list                    Build a priority list
privilege                        Command privilege parameters
prompt                           Set system's prompt
queue-list                      Build a custom queue list
resume-string                   Define a host-specific resume string
rlogin                           Rlogin configuration commands
rmon                            Remote Monitoring
route-map                       Create route-map or enter route-map command mode
router                           Enable a routing process
scheduler                        Scheduler parameters
service                          Modify use of network based services
snmp-serverd                     Modify SNMP parameters
state-machined                  Define a TCP dispatch state machine
tacacs-serverd                  Modify TACACS query parameters
terminal-queued                 Terminal queue commands
tftp-serverd                     Provide TFTP service for netload requests
usernamed                        Establish User Name Authentication
x25d                            X.25 Level 3
x29                            dX29 commands

RouterB(config)#

```

Typing a ? invokes the Help system of the IOS. In this case, all commands available in global configuration mode are displayed.

**Figure 5-4** Output from the ? command

The question mark activates **context-sensitive Help** on the Cisco router. The term “context-sensitive” means that the router evaluates the command mode that you are in, and any command strings you have entered on the line prior to the question mark, before providing the Help screen. For example, when you are in user mode and type the question mark, the Help that follows will be commands available from user mode. However, if you type `ping ?` you will get a list of options you can use with the ping command.

**NOTE**

When the list of Help screen options does not fit on one screen, Help displays only the first screen of options. You can view additional commands line-by-line by pressing the Enter key for each line. You can page through the list of commands by pressing the space bar. Pressing a letter on the keyboard will take you immediately back to the prompt.

**5**

User mode does not allow you to configure the router. To do this, you must go into the **privileged EXEC mode**. To enter privileged EXEC, you can type the `enable` command at the user mode prompt. Next, you may be prompted for a password. If an enable password has been configured, you must enter it. As you type, the password will not be displayed on the terminal screen. If an enable secret password has been configured, then you will type the enable secret password. The different types of passwords are described in greater detail later in this chapter.

After you enter the enable password or the enable secret password, the greater than symbol (>) changes to a pound sign (#) to indicate that you are in privileged EXEC mode (**router#**). Most router configuration takes place in router modes beyond privileged EXEC mode; however, you can do a few things at this prompt to substantially affect router operations:

- *Setup*—The `setup` command will cause the router to enter the system configuration dialog, which allows the router to be completely reconfigured.
- *Copy*—Configurations can be copied from TFTP servers to the router and therefore change the router configuration.
- *Erase*—Configuration files as well as the entire IOS can be erased.

**NOTE**

Privileged EXEC mode is called **enable mode** because you must enter the `enable` command to access it.

## Configuration Modes

Several configuration modes are accessible only through the privileged EXEC mode. This section discusses some of these basic **router configuration modes** and their respective options.

After you have placed the router into enable mode, you will be able to choose from various router configuration options. From the **enable mode prompt** (**router#**), you can view the router’s configuration and access several other configuration modes. You access the basic configuration mode, called **global configuration mode**, by typing `configure terminal` at the enable mode prompt.

From the global configuration mode, you can access several other configuration modes. For example, **interface configuration mode** allows you to configure the Ethernet and serial interfaces on your router. With **line configuration mode**, you can configure the virtual terminals, console, and AUX lines that let you access the router. Router configuration mode permits you to enable routing protocols such as RIP and IGRP. Table 5-1 lists these modes, the associated prompt, the method for entry and exit, and a brief description of what you can accomplish in each mode.

## 124 Chapter 5 Router and IOS Basics

Mode	Prompt	To enter	To exit	Used for
User EXEC	Router>	If there is a line password, enter it. Otherwise, press the Enter key.	logout or exit	Shows the status of the router and allows network operators to manage connections
Privileged EXEC	Router#	Type enable at the prompt.	disable exit logout	Copies, erases, sets up, and shows router settings
Global configuration	Router (config)#	configure	exit end	Allows you to configure various items, including clock, host name, enable password, and enable secret password
Interface configuration	Router (config-if)#	interface fastethernet0/0 or interface serial0/0	exit end	Allows you to configure the settings, such as IP, for a specific interface
Line configuration	Router (config-line)#	line console 0 or line vty 0 4 or line aux 0	exit end	Configures lines, such as the console, virtual terminal, or auxiliary
Router configuration	Router (config-router)#	router rip or router igrp	exit end	Adds or configures RIP, IGRP, or other routing protocols

**Table 5-1** Common configuration modes

Typing `exit` will take you back one level. For example, if your prompt shows `router(config-router)#` and you type `exit`, your prompt will change to `router(config)#`. Typing `end` or pressing the `Ctrl+Z` keys will take you all the way back to the enable prompt. For example, if you see `router(config-line)#` and you type `end`, your prompt will revert to `router#`, not `router(config)#`. Note that if you are typing commands and you see the dollar sign (\$), it means that the line is continued from a previous line.



NOTE

You can abbreviate the commands shown in the table. Usually, the abbreviation for a command is the fewest number of characters that can be used to uniquely identify the command. For example, to enter the enable mode, you can type `enable`, or `en`. (You can also type `enab` and `enabl`.) On simulation questions on the CCNA exam, make sure to type the entire command, without abbreviations.

Often, you can discover abbreviated commands by simply trying them. If the command does not work, the router will tell you that the command is invalid. If you get part of the command correct, the router will show you the point at which you entered an incorrect character by pointing to the character with a caret symbol (^). For example, to show the current running configuration of the router, you can type `show running-config`. However, if you accidentally type `show runing-config`, the router will indicate that the command is incorrect by pointing to the first incorrect character. In Figure 5-5, the first incorrect character is the letter “i.”

```
router#show runing-config
^
% Invalid input detected at '^' marker.

router#
```

**Figure 5-5** Command error checking

Using the shortcut for the show running-config command, which is sh ru, reduces the chance of making a typo.

**NOTE****5**

Once you have a basic understanding of the commands presented in Table 5-1, you are ready to start practicing basic router configuration tasks. One of the first areas that you might want to investigate is password configuration.

## Plethora of Passwords

You can set five passwords on a Cisco router. If you configure the router using the system configuration dialog (setup), you will be prompted for three of these five: the enable password, the enable secret password, and the **virtual terminal password**. You can add a **console password**, an **AUX line password**, and an individual password for each virtual terminal.

Table 5-2 lists and describes these router passwords.

Passwords	Description
<b>Enable</b>	Used only when the enable secret password is not present. This password is not encrypted, but it does restrict access to enable mode if the enable secret password is removed.
<b>Enable Secret</b>	This is the primary password used to access enable mode because it supersedes the enable password. When the enable secret password is configured, only the enable secret password (not the enable password) allows you to access enable mode. This enable secret password is encrypted with the <b>MD5 algorithm</b> .
<b>Console</b>	Protects the router from console access. When this password is set, someone attempting to access the router from the console connection will have to enter a password before he or she can enter any other commands. This password is not configured by default during setup.
<b>AUX</b>	The AUX line can also have a password configured. This password is requested whenever someone attempts to access the router by a modem through the AUX port. This password is not configured by default during setup.
<b>Virtual Terminal</b>	The router identifies each telnet session as a virtual terminal. You can configure a password for any number of virtual terminals or each one individually. Usually, a five-session limit is put on the router. If you type VTY 0 4 when configuring the password, you will be setting a single password for the five virtual terminals. To configure a password for a single virtual terminal, type VTY followed by the terminal number.

**Table 5-2** Router passwords

If you have an enable secret password set, you may see it as a string of miscellaneous characters when viewing your router configuration. Do not mistake those characters for the actual password; they are just a representation of an encrypted password.

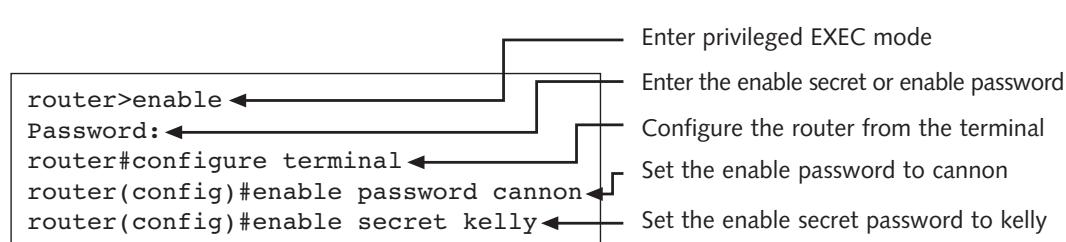


If you want to configure encryption for all of your router passwords, type `service password-encryption` at the global configuration prompt.

In the following sections, you will learn how to configure each of the passwords shown in Table 5-2.

**Enable Password and Enable Secret Password Configuration** You can set both the `enable password` and `enable secret password` from the global configuration mode prompt, which is `router(config)#`. To add or change the enable password or enable secret password, simply type the name of the password you want to configure and follow it with the password you want to set.

Figure 5-6 illustrates the steps to configure the enable password and enable secret password from the terminal.



**Figure 5-6** Setting enable password and enable secret password

Because it is encrypted, the enable secret password is more secure than the enable password. You can view the enable password from the configuration file, but not the encrypted enable secret password. To see the difference, type `show running-config` or `show run` at the enable mode prompt and read the configuration file, as shown in Figure 5-7.

If you want to remove the enable secret password, you can type `no enable secret` at the global configuration mode prompt. You can also type `no enable password` to remove the enable password. Of course, if you remove both the enable secret and enable password, anyone who can log on can configure the router.

The image shows a Cisco router configuration output in a terminal window. The configuration includes various service and interface settings. Two specific lines are highlighted with arrows pointing to callout boxes:

- enable secret 5 \$1\$vdGT\$08FE.EExWM5WWRQCPjDgc/**: This line is annotated with a callout box stating, "The enable secret password is stored in an encrypted form for increased security".
- enable password cannon**: This line is annotated with a callout box stating, "The enable password is stored as plain text and can pose a security risk".

```

Router#show run
Building configuration...

Current configuration : 927 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-enc
!
hostname Router
!
enable secret 5 $1$vdGT$08FE.EExWM5WWRQCPjDgc/ ←
enable password cannon ←
!
interface FastEthernet0/0
 ip address 172.22.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 172.22.3.2 255.255.255.0
 no fair-queue
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
Router rip
 network 172.22.0.0
!
ip http server
ip classless
!
line con 0
line aux 0
line vty 0 4
!
End

```

5

**Figure 5-7** The enable password and enable secret password

To configure the console line, AUX line, and virtual terminal passwords, you must be in a line configuration mode, as the next section discusses.

**Setting Line Passwords** Line passwords are the first line of defense against unauthorized intrusion into the router. You can set passwords for each line used to configure the router. As mentioned previously, these lines are the console line, the AUX line, and each of the five virtual terminal lines. By default, you can configure the virtual terminal passwords using the initial router setup process, but all virtual terminals are set for the same password.

## 128 Chapter 5 Router and IOS Basics

One of the first passwords you might want to configure is the console line password. To configure a console password, you must enter line configuration mode. Figure 5-8 illustrates the process for configuring a console line password.

```

RouterB>en
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#line con 0
RouterB(config-line)#password cisco
RouterB(config-line)#login
RouterB(config-line)#^Z
RouterB#
%SYS-5-CONFIG_I: Configured from console by console
RouterB#

```

**Figure 5-8** Applying a console password

After you have added the password to the console, you can check it by exiting line configuration mode and logging off the terminal. When you then attempt to log on to the terminal, you will be prompted for a password, as shown in Figure 5-9.

```

RouterB con0 is now available
Press RETURN to get started.
User Access Verification
Password:

```

**Figure 5-9** Console password example

You can also configure passwords on the five virtual terminal lines that exist on every router, in much the same way as on the console port. In fact, you must configure a VTY password if you want to enable access via telnet. This is a safety precaution; without it, anyone with the IP address of the router will be able to access it. To configure the VTY password, go into line configuration mode on the router for the VTY lines and add the login and password commands. Figure 5-10 shows the process of applying a VTY password.

```

RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#line vty 0 4
RouterB(config-line)#login
RouterB(config-line)#password Lowry
RouterB(config-line)#^Z
RouterB#
%SYS-5-CONFIG_I: Configured from console by console

```

**Figure 5-10** Applying a VTY password

If you just wanted to set an individual VTY password for VTY line 0, you would type line vty 0 instead of line vty 0 4 at the RouterB(config)# prompt shown in Figure 5-10. The same is true for any other VTY port; they are individually numbered 0, 1, 2, 3, and 4 (five lines total).

Passwords can be placed on auxiliary ports in the same way they are placed on console or vty ports. Using all three of these passwords will at least slow down someone trying to enter your routers. If they happen to get through these passwords, the single most important password (the enable or enable secret password, depending on which one is in use) can stop them from actually modifying the router's configuration.

## Enhanced Editing

By default, the router supports enhanced editing features that allow you to modify lengthy commands. The enhanced editing commands let you jump to the beginning or end of a command line. You can also jump forward or back, character by character, or word by word. Table 5-3 shows the shortcuts and the definitions.

Key Combination	Description
Ctrl+A	Moves the cursor to the beginning of the current line.
Ctrl+E	Moves the cursor to the end of the current line.
Ctrl+F	Moves the cursor one character to the right. You can also accomplish this by pressing the right arrow key.
Ctrl+B	Moves the cursor one character to the left. You can also accomplish this by pressing the left arrow key.
Esc+F	Moves the cursor one word forward.
Esc+B	Moves the cursor one word back.

**Table 5-3** Editing commands

**130** Chapter 5 Router and IOS Basics

You can turn off the enhanced editing features by typing terminal no editing at either the user EXEC or the privileged EXEC prompts. You can turn on terminal editing by typing terminal editing.



When you type an incorrect command, the bogus command might be mistaken for a host name. If this happens, the router will, by default, attempt to look up the host name and give you the corresponding IP address. If you want to prevent the router from doing this, type no ip domain-lookup at the global configuration prompt.

To cancel any command or process, press the Ctrl, Shift, and 6 keys simultaneously. You may also have to let go of those keys and then press the X key to initiate the escape sequence on some routers.

## Command History

The command history allows you to retrieve previously typed commands. You can see up to 10 previously typed commands by typing show history from either the user EXEC or privileged EXEC mode. You can use the up arrow (or press Ctrl+P) to retrieve previous commands. The down arrow (or Ctrl+N) will retrieve recent commands, assuming that you are viewing previous commands. If you type part of a command, you can press the Tab key to complete the command.

To modify the number of commands stored by the router, you can use the terminal command. You can set the history buffer to zero so that it will not store commands, or you can set it to store up to 256 previous commands. For example, to decrease the number of commands stored from the default of 10 to three, you would type terminal history size 3 at the enable prompt.

## Configuring Router Identification

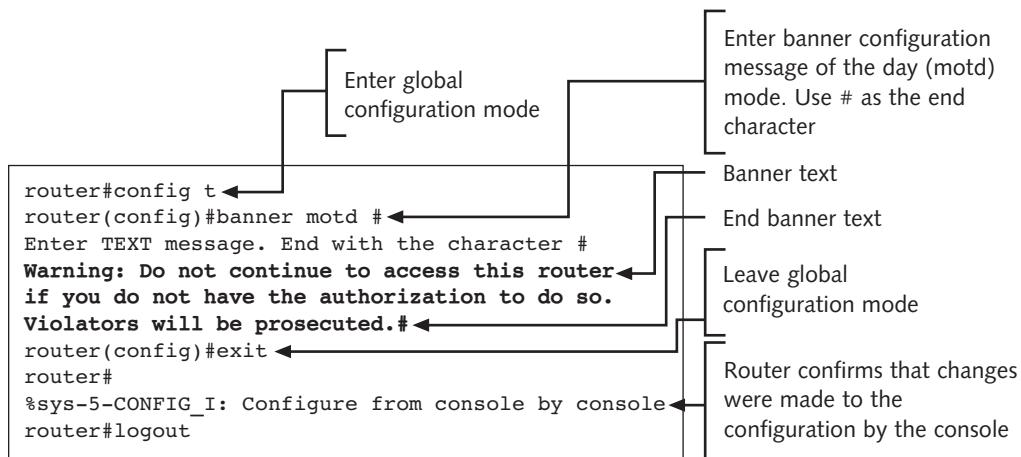
You can identify your router in several ways. The most obvious is the router host name. The default host name is simply `router`, which is displayed at the beginning of every prompt. The command for configuring the host name for the router must be typed in global configuration mode. If you want to set the router host name, type `hostname` followed by the name that you want to set. For example, to set the router's name to `router57`, type `hostname router57`.

Another way to configure identification for the router is to configure a banner. A banner is a message that you can configure to display each time someone attempts to log in to the router. To configure the banner, you must first enter global configuration mode by typing `config t`; then type `banner motd`, followed by a space and a delimiting character. Note that `motd` stands for message of the day, and the delimiting character can be any keyboard letter or symbol.

When you type the delimiting character in a banner configuration, the router will interpret the character as the end of the banner; therefore, it is best to use a delimiting character that will not be typed in your banner message. A typical character used for delimiting the banner message is the pound symbol (#).

The banner `motd` command is typically used as a legal means of warning anyone who accesses the banner that they will be held accountable.

Figure 5-11 illustrates the configuration process for a banner page.



**Figure 5-11** Configuring a banner message

Notice that once the delimiting character is typed, the router assumes that the banner message is complete. To see the banner message, log out and attempt to log on to the router. Figure 5-12 illustrates how the banner message in this section's example would look. To remove the banner, type no banner motd at the global configuration prompt.

```
RouterB con0 is now available
Press RETURN to get started.

Warning: Do not continue to access this router
if you do not
have the authorization to do so.
Violators will be prosecuted.

RouterB>
```

**Figure 5-12** Banner message displayed

Another method of identifying router components is to configure an interface description. You can configure a description for each of the interfaces physically attached to your router by using the description command. The interface description helps you remember which network the interface services. For example, if you wanted to configure a description for the Ethernet0/0 interface to remind you that it is connected to the Department A LAN, you would type commands similar to those shown in Figure 5-13.

```
router#config t
router(config)#interface e0/0
router(config-if)#description Attached to Dept A LAN
```

**Figure 5-13** Configuring an interface description

After you have configured the description for the interface, return to the basic privileged EXEC prompt (router#) and type `show interfaces` to check your work. The description for Ethernet0/0 should now have the text you typed.

## Configuring the Time and Date

Another basic configuration task is to configure the router's time clock and time zone. Use the `clock set` command in enable mode to configure the time. You must be in global configuration mode to configure the time zone. The commands in Figure 5-14 show how to configure the time zone, the time, and the date.

```
router#config t
router(config)#clock timezone pacific -8
router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
router#clock set 12:45:22 30 March 2007
```

**Figure 5-14** Configuring the time and date

When entering the time zone, you must include the name of the time zone and the offset from the **Coordinated Universal Time (UTC)**. The UTC is based on the time in Greenwich, a city in the United Kingdom. All other time zones are either plus or minus a certain number of hours. For example, Eastern Standard Time is minus five, or five hours earlier than in Greenwich. After you have configured the time zone, you can configure the clock. If you configure the time zone and clock in the opposite order, your clock will change after you configure the time zone. To confirm your settings, type `show clock` at the privileged EXEC prompt.

---

## Router Components

A router is a specialized computer and has many of the same hardware components that a typical PC does. This section discusses the hardware elements of the router, including:

- ROM
- Flash memory
- NVRAM
- RAM/DRAM
- Interfaces

### ROM

**Read-only memory (ROM)** loads the **bootstrap** program that initializes the router's basic hardware components. ROM is not modified during normal operations, but it can be upgraded with special plug-in chips. The content of ROM is maintained even when the router is rebooted, which is similar to how ROM operates on a PC.

The ROM monitor firmware runs when the router is turned on or rebooted. You can configure new passwords with ROM monitor if password recovery is necessary. You can also download new software to the router using ROM monitor. You know that you are in ROM monitor mode when the prompt is just the greater-than sign (>) or the greater-than sign preceded by `rommon 1` or something similar (`rommon 1>`).

## Flash Memory

Flash memory is a type of erasable, programmable, read-only memory (EPROM). This means that flash memory is not typically modified during normal operations; however, it can be upgraded or erased when necessary. The content of flash memory is maintained even when the router is rebooted.

Flash memory contains the working copy of the current Cisco IOS and is the component that initializes the IOS for normal router operations. Flash memory on certain series of Cisco routers can store multiple versions of the IOS, which can make upgrading the IOS easier and safer. For example, if an upgrade to the IOS is implemented, but later found undesirable or difficult to use, the router can be configured to use the original copy of the IOS. The show version command displayed in Figure 5-15 provides a summary of IOS information.

```

RouterB#show version

Cisco Internetwork Operating System Software
IOS (ta) C2600 Software (C2600-I-M), Version 12.3 (15b), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Thu 25-Aug-05 13:38 by search
Image text-base: 0x80008098, data-base: 0x80CD9220

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

RouterB uptime is 23 minutes
System returned to ROM by power-on
System image file is "flash:c2600-i-mz.123-15b.bin"

cisco 2621 (MPC860) processor (revision 0x200) with 45056K/4096K bytes of memory
.
Processor board ID JAD051200HP (1421925014)
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(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

```

Annotations from left:

- Show version command displays a summary of IOS information and router configuration
- This router is a Cisco 2600 series router running version 12.3 of the IOS

Annotation from right:

- The router is configured with 2 FastEthernet interfaces and 2 serial interfaces

**Figure 5-15** Output from show version command

## NVRAM

Nonvolatile random access memory (NVRAM) is a special type of RAM that is not cleared when the router is rebooted. The startup configuration file for the router is stored in NVRAM by default. When the router is first shipped, the configuration file is not present. This is the first file created by the person who sets up the router.



NVRAM stores all the user-defined configuration information for the router, which can include the host name of the router, the protocol configurations, and the cache configurations.

The Cisco IOS uses the configuration file in NVRAM during the router boot process, which is explained in the next chapter. Whenever the configuration of the router is updated, the administrator copies the running configuration, which is the one that has just been updated, to the startup configuration. The startup configuration is maintained in NVRAM, whereas the running configuration is maintained in RAM/DRAM.

## RAM/DRAM

Random access memory (RAM), also known as dynamic random access memory (DRAM), is a volatile hardware component because its information is not maintained in the event of a router reboot. This is similar to how RAM operates in a PC. RAM/DRAM contains the working or running copy of the configuration file. During normal operations, changes to the router's running configuration take place in RAM/DRAM.

The IOS contains commands to view each of the router's components. To view the contents of RAM, you can issue one of several commands (because several components reside in RAM). One of the most common commands is `show running-config`. This command displays the configuration running in RAM. This running configuration is also known as the current configuration or the working configuration. Typical output from this command is shown in Figure 5-16. Two other common commands that can show the contents of RAM are `show memory` and `show buffers`. Because they produce long, detailed output, their output has not been included in this text.

Another very useful command is the `show startup-config` command. With this command you can display the current startup configuration file on the router, which is stored in NVRAM. An administrator who wants to ensure that changes are maintained, even if the system is rebooted, must copy the running configuration to the startup configuration. The command to do this is as follows:

```
Copy running-config startup-config
```

This command is commonly abbreviated as follows:

```
Copy run start
```

These commands copy the configuration changes from RAM/DRAM to NVRAM. When the router is rebooted, the IOS will implement these changes through the startup-configuration file. If you want to combine your running configuration with the startup configuration stored in NVRAM, you can type `copy start run` at the privileged EXEC mode prompt.

## Interfaces

A router can ship with a variety of configurable interfaces. A common interface is Ethernet0, which is used to connect the router to an Ethernet LAN. Although this chapter focuses on the Ethernet, serial, console, and auxiliary interfaces, the router can have other types of interfaces, including:

- Token Ring
- Basic Rate Interface (BRI)
- Asynchronous Transfer Mode (ATM)
- Fiber Distributed Data Interface (FDDI)
- Channel Interface Processor (CIP) for Systems Network Architecture (SNA)
- High-Speed Serial Interface (HSSI)

**5**

```

Router#show run
Building configuration...

Current configuration : 927 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-enc
!
hostname Router
!
enable secret 5 $1$vdGT$08FE.EExWM5WWRQCPjDgc/
enable password cannon
!
interface FastEthernet0/0
  ip address 172.22.2.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0
  ip address 172.22.3.2 255.255.255.0
  no fair-queue
!
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
!
interface Serial0/1
  no ip address
  shutdown
!
Router rip
  network 172.22.0.0
!
ip http server
ip classless
!
line con 0
line aux 0
line vty 0 4
!
End

```

The `show run` command displays the configuration currently running in RAM

This router is configured to route IP on the FastEthernet0/0 and Serial0/0 interfaces

This router is using the RIP routing protocol to find best path information. RIP is discussed in detail in Chapter 7

**Figure 5-16** Output from `show running-config` command

You can view all of the configured interfaces for your router with the `show interfaces` command, as shown in Figure 5-17.



Configuration options for the Fast Ethernet and serial interfaces are covered in Chapter 6. The configuration options for the other interfaces are beyond the scope of this text.

## 136 Chapter 5 Router and IOS Basics

The `show interfaces` command lists a summary of the status of the interfaces. If both the Physical layer and Data Link layer protocols are up and running then the interface will be listed as up with line protocol up.

The Serial0/0 interface is listed as down with the line protocol down. There is a cable plugged into this interface but the other end of the cable is not plugged in so the interface isn't sensing a signal.

```
RouterB#show interfaces
```

```
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 0006.2872.73e0 (bia 0006.2872.73e0)
Internet address is 192.5.5.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 10Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
Serial0/0 is down, line protocol is down
```

```
Hardware is PowerQUICC Serial
Internet address is 201.100.11.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
FastEthernet0/1 is up, line protocol is administratively down
```

```
Hardware is AmdFE, address is 0006.2872.73e1 (bia 0006.2872.73e1)
Internet address is 205.7.5.1/24
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)
Auto-duplex, Auto Speed, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

The FastEthernet0/1 interface is listed as up with the line protocol administratively down. In this situation, the `no shutdown` command will often bring the interface back up.

Figure 5-17 Output from the `show interfaces` command

## Chapter Summary

- Cisco routers use the Cisco IOS to provide an interface for network operators and administrators.
- The first mode entered is user EXEC (router> prompt) and the next mode is privileged EXEC (router# prompt).
- In user EXEC, you can accomplish basic tasks such as checking the router status, checking connectivity, and viewing some configuration information.
- To actually configure the router, privileged EXEC mode must be accessed, as this mode leads to the two most common modes for router configuration: global configuration mode and interface configuration mode.
- The privileged EXEC mode is often called enable mode because it is entered using the enable command.
- The enable, enable secret, and VTY passwords are set during initial configuration if the system configuration dialog is used, but they can also be added and changed in global configuration mode (router(config)# prompt).
- When configured, the enable secret password supersedes the enable password because the enable secret is an encrypted password that is not viewable in the configuration file, which means that it has less chance of being compromised. For this reason, it should be different from the enable password.
- The components of a router include ROM, flash memory, NVRAM, RAM/DRAM, and interfaces.
- ROM stores a limited version of the Cisco IOS and routines for checking the hardware during system boot. It is responsible for initializing the router.
- Flash memory stores the Cisco IOS that is loaded by default during system boot.
- NVRAM stores the startup copy of the router configuration file that is loaded by default during system boot.
- RAM/DRAM stores the working copy (running configuration) of the router configuration. This configuration is loaded into RAM from NVRAM by default during bootup. It is erased if the router is rebooted, unless it is saved to the startup configuration.
- Interfaces provide connectivity to various types of LANs and WANs.

5

## Key Terms

**AUX line password** A password used to access the router through the AUX port.

**AUX port** See auxiliary port (AUX).

**auxiliary port (AUX)** A secondary port that allows connection to a modem that will be used for direct access to the router for configuration.

**bootstrap** A small program used to load a much larger program. In the case of a router or switch, the bootstrap program loads the IOS.

**Cisco Internetwork Operating System (IOS)** A router operating system that provides a command-line interface, which allows network operators to check the status of the router and allows network administrators to manage and configure the router.

**command executive** The user interface that interprets commands and is provided by the Cisco IOS (also known as the EXEC).

**console** A physical connection on the back of the router to which you can connect a rollover cable to attach to a PC for router configuration (also known as a console port).

**console password** The password that is used to access the router through the console port.

**console port** *See* console.

**context-sensitive Help** Help with the syntax of commands for the router that is based on the current router mode and prompt, as well as any part of a command that is typed.

**Coordinated Universal Time (UTC)** Based on the time in the city of Greenwich in the United Kingdom. All other time zones are either plus or minus hours of the time in Greenwich.

**dynamic random access memory (DRAM)** *See* random access memory (RAM).

**enable mode** Another name for the privileged EXEC mode. The enable or enable secret password must be entered in order to access this mode.

**enable mode prompt** The prompt that indicates operation in privileged EXEC or enable mode. It has two elements: the host name of the router and the pound (#) symbol.

**enable password** The password that protects enable mode in the event that the enable secret password has been removed.

**enable secret password** An MD5-encrypted password that is not visible when viewing the system configuration; it supersedes the enable password.

**EXEC** *See* command executive.

**flash memory** Erasable, programmable, read-only memory (EPROM). The content of flash memory is maintained when the router is rebooted. Flash memory contains the working copy of the Cisco IOS and it is the component that initializes the IOS for normal router operations.

**global configuration mode** A router mode that allows manipulation of most of the router's generic settings. The prompt for global configuration mode is router (config) #.

**interface configuration mode** A router mode that allows you to configure the Ethernet and serial interfaces. The prompt for this mode is router (config-if) #.

**line configuration mode** A router mode that allows you to configure the virtual terminals, console, and AUX lines that let you access the router. The prompt for this mode is router (config-line) #.

**MD5 algorithm** An algorithm used to encrypt an enable secret password.

**nonvolatile random access memory (NVRAM)** A special type of RAM that is not cleared when the router is rebooted. The startup configuration file for the router is stored in NVRAM.

**privileged EXEC mode** A router mode used to configure the router.

**random access memory (RAM)** Memory that stores the working copy of the router configuration. This configuration is erased if the router is rebooted, unless it is saved to the startup configuration.

**read-only memory (ROM)** Memory that contains the necessary routines to boot the system and check its hardware. It also contains a limited version of the Cisco IOS for use only when the primary copies of the IOS in flash memory or on a TFTP server are accidentally lost.

**RJ-45 to DB-9** A connector that ships with the router to enable connection to a PC with a DB-9 COM port to the router console port.

**RJ-45 to RJ-45 rollover cable** A cable that connects the console port on the back of the router to an RJ-45 to DB-9 connector on the back of a PC. This cable ships with the router.

**ROM monitor mode** A router mode that allows you to configure your router in the event that no valid IOS file is in your flash memory.

**router configuration mode** A router mode that allows you to enable routing protocols such as RIP and IGRP. The prompt for router configuration mode is `router (config-router) #`.

**router#** See enable mode prompt.

**router>** See user EXEC mode.

**system configuration dialog** An automated setup routine that runs if you type “setup” from privileged EXEC mode or if the router is started/restarted without a configuration file.

**5**

**Trivial File Transfer Protocol (TFTP) server** A computer that provides TFTP services and can be used to maintain the IOS and configuration file of a Cisco router.

**user EXEC mode** A router mode that allows a network operator to check router status, see if the interfaces are operational, and review several of the router settings.

**user mode** See user EXEC mode.

**virtual terminal password** A password that is used to access the router over a telnet connection.

**virtual terminals (VTY)** Terminals provided with each Cisco router that can be used by telnet sessions to configure the router.

**volatile** Contents of memory that are lost when the power is turned off. RAM is an example of volatile memory.

**VTY** A Cisco IOS abbreviation for virtual terminal used in commands to reference virtual terminals.

---

## Review Questions

1. The running configuration is also known as the \_\_\_\_\_. (Choose all that apply.)
  - a. startup configuration
  - b. working configuration
  - c. current configuration
  - d. backup configuration
2. If you type `e?` at the `router (config) #` prompt, what is the result of the command?
  - a. You will see a list of usable commands at the global configuration mode prompt.
  - b. You will see a list of usable commands at the global configuration mode prompt that begin with the letter “e.”
  - c. You will see a list of usable commands at any prompt that begins with the letter “e.”
  - d. You will see the configuration register settings.

**140** Chapter 5 Router and IOS Basics

3. If you need to abort a command in the middle of execution, which key sequence should you press simultaneously?
  - a. Ctrl+Esc
  - b. Ctrl+X
  - c. Ctrl+Shift+6
  - d. Ctrl+Alt+Del
4. Which of the following commands will allow you to type a banner for your router?
  - a. router(config-if)# banner message \$
  - b. router(config)# banner motd @
  - c. router(config)# banner msg #
  - d. router# banner config !
  - e. router# banner motd #
5. By default, which of the router's components stores the backup configuration file?
  - a. ROM
  - b. Flash
  - c. IOS
  - d. NVRAM
6. If you are in global configuration mode, which router prompt will you see?
  - a. global#
  - b. router(config)#
  - c. router(config-if)#
  - d. router#
  - e. router(config-g1)#
7. By default (during normal boot operations), where does the router look first for a working version of the Cisco IOS?
  - a. NVRAM
  - b. TFTP
  - c. Flash
  - d. ROM
8. What three commands can you use in privileged EXEC mode to alter the router configuration?
  - a. setup, erase, and copy
  - b. enable, setup, and tftp
  - c. setup, show version, and show buffers
  - d. erase, copy, and show run
9. ROM in a router is nothing like ROM in a PC. True or False?

10. From which of the following prompts can you modify the terminal VTY password?

- a. router(config-line) #
- b. router#
- c. router>
- d. router(config)>

11. What does VTY 1 stand for?

- a. the first virtual Y connector
- b. virtual terminal one
- c. virtual test connection yes on 1
- d. v-modem terminal 1

**5**

12. How do network administrators access a VTY?

- a. ftp
- b. smtp
- c. telnet
- d. http

13. If, after connecting to the router via HyperTerminal, you see only illegible characters in the terminal window, what should you try?

- a. Adjust the baud rate.
- b. Change connectors.
- c. Use a telnet session.
- d. Turn on parity.

14. If you enter a VTY password during the automated setup routine, to which VTY will it apply? (Choose all that apply.)

- a. VTY 0
- b. VTY 1
- c. VTY 2
- d. VTY 3
- e. VTY 4

15. What are the two different levels of setup when using the system configuration dialog?

- a. initial and basic
- b. enable and enable secret
- c. basic and extended
- d. none of the above

16. How do you save your changes to the configuration file to NVRAM?

- a. copy start run
- b. copy run start
- c. copy start flash
- d. copy run flash

**142** Chapter 5 Router and IOS Basics

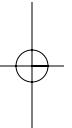
17. From the `router#` prompt and the terminal, what must you type to enter global configuration mode?
  - a. CON 0
  - b. term gf
  - c. conf t
  - d. global conf
18. If you are at the `router(config-if)#` prompt and you press the Ctrl+Z keys simultaneously, which prompt will you see next?
  - a. router>
  - b. router#
  - c. router(config)#
  - d. Press Return to continue
19. Which of the following commands will allow you to enter privileged EXEC mode from the `router>` prompt? (Choose all that apply.)
  - a. en
  - b. ena
  - c. enable
  - d. enab
  - e. enabl
20. What does the `sh ru` command show you?
  - a. remote users
  - b. running configuration
  - c. startup configuration
  - d. remote boot procedure
21. Which password you use used instead of the enable password?
  - a. VTY 0
  - b. console
  - c. AUX
  - d. enable secret
  - e. login
22. Which password is encrypted by default?
  - a. login
  - b. MD5
  - c. enable
  - d. enable secret
  - e. console
  - f. VTY 0

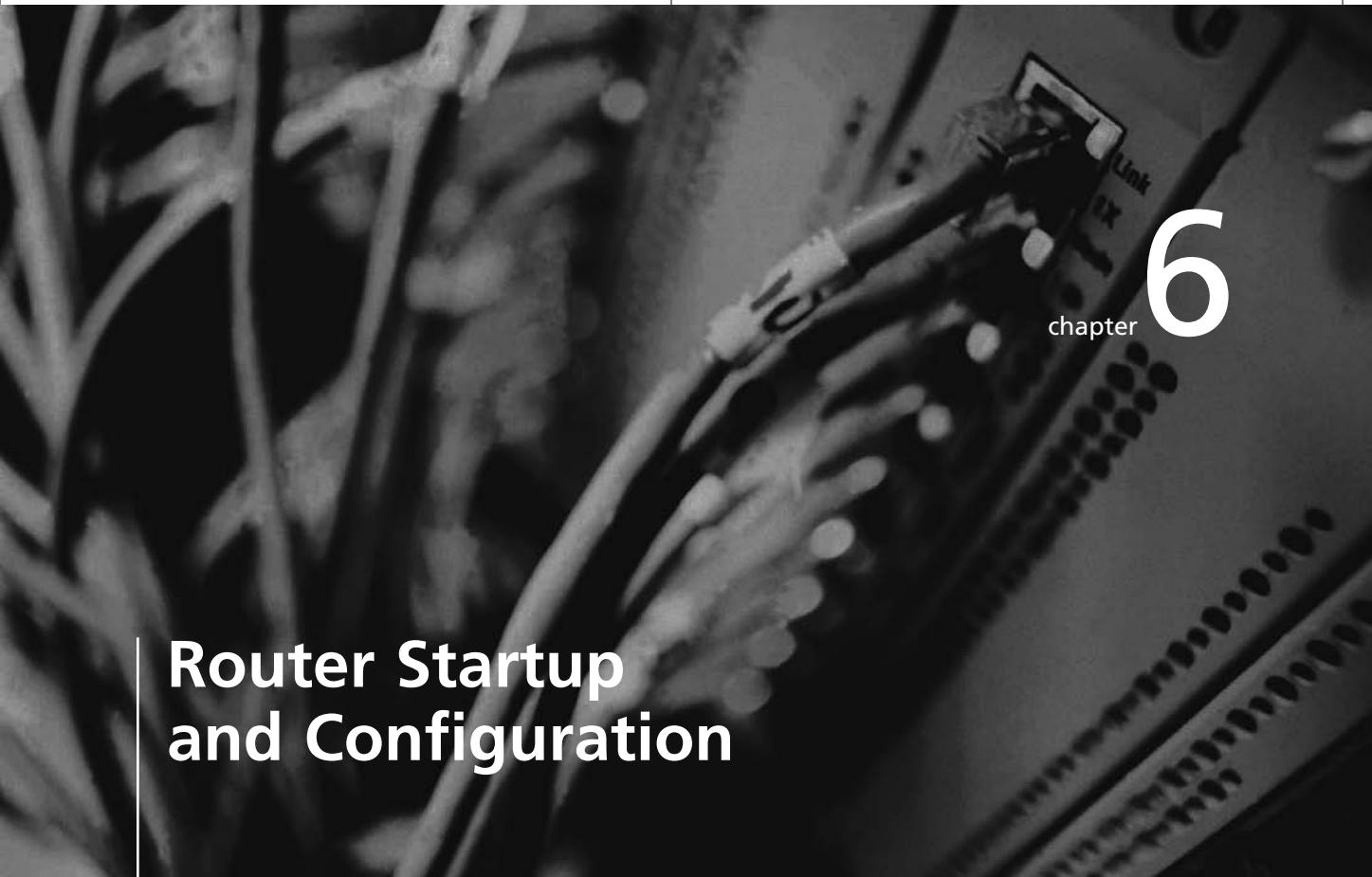
## Case Projects



1. Jennifer and Moe brought a client's router to the office to configure, but they are not sure how to make the physical connections. They want to use a PC in Brad's office to configure the router. The COM2 port is available on this PC, and it has a DB-9 connector. How would you suggest the router be accessed? What hardware will you need? Where will you get the hardware?
2. You have helped Moe and Jennifer connect the router to the PC. Now, it is time to access the router and configure it. The PC is running the Windows XP operating system. What program will you use to access the router? What important parameters must be configured in this program, and what will the initial settings be?
3. Moe and Jennifer have accessed the router successfully. Explain to them which passwords the system configuration dialog will prompt them for during the initial configuration. Describe any particulars regarding the passwords. What other passwords are available to them? When and why might they want to implement these additional passwords?
4. Moe is a terrible typist. Lisa tells him to stop wasting time retying router commands and use the command history and enhanced editing features of the Cisco IOS. When Moe asks her how to do this, she says that she does not remember exactly how the features work. Help Moe and Lisa by explaining to them the easy way to edit router commands. How do you retrieve previously typed commands? How do you move the cursor forward and back along the command line?
5. Lisa is planning to take a CCNA practice exam on the Internet. She is having a difficult time memorizing the components of the Cisco router. List the router components for her and give a brief description of the purpose of each component. How do similar components in a typical PC compare to the router components you have listed?

**5**





chapter  
**6**

# Router Startup and Configuration

**After reading this chapter and completing  
the exercises, you will be able to:**

- Describe the steps involved in starting a router
- Describe and use the Cisco Discovery Protocol
- Configure IP on the Cisco router
- Troubleshoot router connectivity problems

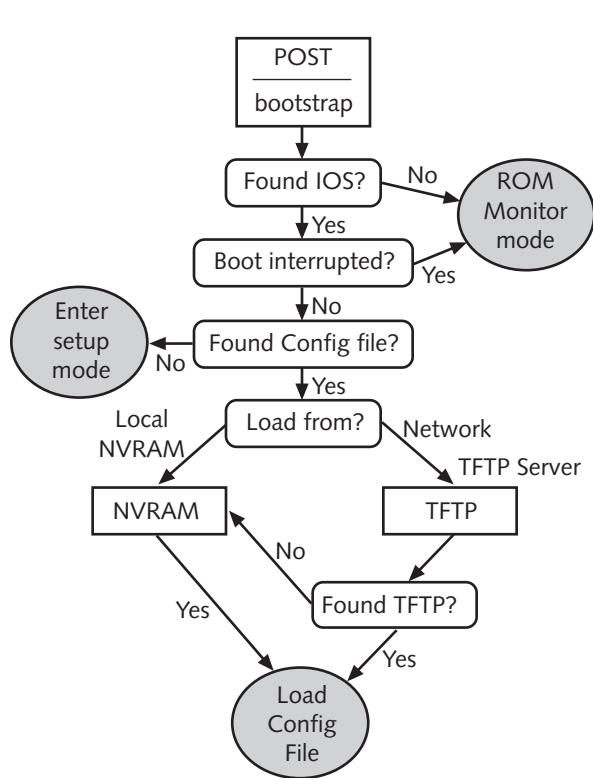
**In this chapter, you will learn about the various configurable components** of the Cisco router and how to manipulate them. The chapter describes basic router configuration and administrative tasks, and introduces the CDP protocol and its configuration. In addition, you will learn how to configure and test IP. You will also learn the steps involved in troubleshooting connectivity problems on a Cisco router.

## Router Startup

A router follows a specific boot process, but the steps in this process can vary from one router to the next. This section discusses the variety of startup options available during the boot process. In general, the boot process follows these steps:

1. Test hardware (POST).
2. Load the bootstrap program.
3. Locate and load the Cisco IOS.
4. Locate and load the router configuration file.

Figure 6-1 illustrates a simplified version of the basic flow of the boot process. The steps in the flowchart are discussed in greater detail in the following subsections.



**Figure 6-1** The boot process

## Test Hardware (POST)

Read-only memory (ROM) in a router typically contains the power-on self-test (POST), the bootstrap program, and often a version of the operating system. Most types of computer equipment perform some type of POST immediately after being turned on. POST is a diagnostic test that determines if the hardware is operating correctly. During the POST, the bootstrap program, also called the **ROM Monitor**, checks basic operations of the attached hardware, including CPU, memory, and interfaces. The ROM Monitor checks the **configuration register** for instructions regarding how to load the Cisco IOS. ROM Monitor and the configuration register are discussed in more detail later in this chapter.

## Router Configuration Files

The router configuration file that loads during the boot process is called **startup-config**. Sometimes this file is referred to as the backup configuration because it is the saved version of the configuration file. Any time you want to revert to the settings in your startup-config, you can reboot the system by powering the router off and back on again, or by issuing the **reload** command at the privileged EXEC mode prompt. As long as you have not saved the running configuration on top of the startup configuration, the running configuration in RAM will be dumped when you reload, and the saved version in NVRAM will be loaded into RAM. It is important to note that when you copy over the startup configuration in NVRAM, that file is replaced. However, when you copy to the running configuration in RAM, either from NVRAM or from a TFTP server, the configuration files are blended.



A **Trivial File Transfer Protocol (TFTP) server** is a computer, such as a PC, UNIX workstation, or laptop that is running TFTP server services. A Cisco router can also operate as a TFTP server. TFTP software allows the Cisco router to transfer the IOS image and router configuration files to the TFTP server via TFTP, a simple connectionless protocol that is less complex than FTP. Many free distributions of TFTP software are available on the Web.

In other words, the resulting working configuration will be a combination of the startup configuration file in NVRAM (or the one on the TFTP server) and the current working configuration in RAM. In addition, there is no **erase run** command. If you want to get rid of the running configuration, you must reload either by command or by turning the router off and on.

If you want to view the contents of the startup-config, you can type **show startup-config** or just **show start** at the enable prompt. If you want to see your working or running configuration, type **show running-config** or just **show run** at the enable prompt.

Table 6-1 lists the most important copy commands and configure commands. If you are curious about additional commands, type **copy ?** at the enable prompt.

## 148 Chapter 6 Router Startup and Configuration

Command from Enable Mode	Description
copy running-config tftp	Copies the running configuration located in RAM to a TFTP server.
copy startup-config tftp	Copies the startup configuration located in NVRAM to a TFTP server.
copy tftp running-config	Copies the configuration from the TFTP server to the running configuration. The reconfiguration of the router is immediate when this command is issued. The running-config is not replaced. The files are blended.
copy tftp startup-config	Copies the configuration from the TFTP server to the startup configuration. The startup-config is replaced with the one from the TFTP server.
copy run start	Copies the working configuration file in RAM to the startup configuration file in NVRAM. Replaces the startup configuration file.
copy start run	Copies the startup configuration file in NVRAM to the running configuration in RAM. Does not replace the file in RAM; the files are blended.
copy flash tftp	Copies the IOS in flash memory to a TFTP server.
copy tftp flash	Copies the IOS from a TFTP server to flash memory.
configure terminal	Used to specify that you want to configure your settings manually from the console terminal.
configure memory	Used to specify that you want to pull your configuration information from NVRAM.
configure network	Indicates that you want to load your working configuration from a TFTP server.
configure overwrite-network	Indicates that you want to overwrite the existing NVRAM with the configuration information stored on the TFTP server.
erase startup-config	Erases the current startup configuration. When you reboot the router, you will be prompted to enter the automated setup program.

**Table 6-1** Important copy and configure commands

Notice there is no copy command that copies between flash and a running or startup configuration file. It is important to think of the IOS and configuration files as separate. The IOS is a relatively large file that is the entire operating system, whereas the configuration files are very small and modify the operation of the router.

## Methods for Making Changes

When changes to the router's configuration or boot process are required, the administrator should follow a logical process for making those changes. Remember that you can usually implement and test changes without saving them to the startup configuration, because changes to the running configuration take place immediately. Almost everything can be done in RAM (running-config). When you are satisfied that the changes are correct, you can

copy the running configuration to the startup configuration. Follow these basic steps to implement changes:

1. Make changes as desired to the configuration.
2. Examine those changes.
3. Determine if the changes meet the desired result.
4. Remove the changes if they do not meet the desired result, or simply reboot the router.
5. Copy the changes from the running configuration to the startup configuration when they do meet the desired result.

If the administrator makes changes that should be tested by rebooting the router, then he or she can copy the startup configuration to a TFTP server first. This way, if the changes do not meet the desired result, those files can be copied back to the router from the TFTP server.

6

## IP on the Router

If the router is initially configured using the initial configuration dialog, you will be asked if you want to enable IP on your router. If you answer yes, you will be prompted to configure IP on each of the interfaces that you want to configure. If you answer no, you can either run setup again later, or you can configure the interfaces manually.

To manually configure IP on an interface, you must first change to interface configuration mode. Then, you can use the `ip address` command to configure an IP address for the specific interface. For example, if you want to configure the IP address 192.168.1.1 with the default Class C subnet mask for the FastEthernet interface, type the following from enable mode:

```
Router#config t
Router(config)#int f0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

Notice that the subnet mask was included in the `ip address` command. The command would be incomplete without the subnet mask. You can also add the word `secondary` to an `ip address` command and configure the address as a second IP address for the interface. Also notice the addition of the `no shutdown` command. This command will enable the interface. In the event you are configuring a serial interface as a **DCE (data communication equipment)**, you will also need to add the `clockrate [bandwidth in bits per second]` command.



If you want to change the way the subnet mask is shown when you view statistics about an interface, type “term ip netmask-format” at the enable mode prompt. You will have to choose decimal, bit-count, or hexadecimal to complete the command; the default is decimal. If you choose bit-count, the mask is displayed in CIDR format.

## IP Connectivity

Once you configure the router for IP, you should test for connectivity. Several commands can help you verify this connectivity. These commands apply to various layers of the OSI model, as described in Table 6-2.

Command	OSI Layer	TCP/IP Layer
telnet	Application layer	Application layer
ping	Network layer	Internetwork layer
trace	Network layer	Internetwork layer
show ip route	Network layer	Internetwork layer
show interfaces	Data Link and Physical layers	Network Interface layer

**Table 6-2** Testing connectivity by layer

When testing connectivity, if you cannot get a connection at a higher layer, check the connectivity of a lower layer. For example, if you cannot get a telnet connection, you should attempt to ping the host to which you are trying to connect.

## Telnet

Telnet is a utility that connects at the highest layer of the OSI model and provides remote access to other devices. Cisco routers allow telnet connections via their virtual terminal ports. If you can establish telnet connectivity to a router, you have established that it is available on the network and that you have connectivity at all layers. After you establish telnet connectivity, you can learn more about the configuration of the remote router by executing commands as if you were connected to the router locally.



If you accidentally initiate a connection with another router from your locally attached router, you can stop the process by pressing Ctrl+Shift+6. You can use this key combination to stop any command from running. You can also use the logout command at the user EXEC or privileged EXEC mode prompt. This will log you out of the remote router but maintain the connection with your local router.

## IP Host Names

When telnetting to a remote router or host, the IP address of the host must follow the telnet command. Rather than using IP addresses, it is easier to refer to a remote host or router using a name. Sometimes, you cannot gain connectivity because the host name that you are trying to connect with is entered in a table incorrectly. For example, suppose you are trying to telnet into router15, but the address for router15 is configured incorrectly on your system. To determine the address to name mapping on your router, check the name table by issuing the following command:

```
router#show hosts
```

You will then see a list of the names configured on your router. If you want to add an entry to your hosts file for name resolution, you must go to **global configuration mode**. For example, if you want to add an entry telling your router that router15 is at IP address 192.168.5.1, type:

```
router(config)#ip host router15 192.168.5.1
```

If later you want to remove that entry, type:

```
router(config)#no ip host router15 192.168.5.1
```

If you find that one of the entries in your host table is incorrect, you can remove it and enter the correct mapping. You can also allow a name server to handle the IP address to name resolution. For example, if you want to specify that a name server with IP address 172.33.44.1 be used by the router for name resolution, enter the command:

```
router(config)#ip name-server 172.33.44.1
```

Then, when a known name is used, the name server will be consulted to provide name resolution for the router. In this example, if you type ping router3, the router will ping the IP address of router3 based on the name resolution in the table located on the device with the IP address 172.33.44.1. Using a name server provides name resolution from one location, making a table configuration on each router unnecessary.

6

## Ping and Trace

If you can not get connectivity at the Application layer, try connectivity at the Internetwork layer. Ping and Trace are available from the user EXEC and privileged EXEC mode. Ping and Trace verify connectivity at the Internetwork layer of the TCP/IP model. Both utilities use ICMP messages to verify that the destination host is reachable, and if not, give possible reasons for the problem. Ping sends an echo request packet to the destination and waits for an echo reply. By default, the Ping utility with Cisco routers is configured to send five packets to the target. Ping can return the following replies:

- !: Successful receipt of the ICMP echo
- ..: Request timed out
- U: Destination was unreachable
- C: Congestion experienced
- I: Ping interrupted
- ?: Packet type unknown
- &: Packet TTL exceeded

Additional information returned from Ping includes the quantity of ICMP packets sent, the timeout duration, the transfer success rate, and the minimum, average, and maximum round trip times for the ICMP packets sent.

If you simply type ping and then press the Return key at the enable mode prompt, you will be able to enter your ping command step by step. You also will be able to control the protocol type (for example, IPX rather than IP), the size of the ping packet, the number of packets sent, and other options. Using the ping command alone is referred to as **extended mode ping**. Extended mode Ping can only be accessed from the enable mode prompt.

Ping is a quick way to determine if internetwork layer connectivity is present. If Ping indicates a problem with connectivity, using Trace may provide a better clue as to the source of the problem. The trace command is similar to the ping command, except that the replies are requested at each hop along the way to the destination. Trace sends multiple ICMP packets with progressively higher time-to-live counters (TTL) until the packet reaches the destination. If three routers are located between the destination and the source of the trace, there will be four replies to the message—one for each hop along the way and one when the trace reaches

the final destination. The `trace` command is useful for determining where in the process the communication is breaking down. The following responses can be returned by a trace:

- !H: Indicates that a router received, but did not forward, the ICMP echo request
- P: Protocol unreachable
- N: Network unreachable
- U: Port unreachable
- \*: Request timed out

## IP Route

If you cannot get connectivity using Ping or Trace, you should check your routing table. If the routing table is sending communications out of the wrong interface, or if there is no entry in the routing table that will handle routing to the target network, it will cause your higher-level connectivity to fail. You can issue the `show ip route` command from the enable mode prompt. This command displays the routing table. Typically, routing tables are dynamically created when routing protocols are configured on the router. If you want, you can use the `ip route` command from the global configuration mode to statically enter routes in the routing table. Very often a routing table will consist of routes learned both through dynamic and static means. Routing is covered in more detail in Chapter 7.

## Checking the Interface

One of the biggest mistakes made when troubleshooting is not checking the interfaces on the router. If the interfaces are down, packets cannot be received or delivered. Router interfaces go down for a variety of reasons, including incorrect IP configuration and cable problems. You can use the `show interfaces` command to view the configuration of IP on your interfaces and to check the status of the interface.

You can check the configuration of a specific interface from the enable mode prompt with the `show interfaces` command. For example, if you want to check the statistics for Serial0/0, type:

```
router#show int s0/0
```

The first line, which reports the status of the interface, is made up of two elements: The first reports the physical status of the interface, and the next reports the status of the line protocol. If the interface and protocol are fully functional, you will see the following information:

```
Serial0/0 is up, line protocol is up
```

This report means that both the interface and line protocol are functioning properly. In other words, the interface is functioning at both the Physical and Data Link layers. You may also see one of the following replies:

- **Serial0/0 is up, line protocol is down**—This tells you that the interface is not receiving any network data or **keepalive frames**, but the physical interface is up and operational. This typically indicates a problem with the router configuration. Check the running configuration using the `show run` command. Make sure routing protocols and static routing commands have been properly configured. Also make sure that the IP address for the interface was entered correctly. On serial interfaces, you will also get this report if the router to which your router is connected through this interface is down. In other words, the remote attached router can push your router interface down.
- **Serial0/0 is up, line protocol is administratively down**—This indicates that you need to use the `no shutdown` command on this interface to bring the

interface back up. This typically happens when configurations are copied to the router from a file or TFTP server.

- **Serial0/0 is down, line protocol is down**—This indicates that the router interface is nonfunctional. This usually occurs when there is no cable attached to the interface, the cable is bad, or the router interface at the other end of the cable is shut down.



NOTE

Different types of interfaces can show different types of reports. For example, a Token Ring interface reports down when no electrical carrier signal is present.

```
lab-c#show interfaces
FastEthernet0/0 is up, line protocol is up ←
    Hardware is AmdFE, address is 0007.85b1.2140 (bia 0007.85b1.2140)
    Description: Attached to FastEthernet LAN lab-c
    Internet address is 223.8.151.1/24
    MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Half-duplex, 10Mb/s, 100BaseTX/FX
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input never, output 00:00:02, 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
Serial0/0 is administratively down, line protocol is down ←
    Hardware is PowerQUICC Serial
    Internet address is 204.204.7.1/24
    MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation HDLC, loopback not set
    Keepalive set (10 sec)
    Last input never, output never, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0 (size/max/drops); Total output drops: 0
    Queueing strategy: weighted fair
    Output queue: 0/1000/64/0 (size/max total/threshold/drops)
        Conversations 0/0/256 (active/max active/max total)
        Reserved Conversations 0/0 (allocated/max allocated)
    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, 0 no buffer
Serial0/1 is up, line protocol is administratively down ←
    Hardware is PowerQUICC Serial
    Internet address is 199.6.13.2/24
    MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation HDLC, loopback not set
    Keepalive set (10 sec)
    Last input never, output never, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0 (size/max/drops); Total output drops: 0
    Queueing strategy: weighted fair
    Output queue: 0/1000/64/0 (size/max total/threshold/drops)
```

Interface f0/0 is fully functional. Frames can be sent and received on this interface.

Interface s0/0 is not functional. In this case there is no cable connection.

Interface s0/1 is not functional but will become functional once the no shutdown command is used on the interface.

**Figure 6-2** Output from the show interfaces command

**Clear Counters** The router keeps detailed statistics regarding data passing across its interfaces. Before using the `show interfaces` command, you may want to clear the existing interface information. You can clear these statistics (counters) on the interface by using the `clear interface` or `clear counters` command. To clear the counters for interface f0/0, type the following:

```
router#clear interface f0/0
```

If you want to clear the counters on all attached interfaces, use the `clear counters` command.

**Debug** One of the most powerful tools you can use to obtain information from your router is the `debug` command. This tool is only available from privileged EXEC mode. Debug has numerous subcommands that allow you to troubleshoot particular protocols. If you want to see all of the debugging counters available, you can use the `debug all` command. However, the `debug all` command will seriously affect router performance, so you should avoid experimenting with debug on a production router. Output from the `debug all` command is displayed in Figure 6-3.

Issuing the `debug all` command displays a warning that this procedure may cause network problems. Only use this command for a short period of time as a troubleshooting tool.

```
lab-c#debug all
This may severely impact network performance. Continue? [confirm] ←
All possible debugging has been turned on
Local MobileIP: aging arp mobility cache entries
00:28:17: RIP-TIMER: periodic timer expired
00:28:17: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (223.8.151.1)
00:28:17: RIP: build update entries - suppressing null update
00:28:18: DHCPD: checking for expired leases.
00:28:45: RIP-TIMER: periodic timer expired
00:28:45: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (223.8.151.1)
00:28:45: RIP: build update entries - suppressing null update
00:28:48: CDP-PA: version 2 packet sent out on FastEthernet0/0
Local MobileIP: aging arp mobility cache entries
00:29:12: RIP-TIMER: periodic timer expired
00:29:12: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (223.8.151.1)
00:29:12: RIP: build update entries - suppressing null update
00:29:42: RIP-TIMER: periodic timer expired
00:29:42: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (223.8.151.1)
00:29:42: RIP: build update entries - suppressing null update
lab-c#no debug all ←
All possible debugging has been turned off
```

Any command can be negated by putting the word no in front of it.

**Figure 6-3** The `debug all` command output

With `debug`, you can also check for specific types of traffic on the wire. For example, if you want to perform general IP packet debugging, type the following:

```
router#debug ip packet
```

Details regarding IP packets received by the router will be displayed. Again, the debug command is powerful but it is also resource-intensive, and should not be run for extended periods of time due to its negative impact on router performance. Use the debug command only when necessary to check network traffic; use the no debug command to disable debugging when you are finished. For example, to turn off all or any debugging you would type:

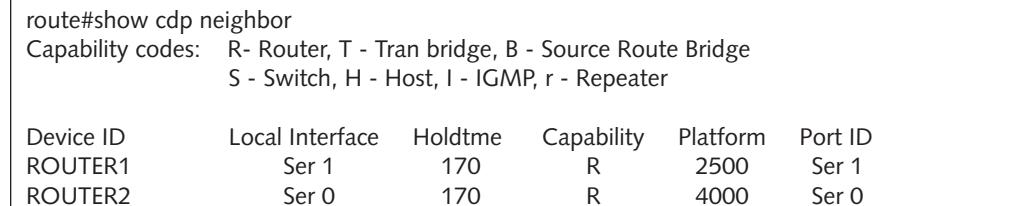
```
router#no debug all
```

You can also type undebug all. Additional debug commands are introduced in later chapters.

## CDP

The **Cisco Discovery Protocol (CDP)** is a Cisco proprietary Data Link layer protocol that shares configuration information between Cisco devices that are connected directly to each other. All Cisco devices, including routers, switches, and wireless access points, can use CDP to discover each other and learn about the configurations of other devices. Using CDP can help you quickly determine the network topology.

With CDP, you can discover other devices on the same LAN segment and those connected over a serial interface. Figure 6-4 illustrates the CDP feedback after the show cdp neighbors command has been issued.



route#show cdp neighbor					
Capability codes: R- Router, T - Tran bridge, B - Source Route Bridge					
S - Switch, H - Host, I - IGMP, r - Repeater					
Device ID	Local Interface	Holdtme	Capability	Platform	Port ID
ROUTER1	Ser 1	170	R	2500	Ser 1
ROUTER2	Ser 0	170	R	4000	Ser 0

**Figure 6-4** The show cdp neighbors command

The show cdp neighbors command supports the following options:

- *FastEthernet*—To learn more about FastEthernet interfaces attached to neighbors
- *Serial*—More information about neighbors connected to serial interfaces
- *Detail*—Detailed information about the CDP neighbor and all attached devices. This detailed information includes device identification, remote interface type, and remote IP address.

CDP was designed to be a low-overhead protocol. CDP broadcasts information every 60 seconds by default. You can modify the length of time between updates by using the cdp timer command. The CDP command is the same for routers and Cisco IOS-enabled switches. For example, to change CDP to update every 120 seconds, type:

```
router(config)#cdp timer 120
```

**156** Chapter 6 Router Startup and Configuration

The CDP information is only held for a set length of time, which is 180 seconds by default. You can modify the length of time that the CDP information is held by issuing the `cdp holdtime` command. For example, to configure CDP packets to be discarded after one minute, type:

```
router(config)#cdp holdtime 60
```

In this example, the CDP information is discarded after 60 seconds. By default, CDP is enabled on all Cisco devices, but you can modify CDP broadcasts on the network. To turn off CDP on the entire router, use the `no cdp run` command at the global configuration prompt. If you want to disable CDP information from being sent on a given interface, change to the interface configuration mode prompt, and then issue the `no cdp enable` command. For example, to remove CDP broadcasts from your FastEthernet0/0 interface, enter the following from enable mode:

```
router#config t
router(config)#interface f0/0
router(config-if)#no cdp enable
```

You can use the `show cdp interface` command in enable mode to retrieve the statistics that CDP will report on the local router's interfaces.



**NOTE**

As an administrator, you can learn about a network's topology by using the `telnet` command in combination with the `show cdp neighbors` or `show cdp neighbors detail` command. Simply telnet into one of the virtual terminals and issue the `cdp` commands that you would use locally to determine attached Cisco devices. CDP is now considered somewhat of a security vulnerability, and you should turn off CDP unless you absolutely need it.

---

## Cisco IOS

The Cisco IOS is usually loaded from flash memory. Figure 6-5 displays the output from a Cisco 2600 series router during bootup under this default condition. If the router cannot find the IOS in flash memory, it will look for a copy on a TFTP server. If it cannot find one there, it will boot a minimal version of the IOS from ROM.

If you want to see information about your router's flash memory, type `show flash` from the enable mode prompt. Figure 6-6 displays the output from the `show flash` command.

### Configuration Register

Every Cisco router has a 16-bit configuration register, which is stored in NVRAM. This register allows you to control several boot functions, including:

- Forcing the system into the bootstrap program
- Enabling or disabling the console Break function
- Setting the console terminal baud rate
- Loading the IOS from ROM
- Loading the IOS from a TFTP server

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)  
Copyright (c) 2000 by cisco Systems, Inc.  
C2600 platform with 49152 Kbytes of main memory

program load complete, entry point: 0x80008000, size: 0x7c94cc  
Self decompressing the image : ##### [OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, California 95134-1706

Cisco Internetwork Operating System Software  
IOS (tm) C2600 Software (C2600-DO3S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)  
Copyright (c) 1986-1999 by cisco Systems, Inc.  
Compiled Tue 07-Dec-99 03:49 by phanguye  
Image text-base: 0x80008088, data-base: 0x80DAD0E8

cisco 2620 (MPC860) processor (revision 0x600) with 39936K/9216K bytes of memory  
.Processor board ID JAD054009NW (3938354089)  
M860 processor: part number 0, mask 49  
Bridging software.  
X.25 software, Version 3.0.0.  
1 FastEthernet/IEEE 802.3 interface(s)  
4 Serial(sync/async) network interface(s)  
32K bytes of non-volatile configuration memory.  
16384K bytes of processor board System flash (Read/Write)

Press RETURN to get started!

**Figure 6-5** Output from the Cisco 2600 series router on bootup

```
lab-c#show flash

System flash directory:
File  Length   Name/status
 1    8164840  aaa1346.bin
[8164904 bytes used, 8612312 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)
```

The IOS filename in flash is aaa1346.bin

**Figure 6-6** Output from the show flash command

## 158 Chapter 6 Router Startup and Configuration

You can examine the configuration register by typing show version at either the enable mode or user mode prompt. Figure 6-7 displays the output of the show version command.

```
lab-c#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-DO3S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 07-Dec-99 03:49 by phanguye
Image text-base: 0x80008088, data-base: 0x80DAD0E8

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

lab-c uptime is 11 minutes
System returned to ROM by power-on
System image file is "flash:aaa1346.bin" ← The IOS filename is aaa1346.bin

cisco 2620 (MPC860) processor (revision 0x600) with 39936K/9216K bytes of memory
.
Processor board ID JAD054009NW (3938354089)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
4 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102 ← The configuration register setting of 2102 specifies that the IOS will be loaded from flash memory as long as there are no boot system commands in NVRAM that specify otherwise. This is the default setting.
```

**Figure 6-7** Output from the show version command

The last line of this output will read Configuration register is followed by a hexadecimal code. The last four digits of the code specify system boot instructions. The very last hexadecimal digit determines from where the IOS will load. The first three hex digits of the last four control other aspects of how the router will operate after it boots. Table 6-3 describes the various IOS boot locations and the typical configuration register values.

Configuration Register	Description
0x2100	Boot into ROM Monitor mode
0x2101	Boot helper image from ROM (RxBoot mode)
0x2102	Check the startup configuration file in NVRAM for boot system commands; load IOS from flash if nothing else is specified. Note that the last digit in 0x2102 can be anything from 2 to F but is usually 2.

**Table 6-3** Configuration register codes

## ROM Monitor Mode

ROM Monitor mode is actually the bootstrap program that is built into the firmware of the router. In addition to initializing the hardware and loading the IOS, ROM Monitor can be used to perform other tasks such as diagnostics and recovering passwords. You can set the router to enter ROM Monitor mode during the boot process by modifying the configuration register. The router will also enter ROM Monitor mode if it cannot find an IOS image during the boot process. The prompt for ROM Monitor mode on the Cisco 1003, 1600, 2600, 3600, 4500, 7200, and 7500 routers is some variation of `rommon>`.



NOTE

On most Cisco routers, you can press the Ctrl+Break keys within the first 60 seconds of the boot process to enter ROM Monitor mode. For security purposes, you must be physically connected to the router via the console port in order for this key combination to work.

6

To configure your system to enter ROM Monitor mode, you can enter the following command at the global configuration prompt:

```
router(config)#config-register 0x2100
```

The 0x2100 is just one example of a hexadecimal register setting that would boot the router into ROM Monitor mode. The important factor is that the last number is 0. To configure your system to boot a smaller IOS image from ROM and enter RxBoot mode, you must enter the following command at the global configuration prompt:

```
router(config)#config-register 0x2101
```

Once again, it is the last hexadecimal digit that forces the router to boot into RxBoot mode. RxBoot mode is described in the next section. To confirm your changes, go to the privileged EXEC mode or user EXEC mode prompt, and then type `show version`. The last line, depending on your previous actions, should have (will be 0x2100 at next reload) or (will be 0x2101 at next reload). You can reboot using the `reload` command. When the router reboots, the ROM Monitor will load the IOS as specified in the configuration register.

Be careful when modifying the configuration register. Using ROM Monitor mode will not cause problems, but entering random hexadecimal commands above 0x0002 may present a variety of problems. Modifying your configuration in this manner is only advisable when there is no other course of action.

## RxBoot Mode

As previously mentioned, ROM in the router contains a limited version of the IOS. This version can be accessed when changes to your system make it impossible to boot from the flash memory and you cannot locate a valid IOS image. When accessing this limited IOS version, you are in **RxBoot mode**. Entering RxBoot mode is often done intentionally when you want to access a TFTP server to download a new IOS. It is typically accomplished by setting the configuration register to 0x2101, then reloading. If your router enters RxBoot mode without your intervention, it means the router could not find a good IOS image. This happens if the IOS in flash is corrupt or has been erased. The prompt for RxBoot mode is the host name of your router followed by `boot` in parentheses. For example, if your router's name is `router2`, the prompt would be `router2(boot)`. In this mode you will

**160** Chapter 6 Router Startup and Configuration

have access to a subset of the Cisco IOS commands used in the normal user EXEC and privileged EXEC modes.

## Boot System Commands

You may want to alter the default sequence for loading the IOS. For example, routers are sometimes configured to boot their IOS image from a TFTP server. You can alter the default sequence by configuring boot system commands.

As long as the configuration register is configured with a 2 as the final hexadecimal digit, the ROM Monitor will look for boot system commands in NVRAM during the bootup process.

A typical IOS filename might look like this: c2600-i-mz.123-15b.bin. If you wanted to enable your system to boot that IOS file from the TFTP server, you would issue the following command from global configuration mode:

```
router(config)#boot system tftp c2600-i-mz.123-15b.bin
```

This command would be broadcast so that a computer running TFTP software would respond. If you entered the show run command, you would see “boot system tftp c2600-i-mz.123-15b.bin 255.255.255.255” in the configuration.



The boot system flash bootflash command will force the router to boot into ROM.

**NOTE**

You can enter as many boot system tftp commands as you want for redundancy. This ensures that your system can boot from a TFTP server, even if the primary server is not available. When you view your configuration after entering multiple boot system tftp commands, you will see multiple boot system lines in the configuration. Boot system commands are executed in the order in which they are entered. To remove any given line, type no boot system tftp, followed by the IOS filename at the global configuration prompt. Remember, if you want these modifications to be applied to your startup configuration, you must type the following at the privileged EXEC mode prompt to ensure that your changes are applied to the startup configuration in NVRAM:

```
copy run start
```

## Backing Up and Restoring the IOS

You should have a backup of your router's IOS. This is especially important when it comes time to upgrade the IOS, because you may have to erase the current IOS first. In addition, the upgrade may not work and you may need to restore the previous IOS version. The command for backing up your IOS to a TFTP server is copy flash tftp. You will be asked for the source filename, the IP address of the TFTP server, and the destination filename. Typically, the destination filename is the same as the source filename and this is the default. Once you have a backup, it is safe to erase the IOS if that is necessary. Type erase flash at the privileged EXEC mode prompt. At this point the only IOS image on the router will be the limited version in ROM. To restore the deleted IOS or a new image to the router, type copy tftp flash and provide the TFTP server IP address and IOS image filename when prompted.



Using the `erase flash` command will remove the IOS from your router, essentially making it nonfunctional. This should only be done in rare cases and when the IOS has been successfully backed up.

NOTE

## Upgrading the IOS

Before you load a new IOS file to your router, use the `show flash` command to ensure there is enough free memory to hold it. The system will tell you how much memory is used and how much is free. If there is not enough memory to hold both the current IOS image and the upgrade, you will have to erase the existing flash memory as previously mentioned.



If you abort the copying process in the middle of copying a new flash memory, your existing flash memory will still be active, assuming that you have not erased it already.

NOTE

6

---

## Router Password Recovery

Sometimes a password is forgotten or compromised. A procedure called **password recovery** on Cisco routers allows you to get into the router without the necessary passwords. For security reasons, you cannot perform the password recovery procedure through telnet or other remote means. You must be physically connected to the router using the console cable. The procedure differs slightly depending on the router series. The password recovery instructions for all router series are on the Cisco Web site at [www.cisco.com](http://www.cisco.com). The steps to perform password recovery on the Cisco 2600 series are:

1. Connect to the router from a PC using the console port and the HyperTerminal program, as described in Chapter 5.
2. If you have access, enter the `show version` command and record the value of the configuration register (e.g., 0x2102). If you can not access the router configuration, you should assume that the configuration register is 0x2102.
3. Turn the router off and on using the power switch.
4. Press Ctrl+Break several times within the first 60 seconds of bootup to break out of the normal boot routine and enter ROM Monitor (`rommon`) mode.
5. At the `rommon 1>` prompt, type `confreg 0x2142` and press Enter. This instructs the router to boot the IOS from flash without loading the configuration from NVRAM.
6. Enter the `reset` command at the `rommon 2>` prompt. The router will reboot.
7. Enter `no` if asked to enter the system configuration dialog.
8. When you get to the `Router>` prompt, enter `enable` to get to privileged mode.
9. Enter the `copy start run` command to load the saved configuration file from NVRAM into RAM. Press Enter to accept the default destination name.
10. Enter the `show run` command to view the configuration. You will be able to see all unencrypted passwords. Any encrypted passwords will have to be reconfigured. To change the `enable secret` command, enter the following commands:

```
Router#config t
```

```
Router(config)#enable secret [secret password]
```

## 162 Chapter 6 Router Startup and Configuration

11. Enter config-register 0x2102 (or the configuration register value you recorded in Step 2) at the global configuration mode prompt to make sure the router reboots in the default manner.
12. Enter the copy run start command to save your changes.

## Security Device Manager

You have learned several ways to configure a Cisco router. The most common configuration method is typing in commands from the command line interface (CLI). You can also use the system configuration wizard, or download a configuration file from a tftp server. A CCNA must also be familiar with yet another way to configure a Cisco router: the **Security Device Manager (SDM)**. SDM is a Web-based tool primarily used for implementing and testing security configurations; it is also available as a free download. SDM can be used with many router models and a wide range of IOS releases. It is most commonly used to configure routing protocols, WAN services, wireless routing, firewalls, virtual private networks (VPNs), and quality of service (QoS). Most of these more advanced concepts will be addressed in later chapters. It is important to note that SDM is typically not used to configure basic functionality on a Cisco router and, in fact, SDM cannot do all things. However, SDM does help with the most complex configuration commands and it allows testing of the configuration. If there is a problem, SDM will even help troubleshoot it for you. In short, SDM makes it easier for network administrators to implement complex configurations requiring many commands much more easily and without the CLI knowledge that was necessary in the past. You can practice with SDM even without a router connected by downloading the demo. You will do this in Lab 6.6. A screenshot of the demo is shown in Figure 6-8.

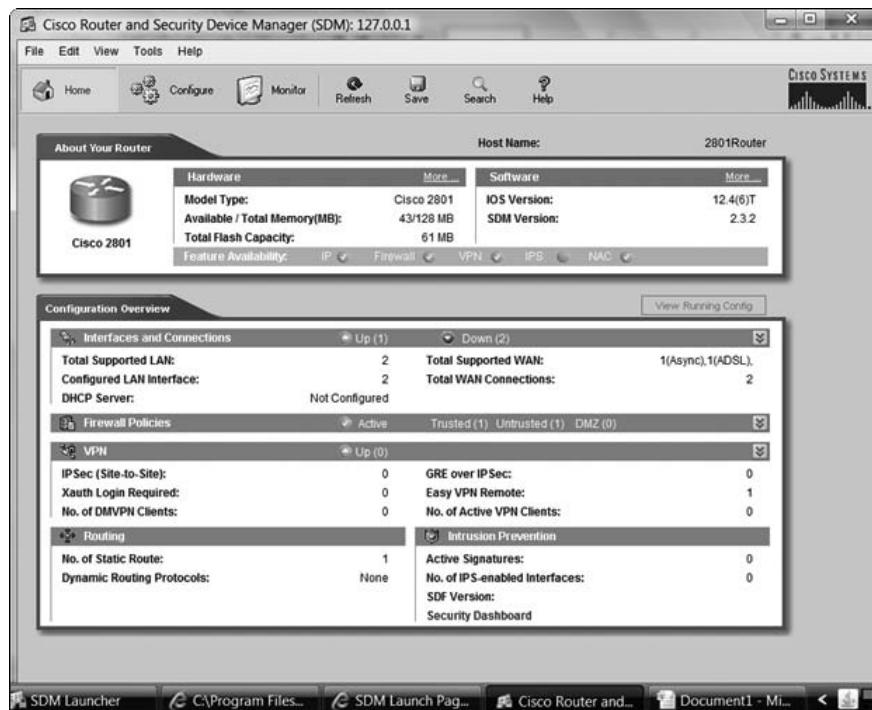


Figure 6-8 Security Device Manager Demo

## Chapter Summary

- When a router boots, it follows a set routine.
- Although a router's boot process can vary, the typical boot process follows a standard sequence. First, the router checks all of its internal hardware components during a process called the POST (power-on self-test). Next, the router loads the basic configuration routine, known as the bootstrap program, from ROM. Then, the bootstrap attempts to locate the Cisco IOS, which in turn loads the router configuration file.
- If the Cisco IOS is set to load from a TFTP server, but the TFTP server cannot be located, then the IOS will boot from flash memory.
- If the IOS cannot be found in flash memory or on the TFTP server, then a limited version will boot from ROM.
- If the Cisco IOS is set to load a configuration file from a TFTP server, but the file or server is not available, the configuration file will be loaded from NVRAM. However, if a configuration file is not available in NVRAM or on a TFTP server, then the automated setup routine will be initialized.
- The Cisco Discovery Protocol (CDP) is proprietary to Cisco devices. This protocol shares information between Cisco devices about other local Cisco devices.
- CDP uses broadcasts to update neighbors every 60 seconds by default (the update time interval is configurable).
- Devices share information about their interface configurations and connections to other devices.
- You can verify router connectivity to other systems by using telnet to determine if there is Application layer connectivity.
- If you cannot get connectivity at the Application layer, try Trace and Ping. Then, check your routing table with the `show ip route` command to determine if there is a problem with the Network layer.
- One of the most important troubleshooting commands is the `show interfaces` command. If your interfaces are not up, you cannot route packets.
- Cisco's Security Device Manager (SDM) is a Web-based tool designed to help you configure Cisco routers. While it does not do everything, it simplifies configuring complex router scenarios primarily involving security.

6

## Key Terms

**Cisco Discovery Protocol (CDP)** A Cisco proprietary Data Link layer protocol that shares configuration information between Cisco devices that are locally connected.

**configuration register** A feature in Cisco routers that is stored in NVRAM and allows the administrator to control several boot functions.

**counters** Detailed statistics kept by a router about data passing across its interface.

**DCE (data communication equipment)** Equipment that performs some type of signal conversion between the terminal device and the transmission facility. Usually the DCE is part of the telco provider's equipment.

**164** Chapter 6 Router Startup and Configuration

**extended mode ping** When you type ping at the privileged EXEC prompt and then press the Return or Enter key, you will be presented with ping options. Extended mode ping options include the destination address of the ping, the protocol, repeat count, and datagram size.

**global configuration mode** A router mode that allows you to manipulate most of the router's generic settings. The prompt for global configuration mode is router(config)#.

**keepalive frames** Data frames sent between two hosts to ensure that the connection between those hosts remains open.

**password recovery** A method of bypassing the router passwords. This cannot be done remotely.

**power-on self-test (POST)** A diagnostic program in ROM that runs when the router is powered on. POST checks hardware availability.

**ROM Monitor** A bootstrap program that runs during the power-on self-test and checks basic operations of hardware, including CPU, memory, and interfaces.

**ROM Monitor mode** A router mode in which you can configure the router manually.

**RxBoot mode** A configuration mode that can be entered when changes to a system make it impossible to boot from the flash memory and a valid IOS image cannot be located.

**Security Device Manager (SDM)** A Web-based tool for configuring complex security and other parameters on a Cisco router.

**startup-config** The router configuration that loads from NVRAM into RAM when the router boots up.

**Trivial File Transfer Protocol (TFTP) server** A computer, such as a PC, laptop, or UNIX workstation, that can be used to maintain Cisco IOS versions and Cisco router configuration files. TFTP is a protocol that is used to copy files back and forth from a computer running TFTP server services.

---

## Review Questions

1. If you want to see the hexadecimal boot setting for the configuration register, which command would you use? (Choose all that apply.)
  - a. router> sh int
  - b. router> sh ver
  - c. router#sh ver
  - d. router#sh int
  
2. When the trace command is used, multiple packets are sent to a remote destination with:
  - a. progressively higher TTL values until a packet reaches the destination
  - b. progressively lower TTL values until a packet is returned from the destination
  - c. progressively smaller hop counts
  - d. pull routing tables

3. If you want to configure the values that Ping uses and have access to extended mode ping options, which of the following represents the appropriate prompt and the command you would type before pressing the Enter key?
- router#ping
  - router#ping ex md
  - router#ping motd
  - router> ping
  - router#ping -e
  - router> ping -e
4. What is usually stored in NVRAM? (Choose all that apply.)
- configuration register
  - backup copy of the IOS
  - limited version of the IOS
  - configuration file
5. Which of the following connectivity utilities use ICMP messages for troubleshooting the connection? (Choose all that apply.)
- Ping
  - Telnet
  - Trace
  - IP route
  - Show version
6. Which layer of the OSI model contains the telnet utility?
- Application
  - Network
  - Data Link
  - Physical
  - Transport
7. Which of the following information is *not* visible after you issue a ping?
- quantity of ICMP packets sent
  - timeout duration
  - success rate
  - MAC address
  - round trip times
8. If the packet type is unknown, what does Ping report?
- !
  - .
  - ?
  - U

**166** Chapter 6 Router Startup and Configuration

9. Which of the following commands are considered incomplete or will not be recognized by the router's IOS? Assume that the Enter key is pressed immediately after the command. (Choose all that apply.)
  - a. router> ping 192.168.1.1
  - b. router#ping
  - c. router> ping
  - d. router#config
  - e. router> config
10. Which of the following maps the route from HostA to HostB across the Internet?
  - a. show ip route command
  - b. Ping
  - c. Trace
  - d. Finger
11. If the configuration register is set to 0x2102, where will the system look for boot instructions?
  - a. Flash
  - b. NVRAM
  - c. RAM
  - d. ROM
12. If there are no specific instructions to the contrary, from where does the system attempt to load the IOS?
  - a. ROM
  - b. RAM
  - c. NVRAM
  - d. Flash
13. If you want to see information about other Cisco devices attached to your router, which of the following commands would you use?
  - a. show cisco neighbor
  - b. show cdp neighbors
  - c. show cdp config
  - d. initiate cdp scan
14. What is the purpose of CDP?
  - a. to communicate hardware information between Cisco and non-Cisco routers
  - b. to communicate hardware information between switches and hubs
  - c. to communicate hardware information between Cisco routers and switches
  - d. to update routing tables

15. Which of the following is the final step in the router boot process?
- Locate and load Cisco IOS
  - Load bootstrap
  - Locate and load router configuration file
  - POST
16. Which of the following occurs after the loading of the bootstrap?
- Test hardware
  - Configuration register is examined to determine from where to load the IOS
  - Locate and load router configuration file
  - POST
17. What is another name for enable mode? **6**
- Enable secret mode
  - Privileged EXEC mode
  - Login mode
  - User mode
18. By default, what will happen if the IOS cannot be found in flash memory?
- The router attempts to load a minimal copy from ROM.
  - The router uses CDP.
  - The router contacts an HTTP server.
  - The router automatically shuts down.
19. If the router is configured to load the IOS from a TFTP server, where will the router look next for the IOS?
- ROM
  - Flash
  - FTP server
  - HTTP server
  - CDP
20. Which command could you use to back up the IOS to a TFTP server?
- copy IOS tftp
  - copy flash tftp
  - copy rom tftp
  - copy running-config tftp
21. If you want to see information about other Cisco devices attached to your router, including their IP addresses, which of the following commands would you use?
- show cisco neighbors
  - show cdp neighbors

**168** Chapter 6 Router Startup and Configuration

- c. show cdp neighbors detail
  - d. show cdp neighbors Ethernet
22. What command is used to erase the configuration file on a Cisco router?
- a. erase startup config
  - b. delete start
  - c. disable nvram
  - d. delete nvram
23. The show interfaces command displays the following output: FastEthernet0/0 is up, line protocol is administratively down. What do you infer?
- a. There is no cable attached to the FastEthernet0/0 interface on the router.
  - b. The no shutdown command needs to be configured on the FastEthernet0/0 interface.
  - c. Incompatible routing protocols have been configured on the router.
  - d. There is a physical problem with the Fast/Ethernet0/0 interface on the router.
24. What is the purpose of a hosts file on a router?
- a. to allow you to use host names instead of IP addresses when referring to network devices
  - b. to facilitate ARP on the router
  - c. to allow routers to see other devices on the network
  - d. to block unwanted hosts from using the router
25. What is the purpose of SDM?
- a. to allow configuration of a Cisco router using the CLI
  - b. to allow configuration of a Cisco router using a Web-based tool
  - c. to allow configuration of a Cisco router using menu codes
  - d. to allow remote password recovery

---

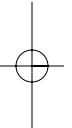
## Case Projects



CASE PROJECTS

1. Lisa and Moe are discussing the CDP protocol. They know it was developed by Cisco and is not part of any protocol suite with which they are familiar. What can you tell them about CDP? Specifically, what is the purpose of this protocol? With which OSI layer is it associated? Is it enabled by default? What is the update interval? On a router, how do you turn it on and off? On a single interface on a router, how do you turn it on and off? Why might you want to turn it off?
2. Moe and Jennifer have configured a router for a client. With the network administrator's help, they have connected it to the client's network. Unfortunately, it is not working. They have called you for guidance. What troubleshooting steps do you recommend?

3. While configuring a client's router, Moe types the `erase flash` command. What are the consequences of this action? What steps will the router go through when it boots if the router is not configured to boot from a TFTP server?
4. Moe is embarrassed about erasing the router's flash memory. Lisa thinks the company has a backup flash file on a TFTP server. They have got you on the phone, and they want you to step them through the procedure to recover the router's operating system. The IOS filename is `c2600-i-mz.123-15b.bin`.





7  
chapter

# Routing Protocols

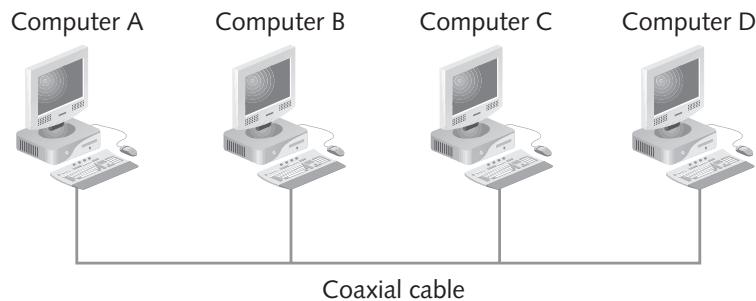
**After reading this chapter and completing the exercises, you will be able to:**

- Differentiate between nonroutable, routed, and routing protocols
- Define Interior Gateway Protocols, Exterior Gateway Protocols, distance-vector routing protocols, and link-state routing protocols
- Explain the concepts of count-to-infinity, split horizon, split horizon with poison reverse, and hold-down timers
- Describe, configure, and monitor the interior routing protocol RIP
- Explain static routing and administrative distance
- Configure static routing and default routes

**This chapter explains the concepts of nonroutable, routed, and routing** protocols, with a discussion of major protocols in each category. The chapter also examines the distinction between distance-vector and link-state routing protocols. In addition, you will learn the proper way to configure and monitor the Routing Information Protocol (RIPv1) on Cisco routers. This chapter also presents the concepts and techniques required to configure static routing and default routes.

## Nonroutable Protocols

In the early days of networking, networks were small collections of computers linked together for the purposes of sharing information and expensive peripherals such as high-end laser printers. Few companies could afford to link all their computers together on a local area network (LAN). Instead, using coaxial cable, computers were hooked together in work-groups. Figure 7-1 shows a typical early network.



**Figure 7-1** Early network model using coaxial cable

Early networks were sometimes configured as **peer-to-peer networks**, in which computers communicate with and provide services to their “peers.” Peer-to-peer networks do not pass packets between multiple networks. All communication occurs on the one network segment where the peer-to-peer network exists.

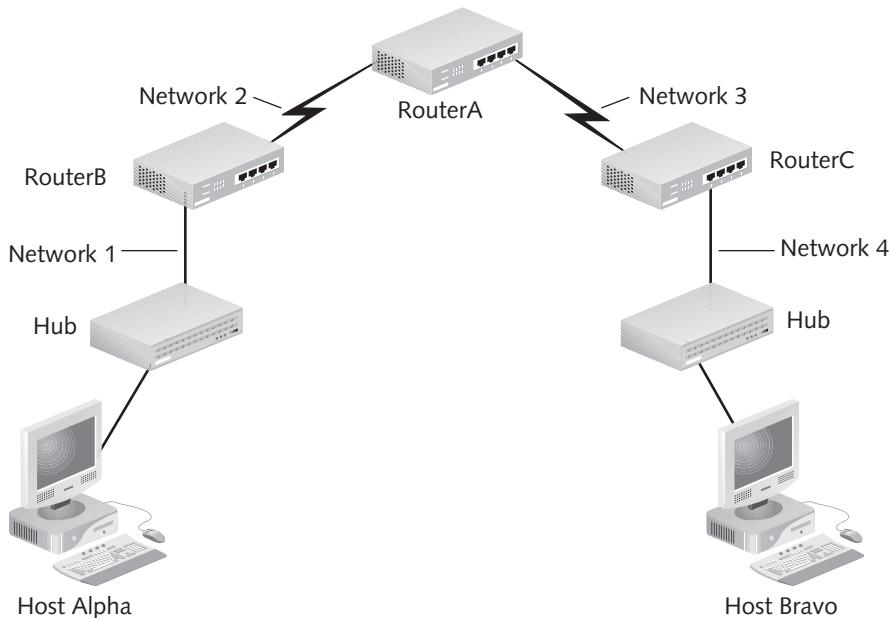
Due to the localized nature of traffic on a peer-to-peer network, network source and destination information is not needed and would produce unnecessary overhead. Instead, peer-to-peer networks can use small and efficient nonroutable protocols.

Several **nonroutable protocols** exist in today’s networking world, but NetBEUI, short for NetBIOS Enhanced User Interface, is the most common. NetBEUI ships with all Microsoft Windows operating systems. In small, peer-to-peer networks, NetBEUI is easy to configure and use. It is also fast and efficient.

Unfortunately, NetBEUI cannot scale into large internetworks because it cannot hold Network layer information in its network header. Without this information, packets cannot be routed between multiple network segments. Therefore, if you try to use NetBEUI—or any nonroutable protocol—in a network with multiple networks, communication between the networks will fail.

## Routed Protocols

**Routed protocols** have packet headers that can contain Network layer addresses. Routed protocols were developed to support networks consisting of multiple networks or subnetworks. Figure 7-2 shows a typical **internetwork** within which routed protocols, such as TCP/IP or IPX/SPX, are used.



**Figure 7-2** Common internetwork

In this sample internetwork, Host Alpha can communicate with Host Bravo only if Host Alpha uses a protocol that can add Network layer addressing to each packet header. With this Network layer addressing, information from Alpha can traverse the internetwork from Network 1 to Network 4. Without the Network layer information, all packets are only able to communicate within Network 1. **Transmission Control Protocol/Internet Protocol (TCP/IP)** and **Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)** are two protocols that can carry Network layer information. Thus, routers can route them through an internetwork.



IPX/SPX is a proprietary protocol suite developed by Novell. While it is routable, it cannot be routed across the Internet like TCP/IP and therefore is limited.

**NOTE**

For routed protocols to work on a network, every device (computer, printer, and router interface port) must be configured with a unique IP or IPX address. These Network layer **logical addresses** allow TCP/IP or IPX/SPX packets to be routed throughout the internetwork. Figure 7-3 shows the sample network with IP addresses assigned to each device.

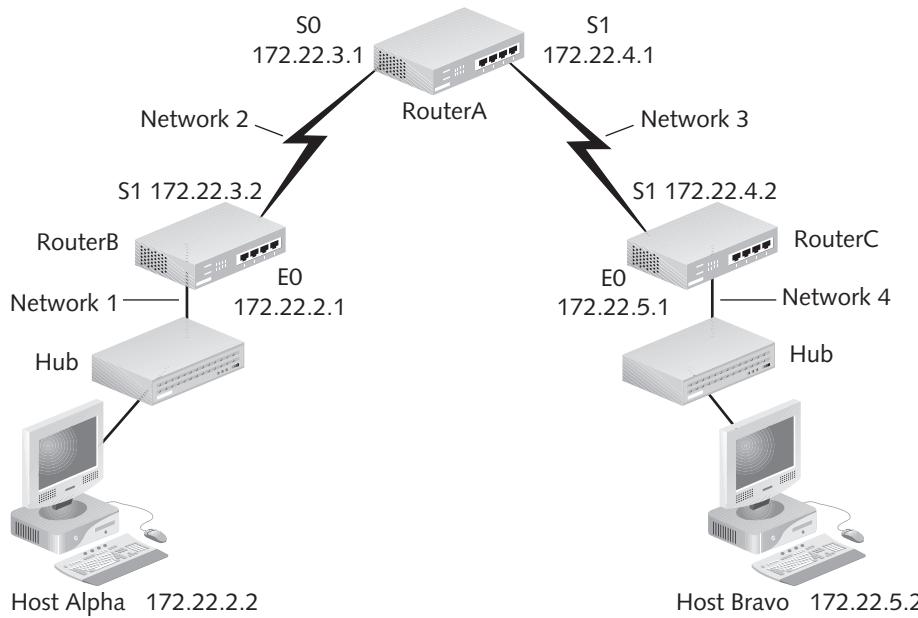


Figure 7-3 Common internetwork with IP addresses

## Routing Protocols

For proper network connectivity, you need more than just routed protocols on large internetworks. In order for routers to find the correct path for routed protocols, they use routing protocols to build routing tables that specify where every network in the internetwork is located. The administrator can also build routing tables statically; static routing is described later in this chapter. **Routing protocols** are protocols used by routers to make path determination choices and to share those choices with other routers. Table 7-1 shows a conceptual routing table that RouterB in Figure 7-3 would use to route a TCP/IP packet from Network 1 to Network 4.

Network	Path	Distance
Network 2	Available via RouterB	Directly connected
Network 3	Available via RouterA	1 hop
Network 4	Available via RouterC	2 hops

Table 7-1 Conceptual routing table

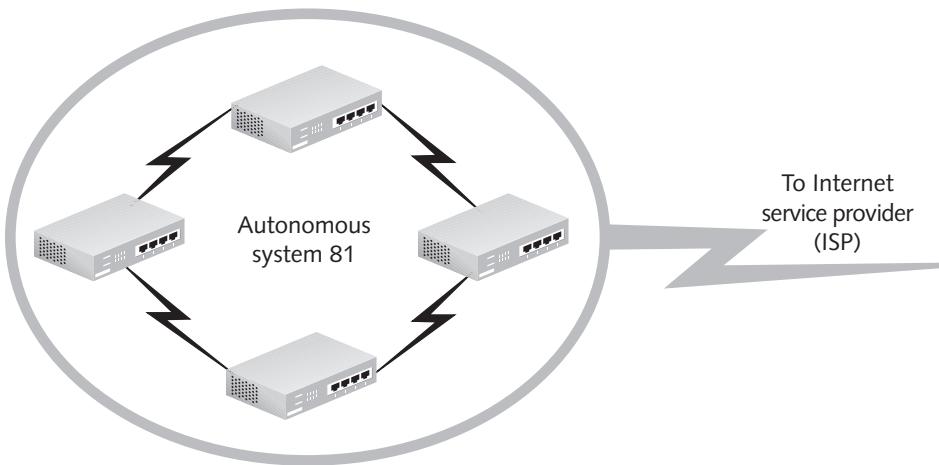
This table shows that RouterB can reach any of the networks in the internetwork. The Distance column refers to hop count as the single metric used in this routing table. **Hop count** is the number of routers a packet must pass through to reach a particular network. A **metric** is a

value used to define the suitability of a particular route. In other words, routers use metrics to determine which routes are better than other routes.



In the internetwork shown in Figure 7-3, routing metrics are simple because of the single-path nature of the internetwork. The route to Network 4 from RouterB will be via RouterA and RouterC; there is no better path available.

An **autonomous system (AS)**, which uses Interior Gateway Protocols as routing protocols, is a group of routers under the control of a single administration. Figure 7-4 shows Big Tin Inc.'s AS.



**Figure 7-4** Big Tin Inc.'s AS

Big Tin Inc. has an autonomous system consisting of four routers under the control of local network engineers. In general, an AS runs a single routing protocol.

Routing protocols come in two major categories: **Interior Gateway Protocols (IGPs)** are the routing protocols used within an AS, and **Exterior Gateway Protocols (EGPs)** are routing protocols used to route information between multiple autonomous systems.

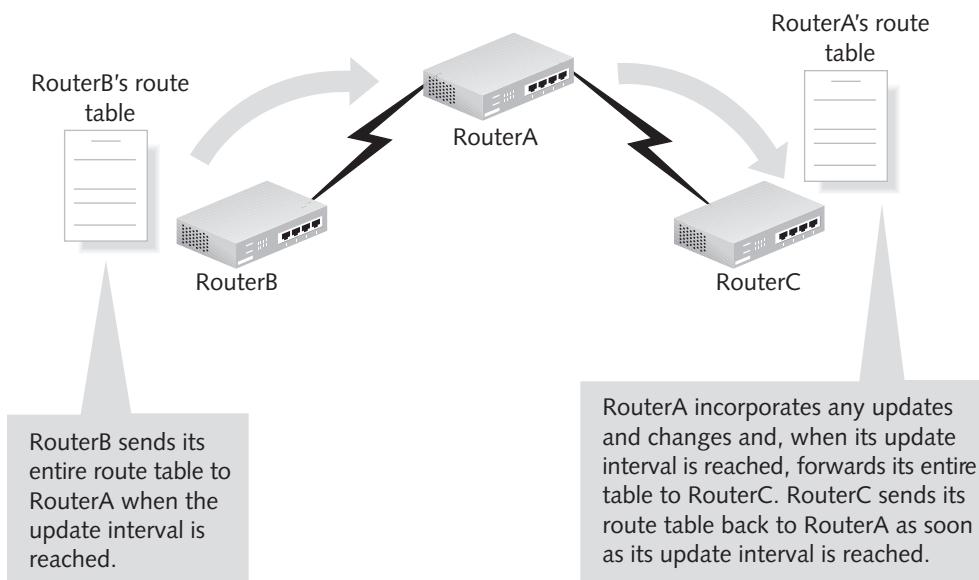
**Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF)** are examples of IGPs. RIP and IGRP are distance-vector routing protocols, and OSPF is a link-state routing protocol; these two protocol categories are discussed in the following section. EIGRP is a hybrid routing protocol developed by Cisco to overcome some of the limitations associated with IGRP, in particular, and distance-vector routing protocols in general. As a hybrid routing protocol, EIGRP combines the best attributes of both distance-vector and link-state routing protocols. Additionally, EIGRP, when used with the `no auto summary` command, can support variable-length subnet masking (VLSM). EIGRP, like IGRP, is Cisco proprietary and can only be used between Cisco routers. IGRP has been replaced by EIGRP in the most recent versions of the Cisco IOS.

**Border Gateway Protocol (BGP)** is an example of an EGP. EGPs are the other category of routing protocols and are generally covered in depth in a CCNP Routing course.

## Two Types of IGPs

IGPs are subdivided into two major types: **distance-vector** and **link-state**. These protocol types accomplish the same task—determining routes within an autonomous system—but they do so via different mechanisms.

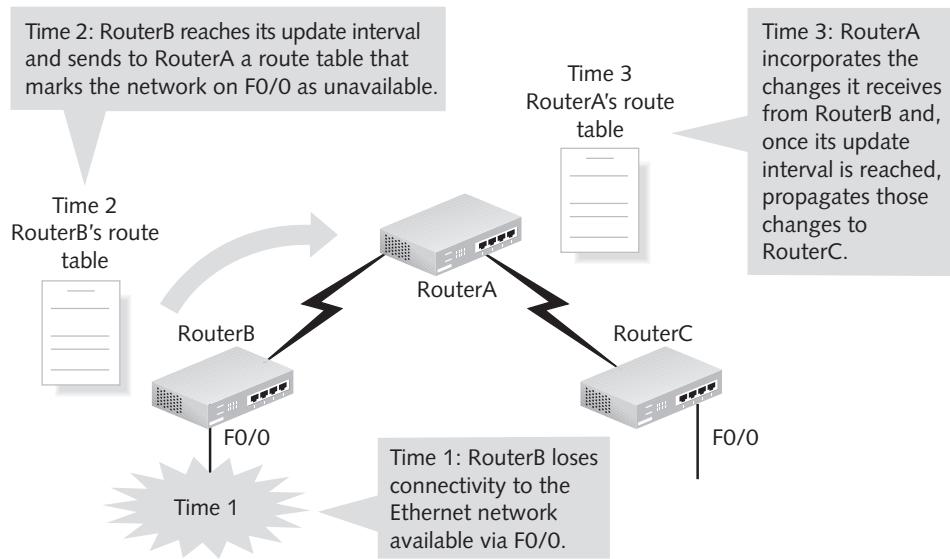
**Distance-Vector Routing Protocols** Distance-vector routing protocols broadcast their entire routing table to each neighbor router at predetermined intervals. The actual interval depends on the distance-vector routing protocol in use, but varies between 30 and 90 seconds. Figure 7-5 shows how this process occurs.



**Figure 7-5** Distance-vector routing protocol process

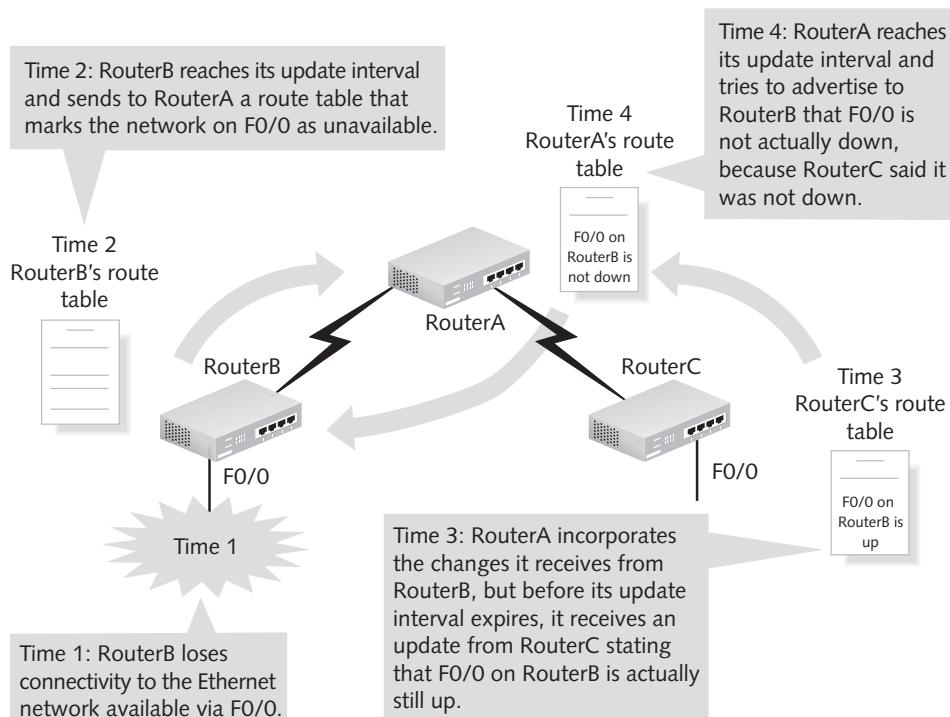
As the updates propagate throughout the network, RouterC will only receive information about RouterB's routing table via RouterA. This is sometimes referred to as **routing by rumor**. It is also one of the main problems with distance-vector routing protocols. If RouterB and RouterA have an update interval of 30 seconds, RouterC will not learn about network topology changes (changes in router interface states or route metrics) on RouterB for up to a minute. Figure 7-6 shows the types of problems this slow time to convergence can cause. **Convergence** is a state where all routers on the internetwork share a common view of the internetwork routes.

Figure 7-6 shows that the time it will take the network to converge depends on the amount of time between update intervals on RouterB and RouterA. Given the small size of this sample network, the amount of time to converge would be fairly minimal. Still, for a short amount of time, RouterC mistakenly believes the Ethernet network attached to RouterB is viable and continues routing packets addressed to hosts on that network.



**Figure 7-6** Distance-vector convergence example

Problems, such as routing loops, can occur with distance-vector protocols if control measures are not put in place. **Routing loops** are often referred to as **count-to-infinity** problems because loops, without preventive measures (described next), will cause packets to bounce around the internetwork infinitely. Figure 7-7 illustrates the types of problems that can occur with routing loops.



**Figure 7-7** Distance-vector convergence problems

In this internetwork, true loops are not possible because of the linear nature of the network design. Still, the scenario presented in Figure 7-7 shows that the internetwork could, without proper precautions, readvertise a route that was actually not accessible. To prevent these problems, techniques such as defining a maximum, split horizon, split horizon with poison reverse, and hold-down timers are used to reduce the chances that incorrect routing table information will be propagated. Each technique is described below.

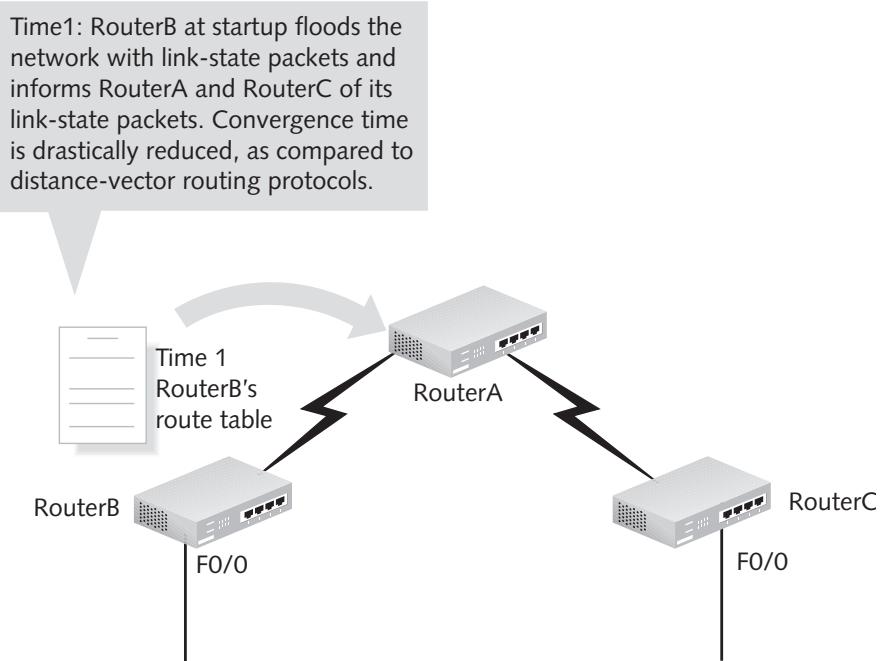
**Defining a maximum** is one of the easiest ways to limit count-to-infinity problems. If you assign a packet a maximum hop count, it cannot bounce infinitely around the internetwork. RIP, one of the most common distance-vector protocols, defines a maximum hop count of 15. Therefore, if a routing loop did occur on a RIP internetwork, the packet would only travel through 15 routers before the packet exceeded its TTL and was dropped. In other words, the 16th router that the packet tried to cross on a RIP internetwork would see that the packet had exceeded its TTL and would drop the packet. In the internetwork illustrated in Figure 7-7, packets could potentially bounce around infinitely. For the RIP (version 1) routing protocol, hop count is the sole metric used to determine the relative desirability of a particular path.

**Split horizon** and **split horizon with poison reverse** are two other common ways to prevent routing loops when using distance-vector routing protocols. Split horizon controls what information a router will send out through a particular interface. In short, a router will not send route information that it learned originally through an interface back through the same interface. For example, if RouterA in Figure 7-7 uses split horizon, it will not accept the update regarding F0/0 on RouterB from RouterC at Time 4. (Time 4 in Figure 7-7 represents the time when RouterC's update interval expires and RouterC sends out its update table.) It will not accept the update because it would need to be sent out of the interface from which RouterA originally learned that F0/0 on RouterB was down. If RouterA uses split horizon with poison reverse, it not only refuses to accept RouterC's update regarding F0/0 on RouterB, but it also responds to RouterC's attempted update. RouterA will tell RouterC that the route to F0/0 on RouterB is no longer available by indicating that the hop count has been exceeded. In other words, it poisons the erroneous route advertised by RouterC so that no other router will see this as a viable route.

Another common technique used to stop routing loops is the **hold-down timer**. Hold-down timers allow a router to place a route in a state where it will not accept any changes to that route. If RouterA uses hold-down timers in Figure 7-7, the update from RouterC is ignored because the route would be in “hold-down” for a period of time after it was marked down. During this hold-down period, the router will not accept an update if it has a less favorable metric. It will accept an update and release the timer if the update has a more favorable metric. This prevents improper route information from being propagated throughout the internetwork. Hold-down timers are configurable by the network administrator.

**Link-State Routing Protocols** Link-state routing protocols are the second type of routing protocols you can use to exchange route information between routers in an autonomous system. They behave very differently from distance-vector routing protocols. Routers configured with a link-state routing protocol use **link-state advertisements (LSAs)** to inform neighbor routers on the internetwork. However, instead of sending their entire routing tables, the LSAs contain only the local links for the advertised router. The **Shortest Path First (SPF) algorithm** uses the link information to compute the routes. So, router CPU resources are used instead of bandwidth.

**Link-state packets (LSPs)**, which are the packets used to send out LSAs, allow every router in the internetwork to share a common view of the **topology** of the internetwork. Figure 7-8 shows



**Figure 7-8** Link-state advertisements



how a router configured with a link-state routing protocol **floods**, or multicasts, LSPs to the network so that every other router on the internetwork has a common view of its topology.

In the example in Figure 7-8, the network quickly reaches a state of convergence due to the flooding of link-state packets. This rapid convergence is one significant advantage that link-state routing protocols have over distance-vector routing protocols. Also, later updates by the routers in the internetwork will be **triggered updates**. These updates occur due to network topology changes, not periodic routing table advertisements. In other words, RouterB will flood the internetwork with LSPs if a change occurs to its routing table. This announcement contains only the changes in the routing table, not the entire routing table. This conserves bandwidth on the internetwork links.

Using link-state routing protocols does have some drawbacks. Due to the complexity of the Shortest Path First algorithm and the need to hold a view of the entire internetwork topology, routers using link-state protocols must be configured with more memory and processing power than those using distance-vector routing protocols. In addition, link-state routing protocols such as OSPF are much more complicated to configure on the routers. This is why, for smaller-scale internetworks, distance-vector routing protocols such as RIP and IGRP are typically used instead of OSPF.

Table 7-2 summarizes the key characteristics associated with distance-vector and link-state routing protocols.

Now that you have been introduced to the theory behind routing protocols, you need to learn how to actually configure a specific protocol on Cisco routers. RIP is the most commonly used distance-vector protocol and is tested on the CCNA exam, so you will learn to configure it in the next section.

Distance-Vector	Link-State
Periodically broadcasts entire routing table to neighbor routers	Multicasts links to all routers in the AS on startup; all other routing table updates contain only updated routes; updates occur when a network topology change occurs
Slow to converge	Fast to converge due to link-state advertisements
Prone to routing loops because of routing-by-rumor nature	Less prone to routing loops because all other routers share a common view of the network
Easy to configure and administer	Harder to configure; requires greater memory and processing power on each router
Consumes relatively more bandwidth	Consumes relatively less bandwidth

**Table 7-2** Major characteristics of distance-vector and link-state routing protocols

## Routing Information Protocol

The easiest Interior Gateway Protocol to configure is RIPv1 (RIP version 1).



Another version of RIP, called RIP version 2 (RIPv2), is more sophisticated. RIPv2 and other more advanced routing protocols are covered in Chapter 8. When discussing RIP in the context of the CCNA exam, you should assume RIPv1 unless version 2 is specified.

RIP is a distance-vector routing protocol that broadcasts entire routing tables to neighbors every 30 seconds, out of every interface. RIP uses hop count as its sole metric. This means RIP lacks the capability to factor in link speed or congestion between routers; thus, the shortest path chosen by RIP is not always the fastest. As previously mentioned, RIP has a maximum hop count of 15. As a result, RIP does not work in large internetworks. RIP has the following attributes:

- It is a distance-vector routing protocol.
- It has a maximum hop count of 15.
- 16 hops is considered infinity.
- Hop count is the only metric available for path selection.
- It broadcasts the entire routing table to neighbors every 30 seconds.
- It is capable of load balancing.
- It is easy to configure.

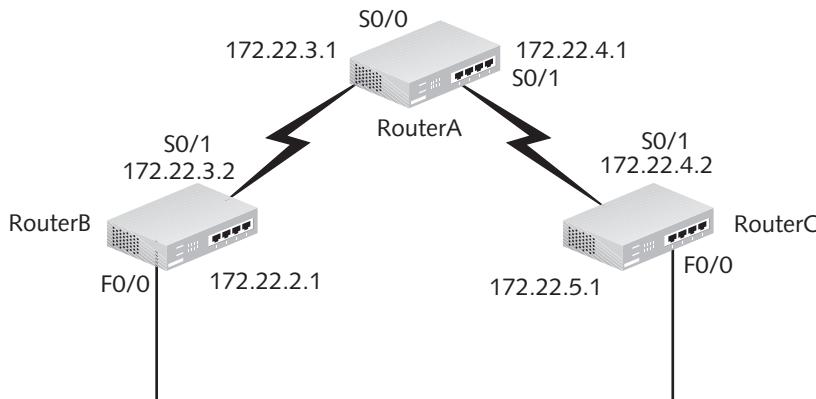
In addition, RIP is susceptible to all the problems normally associated with distance-vector routing protocols. It is slow to converge and forces routers to learn network information only from neighbors. Still, RIP is popular because it is easy to configure.

To install RIP on a Cisco router using TCP/IP, you must perform the following two tasks:

- Enable RIP.
- Configure RIP routing for each major network you want to advertise.

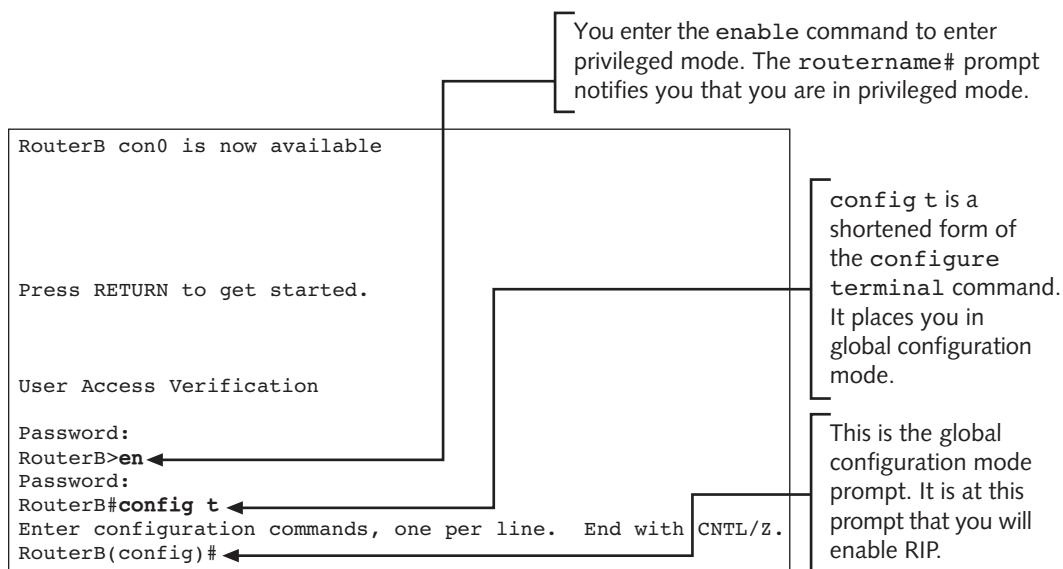
## Enabling RIP Routing

For the following discussion of RIP, we will use the network in Figure 7-9. For brevity, we will only focus on enabling RIP on RouterB. You can assume that RIP has already been configured on RouterA and RouterC.



**Figure 7-9** Sample IP network

To start configuring RIP, you must first enter privileged mode and then global configuration mode on your router. Once you type the `enable` command and `config terminal` command to enter global configuration mode, router output similar to that shown in Figure 7-10 should appear.



**Figure 7-10** Global configuration mode

Once in global configuration mode, you must enable RIP with the `router rip` command. The command to enable RIP is displayed in Figure 7-11.

```

Password:
RouterB>en
Password:
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#router rip ←
RouterB(config-router)#network 172.22.0.0 ←
RouterB(config-router)#^Z
RouterB#
%SYS-5-CONFIG_I: Configured from console by console
RouterB#

```

The `router rip` command enables RIP routing on the router

The `network [network #]` command is used to specify the major networks RIP will advertise

**Figure 7-11** Configuring RIP

## Configuring RIP Routing for Each Major Network

Figure 7-11 also displays the commands necessary to turn on RIP routing for a particular major network. The `network [network #]` command in Figure 7-11 turns on RIP routing for the major class B network 172.22.0.0. If you have multiple major networks configured on a router, an individual `network [network #]` command must be issued for each separate network directly connected to that router.

After you have enabled RIP routing globally and configured each major network that the router will advertise with RIP updates, RIP is fully configured on the router. After the update interval of 30 seconds passes on each router, RouterB will eventually learn of all networks. You use the `show ip route` command to display the routing table. Figure 7-12 shows the output from the `show ip route` command on RouterB.

The `show ip route` command will work in privileged or user mode

This entry shows the administrative distance and hop count of the destination network. Network 172.22.5.0 has an administrative distance of 120 and is 2 hops away. All routes learned via RIP will have administrative distances of 120.

```

RouterB#show ip route ←
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
       area
       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
Gateway of last resort is not set
      172.22.0.0/16 is subnetted, 4 subnets
C        172.22.2.0 is directly connected, FastEthernet0/0
C        172.22.3.0 is directly connected, Serial0/1
R        172.22.4.0 [120/1] via 172.22.3.1, 00:00:15, Serial0/1
R        172.22.5.0 [120/2] via 172.22.3.1, 00:00:15, Serial0/1
RouterB#

```

The R signifies that the route was learned via RIP.

**Figure 7-12** Output from the `show ip route` command

The output in Figure 7-12 illustrates an extremely important concept called administrative distance. **Administrative distance** is a value used to determine the reliability of the information regarding a particular route. Administrative distances range from 0–255. The larger the number, the less reliable the routing protocol is considered to be. The more reliable routing protocol will always be favored over the less reliable and will therefore have its route installed in the IP routing table of the router. Table 7-3 shows common routing protocols and their administrative distances.

The value 120, shown in the routing table in Figure 7-12 after subnet 172.22.4.0 and 172.22.5.0, is the administrative distance for RIP. A metric of 1 (1 hop) is listed after the 120 for the 172.22.4.0 entry, and a metric of 2 (2 hops) is listed after the 120 for the 172.22.5.0 entry. Remember, RIP uses hops as its sole metric.



Route Learned via:	Administrative Distance
Directly connected network	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
Unknown	255

**Table 7-3** Administrative distances

If a route is being discovered using both RIP and a directly connected interface, the route available via the directly connected interface will be the preferred route because it has a lower administrative distance. Likewise, if both IGRP and RIP advertise a route for a particular network, the IGRP route will be used because it is considered more reliable due to its lower administrative distance.

### Show ip protocol and debug ip rip Commands

You can use the `show ip protocol` and `debug ip rip` commands to monitor RIP. You can type the `show ip protocol` command in either user mode or privileged mode. When you type this command, you will receive output similar to that shown in Figure 7-13.

In Figure 7-13, you can see the timers associated with RIP. RIP updates on TCP/IP networks, as stated previously, occur every 30 seconds. A route is considered invalid if six consecutive update intervals pass without an update from that route. The hold-down time of 180 seconds allows the router to stabilize its routing table to help prevent routing loops when a network path does go down. Finally, the `flush interval` is the time at which a route will be totally removed from the routing table if no updates are received.

## 184 Chapter 7 Routing Protocols

```

RouterB>show ip protocol ←
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 6 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 1, receive any version
    Interface      Send      Recv      Key-chain
    FastEthernet0/0   1        1 2
    Serial0/1       1        1 2
  Routing for Networks:
    172.22.0.0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.22.3.1           120          00:00:27
  Distance: (default is 120)

RouterB>

```

The show ip protocol command will work in privileged or user mode.

All RIP timers are displayed via this command.

**Figure 7-13** Output from the show ip protocol command

The debug ip rip command, like all debug commands, should only be used when troubleshooting RIP. This command displays real-time RIP updates being sent and received and places very high processing demands on your router, which could affect network performance. Figure 7-14 shows the output of the debug ip rip command.

```

RouterB>en
Password:
RouterB#debug ip rip ←
RIP protocol debugging is on
RouterB#
RIP: received v1 update from 172.22.3.1 on Serial0/1
  172.22.4.0 in 1 hops
  172.22.5.0 in 2 hops
RouterB#
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0
  subnet 172.22.3.0, metric 1
  subnet 172.22.4.0, metric 2
  subnet 172.22.5.0, metric 3
RIP: sending v1 update to 255.255.255.255 via Serial0/1 (172.22.3.2)
  subnet 172.22.2.0, metric 1
RIP: ignored v1 update from bad source 172.22.5.1 on FastEthernet0/0
RIP: received v1 update from 172.22.3.1 on Serial0/1
  172.22.4.0 in 1 hops
  172.22.5.0 in 2 hops
RouterB#
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0
  subnet 172.22.3.0, metric 1
  subnet 172.22.4.0, metric 2
  subnet 172.22.5.0, metric 3
RIP: sending v1 update to 255.255.255.255 via Serial0/1 (172.22.3.2)
  subnet 172.22.2.0, metric 1
RIP: ignored v1 update from bad source 172.22.5.1 on FastEthernet0/0
RouterB#no debug ip rip ←
RIP protocol debugging is off
RouterB#

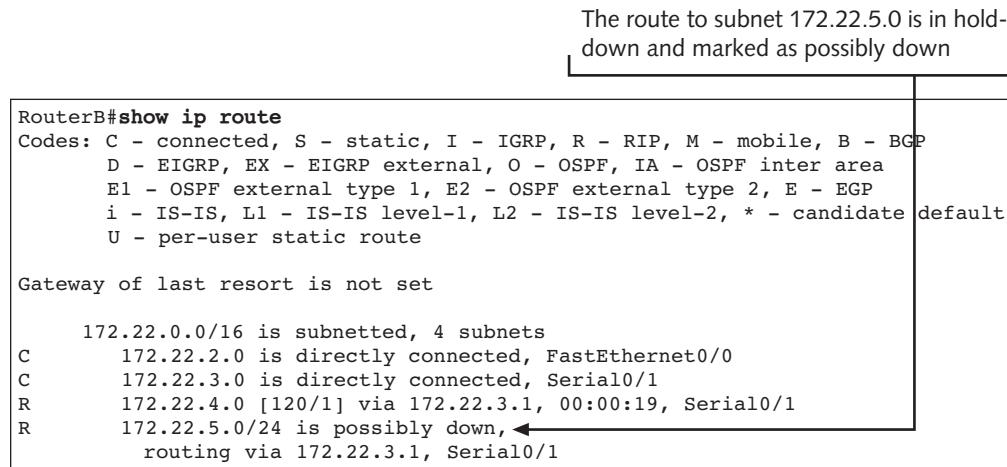
```

The debug ip rip command only works in privileged mode.

The no debug ip rip command turns off RIP debugging.

**Figure 7-14** Output from the debug ip rip command

As previously mentioned, RIP is slow to converge, like most distance-vector routing protocols. If RouterC in Figure 7-9 loses its connection to subnet 172.22.5.0 on Ethernet0, RouterB will learn about the route status changing. However, it could take at least a minute for the changes to propagate throughout the network (30 seconds maximum for the update interval on RouterC and RouterA). Once RouterB learns of the change in status for network 172.22.5.0, it marks the route as possibly down and initiates a hold-down timer. You can type the `show ip route` command on RouterB to display this change in status. Figure 7-15 shows the results of the `show ip route` command after Ethernet0 on RouterC becomes inaccessible.



```

RouterB#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
      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

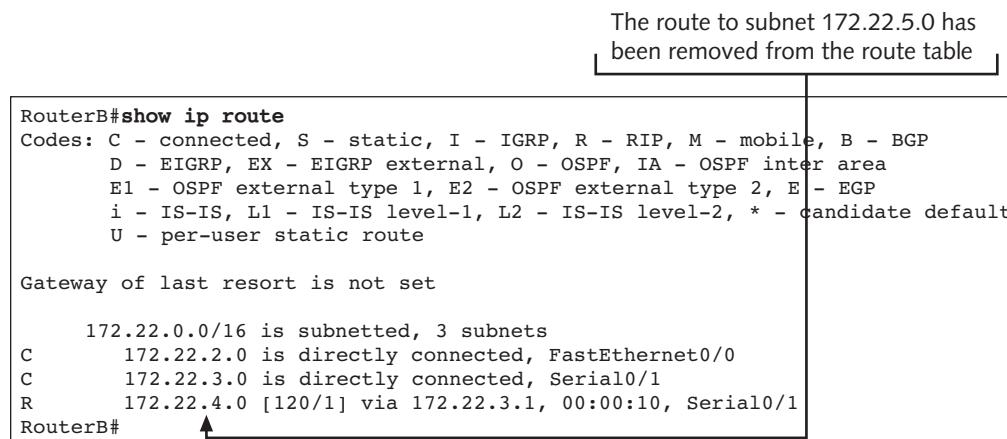
Gateway of last resort is not set

172.22.0.0/16 is subnetted, 4 subnets
C        172.22.2.0 is directly connected, FastEthernet0/0
C        172.22.3.0 is directly connected, Serial0/1
R        172.22.4.0 [120/1] via 172.22.3.1, 00:00:19, Serial0/1
R        172.22.5.0/24 is possibly down, routing via 172.22.3.1, Serial0/1

```

**Figure 7-15** Output from the `show ip route` command

Eventually, the route will be flushed from the routing table. Still, with a hold-down time of 180 seconds and a flush timer of 240 seconds, the time it takes for the internetwork to converge can become excessive. If you issue the `show ip route` command after the route has been flushed from the routing table, you will get the router output displayed in Figure 7-16.



```

RouterB#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
      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

Gateway of last resort is not set

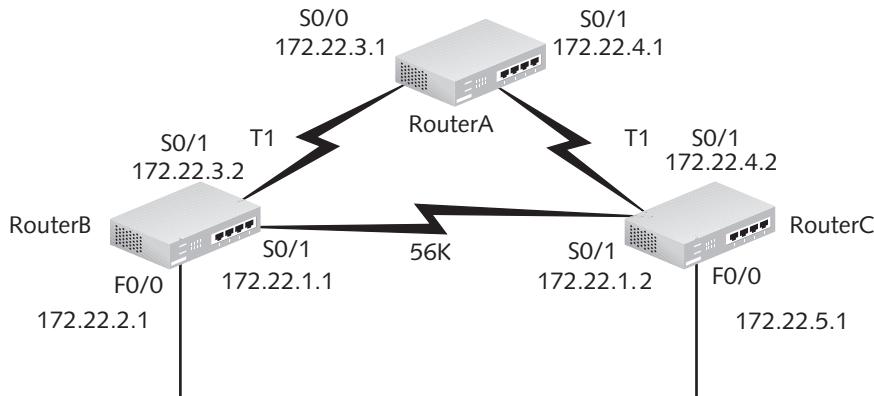
172.22.0.0/16 is subnetted, 3 subnets
C        172.22.2.0 is directly connected, FastEthernet0/0
C        172.22.3.0 is directly connected, Serial0/1
R        172.22.4.0 [120/1] via 172.22.3.1, 00:00:10, Serial0/1
RouterB#

```

**Figure 7-16** New output from the `show ip route` command



Note that RIP relies on hop count as its single metric. In the network in Figure 7-17, a router configured to use RIP would always route packets to the subnet 172.22.5.0 via the 56-Kbps link between RouterB and RouterC because of the hop count of one.



**Figure 7-17** RIP problems caused by hop count reliance

As this network is configured, it may actually be faster to route packets along the T1 lines. This route, with a hop count of two, will not be used by RIP as the best route even though it may be faster. To combat this problem associated with distance-vector protocols such as RIP, Cisco developed its own proprietary distance-vector protocol, called IGRP.

## Interior Gateway Routing Protocol

IGRP is a proprietary distance-vector routing protocol created by Cisco to solve some of the problems associated with RIP. A larger hop-count metric allows IGRP to be used on larger networks. In fact, IGRP supports a hop count of 255, although 100 is the default if hop count is configured to be used as a metric. If, for example, IGRP is configured to use hops as a metric and 255 hops is the value configured, on the 256th hop IGRP will return an ICMP destination network unreachable message. In some situations you may actually want to reduce IGRP's hop count to speed convergence and route processing. The `metric maximum-hops` command allows you to set the maximum hop count for IGRP. You should set the hop count to the maximum number of routers within your network if you are going to use hops with IGRP.

IGRP does not use hops as a metric by default. The default metrics for IGRP are bandwidth and delay only. IGRP can also be configured to use load and reliability metrics. The metrics that can be configured for IGRP are:

- *Hops*—Number of routers between source and destination networks
- *Load*—The load on a link in the path
- *Bandwidth*—The speed of the link (default)
- *Reliability*—Measures reliability with a scale of 0 to 255
- *Delay*—The delay on the medium (default)
- *MTU*—The size of the datagram

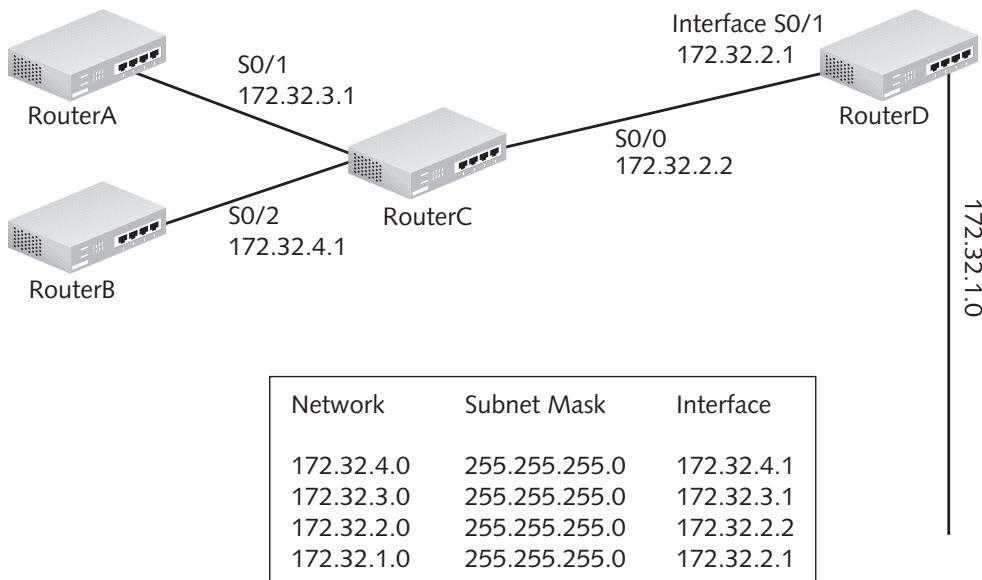
As previously mentioned, IGRP is no longer supported on newer versions of the Cisco IOS. You will learn to configure the enhanced version of IGRP, which is EIGRP, in Chapter 8.

## Static Routing

Although routing protocols are easy to configure and maintain, many times they are unnecessary. Some networks are so small that using a routing protocol creates unnecessary traffic and an inefficient use of router processor resources. In addition, some networks may have only one route out and therefore can be configured with a single static route. Routers with only one route out are also known as **stub routers**. Stub routers are usually the last router in a chain. Networks with one route to the Internet are called **stub networks**. Static routes are configured by a network administrator using the `ip route` command, as described in the next section.

### Adding Static Routes

Figure 7-18 shows the routing table for RouterC. As previously mentioned, this table can be dynamically configured using routing protocols such as RIP, or the table can be built statically using `ip route` commands. Although static routing gives the administrator full control as to how packets will be routed, the disadvantage of using static routing is the initial manual configuration and the possible reconfiguration if routes are changed. Notice that for all interfaces that are physically attached to RouterC, the route to the network is through a local interface on the router. However, for packets destined to network 172.32.1.0, RouterC must forward them to RouterD. As you can see, RouterC is configured to send the packets to the 172.32.2.1 interface on RouterD because that is the next hop for the packet from the perspective of RouterC.



**Figure 7-18** Routing table for RouterC

The commands that would be necessary to statically construct the proper routes for the routing table on RouterD to reach all the shown networks are shown below. To statically configure a route, you must type the destination network identifier, subnet mask, and the IP address of the interface of the next hop in the path. The syntax for the `ip route` command is:

```
ip route [destination network address] [destination network mask]
[ip address next hop interface] [administrative distance]
```

The administrative distance is optional; you only have to add an administrative distance if you want to change the default administrative distance of 1 (see Table 7-3). The following entries for RouterD would allow it to route to all the networks in Figure 7-18:

- RouterD# config t
- RouterD(config)# ip route 172.32.3.0 255.255.255.0 172.32.2.2
- RouterD(config)# ip route 172.32.4.0 255.255.255.0 172.32.2.2



You can substitute the outgoing physical port for the next hop IP address in the `ip route` command.

**NOTE**

The two entries for networks attached to RouterC are headed for the same interface. RouterD must move those packets destined for networks on the remote side of RouterC to the interface on RouterC that is connected to RouterD. Static routes to 172.32.2.0 and 172.32.1.0 are unnecessary because RouterD has directly connected interfaces to those two networks.

Static routes are very powerful, as they allow administrators complete control over path selection. In addition, they use less bandwidth, less memory, and fewer CPU resources than routing protocols.

**Changing Administrative Distance** The `ip route` command also allows you to configure an administrative distance, which, as discussed previously, is a value used by the router to select the best route to a destination when there are two or more different routes to the same destination being reported from more than one source—for example, from RIP, IGRP, and from a static entry. The default administrative distances were listed previously in Table 7-3.

Static routes have a much lower default metric than routes learned by **dynamic routing protocols**, because a static route is considered to be a preferred route since someone took the trouble to enter it. Of course, if you want the static route to be used as a backup route to one learned via a dynamic routing protocol, be sure to set the administrative distance of the static route higher than that of the default dynamic routing protocol. Remember, unless you add an administrative distance value to the end of your `ip route` command, the administrative distance will be 1. For example, to set an administrative distance of 150 for the static entry to network 192.168.5.0, type:

```
router(config)#ip route 192.168.5.0 255.255.255.0 192.168.4.2 150
```

An interface such as f0/0 can be shut down by typing the shutdown command. The following commands could be used to shut down this interface:

- router#configure t
- router(config)#int f0/0
- router(config-if)#shutdown

If you want your static route mappings to remain, even if an interface is shut down, you must add permanent to the end of the ip route command—otherwise the route will be deleted from the routing table when the interface is shut down.

**Configuring a Default Route** When you connect a router to the Internet, as a practical matter, you cannot and would not want to enter all of the possible networks that are beyond your network. The table would be massive and difficult to maintain. Once you have the routing table set up to handle all of the networks that you care to configure, and you want all other packets to go to a specific location (usually a router that connects to the Internet), you can enter a **default route** for your router. When you do, all packets that are not defined specifically in your routing table will go to the specified interface for the default route. A default route is a type of static route that the administrator configures. Without a default route, all packets addressed to destinations on networks not specifically listed in the routing table will not reach their destinations. This is why most network administrators use a combination of dynamic routing protocols and static routes to maintain the routing tables on their routers. In the case of stub networks, very often only static routing is used. When IP routing is enabled, you can use the ip default-network command or the ip route 0.0.0.0 0.0.0.0 command to configure a default route. The way in which routing protocols propagate the default route information varies for each protocol and is beyond the scope of this text and the CCNA exam.

The ip default-network command is typically configured on the routers that connect to a single router with a static default route. Look at Figure 7-18 again. This time, assume that RouterD connects to the Internet and that Routers A, B, and C are part of the internal network. If you are in charge of configuring Routers A, B, and C and you want to ensure that all packets destined for any external network are routed properly, enter the following command on Routers A, B, and C:

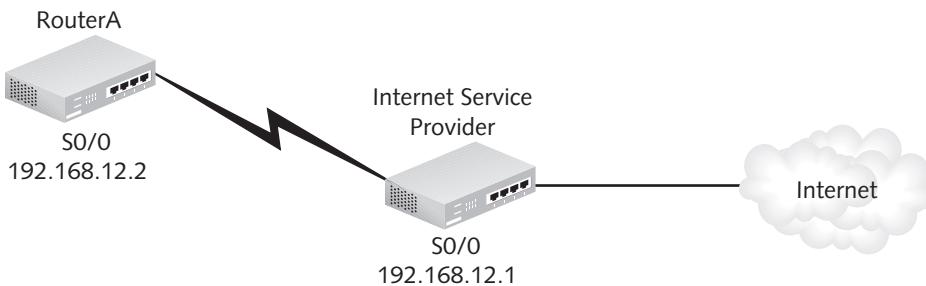
```
RouterA(config)# ip default-network 172.32.1.0
```

RouterA and RouterB would use RouterC interfaces as their default gateways. RouterC could use interface 172.32.2.1 as its default gateway. This means that it would be up to RouterD to route packets to the Internet for all internal hosts. To allow RouterD to route these packets, you would need to configure a default route as described below.

A default route uses the following format:

```
RouterD(config)# ip route 0.0.0.0 0.0.0.0 [next hop  
router ip address] [administrative distance]
```

The zeroes in the command represent any destination network with any mask. Default routes are sometimes called **quad zero routes**. A default route is used only if no other route to a network exists in the routing table. In short, a router configured with a default route sends packets destined to a network for which it does not have a route to the next specified hop router. Figure 7-19 shows a network where a default route would be ideal.



**Figure 7-19** Default route example

As the figure shows, RouterA only has one way out to the Internet. The router of the Internet service provider (ISP) could therefore be set as the next hop router for all routes for which RouterA did not have a route. To accomplish this, the following command would be added to RouterA:

```
RouterA(config)# ip route 0.0.0.0 0.0.0.0 192.168.12.1
```

With the addition of this static default route, any packet destined for a network for which RouterA does not have an explicit route in its routing table will be forwarded to the ISP router.

## Chapter Summary

- Protocols vary in their functions. Some protocols are designed to be used in small networks without the need for Network layer addressing. These protocols are described as nonroutable protocols.
- The most common nonroutable protocol is NetBEUI.
- Other protocols were designed with the ability to move between multiple networks via Network layer addressing. These protocols are routed protocols.
- The most common routed protocol suite is TCP/IP.
- Protocols must be available that can find the best path throughout an internetwork and relay that information to routers. Routing protocols serve this function on modern networks.
- Routing protocols are classed in two major groups: Interior Gateway Protocols and Exterior Gateway Protocols.
- Interior Gateway Protocols are routing protocols that function within a single autonomous system. Exterior Gateway Protocols function as routing protocols between autonomous systems.
- Interior routing protocols are further divided into distance-vector and link-state routing protocols.
- These two types of Interior Gateway Protocols use very different methods to determine the best path in an internetwork.
- Distance-vector protocols periodically broadcast entire routing tables to neighbor routers.

- Link-state protocols multicast link updates to routers in their area upon startup and when network topology changes.
- Two common distance-vector IGPs discussed in this chapter are the Routing Information Protocol and the Interior Gateway Routing Protocol.
- RIP is an easy-to-configure routing protocol that uses hop count as its sole metric. RIP has a hop count limit of 15. RIP uses split horizon, split horizon with poison reverse, and hold-down timers to help limit routing loops. RIP can be used on Cisco and non-Cisco routers.
- IGRP is also a distance-vector routing protocol. IGRP has a maximum hop count of 255. IGRP is not limited to using hop count as its sole metric. IGRP can also use load, bandwidth, reliability, and delay when determining best path. IGRP uses only bandwidth and delay by default. IGRP is a Cisco-proprietary protocol and can only be used on Cisco routers. IGRP is no longer supported.
- Static routes are used to conserve bandwidth and lower memory and CPU load on a router while still allowing for correct routing table creation.
- Static routes give administrators control and flexibility in path selection in a network.

7

---

## Key Terms

**administrative distance** A value used to determine the reliability and desirability of a particular routing table update.

**autonomous system (AS)** A group of routers under the control of a single administration.

**Border Gateway Protocol (BGP)** An Exterior Gateway Protocol used to route between multiple autonomous systems.

**convergence** The point at which all routers on a network share a similar view of the network.

**count-to-infinity** A routing loop whereby packets bounce infinitely around an internetwork.

**default route** A static route that directs all traffic not specified anywhere else in the routing table to a particular route. Same as quad zero route.

**defining a maximum** A technique used with distance-vector routing protocols to prevent packets from bouncing infinitely throughout an internetwork by setting a maximum hop count.

**distance-vector** A routing protocol that functions by broadcasting the entire routing table periodically to all connected neighbors; examples include RIP and IGRP.

**dynamic routing protocol** A protocol that builds the routing table automatically. Examples include RIP, IGRP, EIGRP, and OSPF.

**Enhanced Interior Gateway Routing Protocol (EIGRP)** A proprietary Cisco routing protocol developed to overcome some of the limitations associated with distance-vector protocols. EIGRP is considered a hybrid routing protocol.

**Exterior Gateway Protocol (EGP)** A gateway protocol used to route between multiple autonomous systems.

**flood** The process of multicasting packets onto a network.

**192 Chapter 7 Routing Protocols**

**flush interval** The time at which a route is totally removed from the routing table.

**hold-down timer** A technique used to stop routing loops in which updates from an inferior source are not allowed for a certain interval. Used by routers to stabilize routing tables and to prevent erroneous routing table updates.

**hop count** A count of the number of routers a packet must pass through to reach a destination network.

**Interior Gateway Protocol (IGP)** A gateway protocol used to route within one autonomous system.

**Interior Gateway Routing Protocol (IGRP)** A proprietary Cisco distance-vector routing protocol that uses delay and bandwidth as its default metrics.

**internetwork** Multiple networks connected by routers.

**Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)** A routed-protocol stack developed by Novell for use with the Netware network operating system.

**link-state** Routing protocols that function via link-state advertisements using link-state packets to inform all routers on the internetwork of routing information. OSPF is the most common link-state routing protocol.

**link-state advertisements (LSAs)** Routing information packets used by link-state routing protocols to advertise their local network link information to neighbor routers in an internetwork.

**link-state packets (LSPs)** Packets used to send out link-state advertisements.

**logical addresses** Layer 3 addresses (also referred to as Network layer addresses) that allow routing protocols to determine the best path to a particular host.

**metric** A value used to define the suitability or desirability of a particular route.

**nonroutable protocols** Protocols that do not contain Network layer addressing and therefore cannot pass between multiple networks.

**Open Shortest Path First (OSPF)** A link-state routing protocol based upon open (nonproprietary) standards.

**peer-to-peer networks** Small networks, normally consisting of fewer than 10 computers, in which each computer can give and receive network services.

**quad zero route** *See default route.*

**routed protocols** Protocols that contain Network layer addressing and therefore can pass between multiple networks.

**routing by rumor** The learning of routes through secondhand information, and not directly from the router experiencing the change. Routing by rumor is characteristic of distance-vector routing protocols.

**Routing Information Protocol (RIP)** A distance-vector routing protocol that uses hop count as its only metric.

**routing loops** A network state in which packets are continually forwarded from one router to another in an attempt to find the destination network.

**routing protocols** Protocols used by routers to define and exchange routing table information in an internetwork.

**Shortest Path First (SPF) algorithm** A complex algorithm used by link-state routing protocols to determine the best path in an internetwork.

**split horizon** A technique used by routers to prevent routing loops. In short, a router will not send an update for a route via an interface from which it originally received knowledge of that route.

**split horizon with poison reverse** A split horizon in which the router responds to attempts to update a route with an update that marks the route in contention as unreachable.

**static route** A route manually added by a network administrator to the routing table of a router.

**stub network** A network with only one route to the Internet.

**stub router** A router that is last in a chain of routers. There is only one path for all hosts connected to this router to get to the outside world.

**topology** The physical or logical structure of a network.

**Transmission Control Protocol/Internet Protocol (TCP/IP)** Routed protocol stack developed in the late 1960s for use on the network that preceded the Internet; protocol stack of the modern-day Internet.

**triggered updates** Updates that occur due to network topology changes, not periodic routing table advertisements.

7

---

## Review Questions

1. What is the administrative distance of RIP?
  - a. 100
  - b. 110
  - c. 120
  - d. 90
2. Link-state routing protocols. (Choose all that apply.)
  - a. use link-state advertisements to notify routers of route changes
  - b. send routing tables to neighbors
  - c. reach convergence faster than distance-vector routing protocols
  - d. determine the best path via the hop count algorithm
3. RIP has a maximum hop count of.
  - a. 255
  - b. 16
  - c. 15
  - d. 254
4. Which command enables RIP on a router?
  - a. router network RIP
  - b. router rip
  - c. router igrp
  - d. router ospf

**194** Chapter 7 Routing Protocols

5. Which command will show the IP routing table of a router?
  - a. show ip route
  - b. show ip protocol
  - c. debug ip igrp events
  - d. show run
6. Nonroutable protocols are able to pass packets among multiple networks. True or False?
7. IGRP can use which of the following as metrics? (Choose all that apply.)
  - a. hop count
  - b. bandwidth
  - c. delay
  - d. split horizon
8. Which of the following is a routed protocol? (Choose all that apply.)
  - a. NetBEUI
  - b. TCP/IP
  - c. IPX/SPX
  - d. RIP
9. Which of the following helps to prevent routing loops? (Choose all that apply.)
  - a. split horizon
  - b. count-to-infinity
  - c. hold-down timers
  - d. split horizon with poison reverse
10. At which router prompt can you use the `router rip` command?
  - a. routerB#
  - b. routerB>
  - c. routerB(config)#
  - d. routerB(config-router)#
11. At which router prompt can you issue the `network [network #]` command?
  - a. routerB#
  - b. routerB>
  - c. routerB(config)#
  - d. routerB(config-router)#
12. The `debug ip rip` command can be used in user mode and privileged mode. True or False?

13. Which of the following routing protocols can route between autonomous systems? (Choose all that apply.)
- a. IGRP
  - b. RIP
  - c. BGP
  - d. EGP
14. What type of routing protocol is used within autonomous systems?
- a. Exterior Gateway Protocols
  - b. TCP/IP
  - c. NetBEUI
  - d. Interior Gateway Protocols
15. RIP and IGRP both advertise a route to a particular network. Which route will be added to the routing table?
- a. the RIP route
  - b. the IGRP route
  - c. both RIP and IGRP routes
  - d. BGP-enhanced IGRP
16. What command is used to display RIP timers?
- a. show ip route
  - b. show run
  - c. debug ip rip
  - d. show ip protocol
17. What two commands are needed to configure RIP on a router? (Choose all that apply.)
- a. network rip
  - b. router rip
  - c. router network rip
  - d. network [network #]
18. A metric is a variable used to determine the suitability of a route. True or False?
19. A major drawback of link-state routing protocols is:
- a. routing by rumor
  - b. increased memory and processing required on routers
  - c. slow time to convergence
  - d. inability to adapt to network topology changes

**196** Chapter 7 Routing Protocols

20. Which of the following commands would enable a routing protocol that is only concerned with hop count?
- router# router igrp
  - router(config)# router igrp
  - router# router rip
  - router(config)# router rip
  - router# router ospf
21. Which of the following are true about administrative distance? (Choose all that apply.)
- The higher the administrative distance, the more desirable the route.
  - Administrative distances are used with static routes.
  - The default administrative distance for RIP is 120.
  - The default administrative distance for static routes is higher than those for dynamic routes.
  - The default administrative distance for a connected network is lower than that for the default route of IGRP.
22. What does the number 240 stand for in the following command?
- ```
Router(config)# ip route 192.168.1.0 255.255.255.0 240
```
- number of masked bits
  - decimal subnet mask
  - number of hops
  - administrative distance
  - autonomous network number
23. If you want to monitor real-time RIP traffic, which command would you type?
- router> router rip
  - router# router rip
  - router# show rip
  - router(config)# show rip
  - router# debug ip rip
24. Which of the following does RIP support? (Choose all that apply.)
- load balancing
  - link reliability metric
  - bandwidth metric
  - delay metric

## Case Projects



1. Winslow Networks has been hired by Big Tin Inc. to redesign Big Tin's network. Currently, the network consists of 14 routers with a potential growth of three routers in the next four months. Moe suggests that the company implement RIP for internetwork routing because it is so popular and easy to configure. Is this the best possible solution for Big Tin Inc.? Justify your answers.
2. Hogan's, an international food services conglomerate, wants to implement wide area network links between its 25 plants spread across 13 countries. You have been brought in as a consultant on the project. Hogan's wants convergence to be as quick as possible, and, due to slow WAN links in some undeveloped countries, it must reduce routing table updates to the absolute minimum to conserve bandwidth. Hogan's suggests using a distance-vector routing protocol because of its relative simplicity. Create a network design using the distance-vector protocol you feel will meet Hogan's needs. What metrics are used by default? Which metrics can and should be configured? Justify your answer.
3. Moe and Jennifer are configuring RIP on a client's router, and they want your help. The network number is 204.207.5.0. The router has three interfaces. The IP addresses for the interfaces are 204.207.5.97, 204.207.5.113, and 204.207.5.82. The subnet mask is 255.255.255.240. The host name for the router is "newyork". What mode should Moe and Jennifer be in to use the `router rip` command? What will the prompt look like? How will the prompt change after the `router rip` command is issued? Jennifer has written the following commands for entry next:

```
network 204.207.5.96  
network 204.207.5.112  
network 204.207.5.80
```

What do you tell her?





# 8

chapter

## Advanced Routing Protocols

**After reading this chapter and completing the exercises, you will be able to:**

- Describe classful and classless routing protocols
- Describe and configure RIPv2
- Describe and configure EIGRP
- Describe and configure OSPF
- Control routing traffic

**Routing protocols are an integral part of a functioning network. Distance-**

vector routing protocols such as RIP version 1 or Interior Gateway Routing Protocol (IGRP) are sufficient in simple networks, however today's complex networks demand more advanced protocols. This chapter begins with a discussion of classful and classless routing protocols. It continues with an examination of the classless routing protocols RIP version 2, EIGRP, and OSPF. By the end of the chapter, you should be able to describe and configure each of these protocols. The chapter concludes with a discussion of controlling routing traffic and basic Border Gateway Protocol configuration.

## Classful and Classless Routing Protocols

Routing protocols divide into the broad categories of interior or exterior gateway protocols and distance-vector protocols or link-state protocols. These broad definitions describe where each routing protocol is best used, either within the autonomous system or between autonomous systems. These definitions also describe how the routing protocols handle routing table updates and routing table creation. In general, distance-vector routing protocols send periodic updates of the entire routing table to their directly connected neighbors, while link-state protocols flood nonperiodic link-state advertisements of only changed routes throughout the entire internetwork.

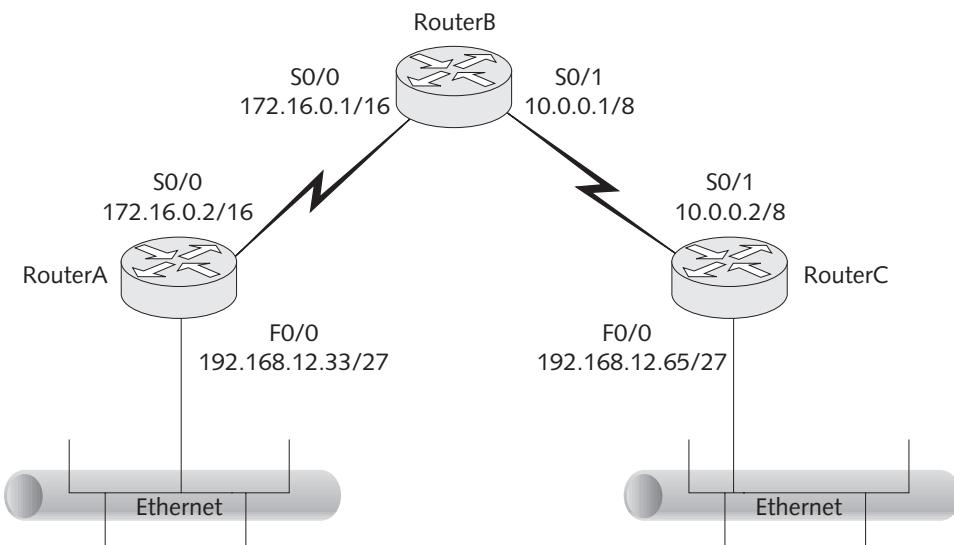
While these characteristics generally define how routing protocols operate, another factor also helps to delineate them. Each routing protocol is defined as either classful or classless, terms that describe how the routing protocol handles subnet mask information in its routing table updates. **Classful routing protocols** summarize networks to their major network boundaries (Class A, B, or C) and do not carry subnet mask information in their routing table updates. These protocols cannot be used in networks with either discontiguous subnets or networks using variable length subnet masks (VLSM), because they summarize to the major network boundaries. RIPv1 and IGRP are classful routing protocols; they do not carry any subnet mask information in their routing table updates. Figure 8-1 shows the update message format for RIPv1.

|                               |             |                  |
|-------------------------------|-------------|------------------|
| Command (1)                   | Version (1) | must be zero (2) |
| Address Family Identifier (2) |             | must be zero (2) |
| IP Address (4)                |             |                  |
| must be zero (4)              |             |                  |
| must be zero (4)              |             |                  |
| Metric (4)                    |             |                  |

**Figure 8-1** RIPv1 message format

The IP address field is particularly important when discussing classful protocols. It is four bytes in size, just large enough for a 32-bit IP address. The message update format in RIPv1 does not have room for subnet mask information in the IP address field, and it does not contain a field dedicated to carrying subnet mask information—which is why RIPv1 uses major network numbers rather than subnet numbers.

Figure 8-2 shows an example of how different major networks separate two subnets from the same major network, 192.168.12.0/24. This is called discontiguous subnets.



**Figure 8-2** Network with discontiguous subnets



The command outputs in this chapter are taken from Cisco 1721 routers with a single WAN Interface Card (WIC) installed.

NOTE

Figure 8-3 shows the configuration of RIPv1 on RouterA from the preceding illustration. As shown in the output of the `show run` command in the figure, RIPv1 summarizes the network entries to the major network. This will cause problems in the network in our example. Figure 8-4 shows the routing table of RouterB after RIPv1 has been configured on just RouterA and RouterB. RouterB believes the major network 192.168.12.0 is available via RouterA's S0/1 interface.

## 202 Chapter 8 Advanced Routing Protocols

```

RouterA(config)#router rip
RouterA(config-router)#network 172.16.0.0
RouterA(config-router)#network 192.168.12.32←

RouterA(config-router)# ^z
RouterA#sh run
01:07:51: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...

Current configuration : 519 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
!
ip subnet-zero
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.12.33 255.255.255.224
 no keepalive
 speed auto
!
interface Serial0/0
 ip address 172.16.0.2 255.255.0.0
 no fair-queue
!
interface Serial0/1
 no ip address
 shutdown
!
router rip
 network 172.16.0.0
 network 192.168.12.0←
!
ip classless
no ip http server
!
!
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

RouterA#

```

Normally, you configure RIPv1 by including in the command major networks on each interface. This example intentionally includes the subnetwork address instead to show that RIPv1 automatically summarizes to the major network number, even though the subnetwork address was entered in the command.

Figure 8-3 Configuring RIPv1 on RouterA

RouterB receives updates from RouterA stating that the 192.168.12.0 network is available through it.

```

RouterB#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, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

R 192.168.12.0/24 [120/1] via 172.16.0.2, 00:00:11, Serial0/0
C 172.16.0.0/16 is directly connected, Serial0/0
C 10.0.0.0/8 is directly connected, Serial0/1
RouterB#

```

**Figure 8-4** Router B's routing table—partial network configuration



After configuration of RouterC with RIPv1, however, RouterB's routing table changes quickly to include not one, but two equal cost routes to the 192.168.12.0 network. In this case, RouterB thinks it can load-balance over the two routes. Figure 8-5 shows the two equal cost routes in RouterB's routing table. Figure 8-6 shows a ping attempt by RouterB to the IP address 192.168.12.33 using the extended ping commands. As you can see, the ping works, but only intermittently—a result of the dual equal cost routes in RouterB's routing table.

After configuration of RouterC with RIPv1, RouterB erroneously believes it has two equal cost routes to the 192.168.12.0 network.

```

RouterB#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, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

R 192.168.12.0/24 [120/1] via 172.16.0.2, 00:00:01, Serial0/0
               [120/1] via 10.0.0.2, 00:00:09, Serial0/1
C 172.16.0.0/16 is directly connected, Serial0/0
C 10.0.0.0/8 is directly connected, Serial0/1
RouterB#

```

**Figure 8-5** Router B's routing table—full network configuration

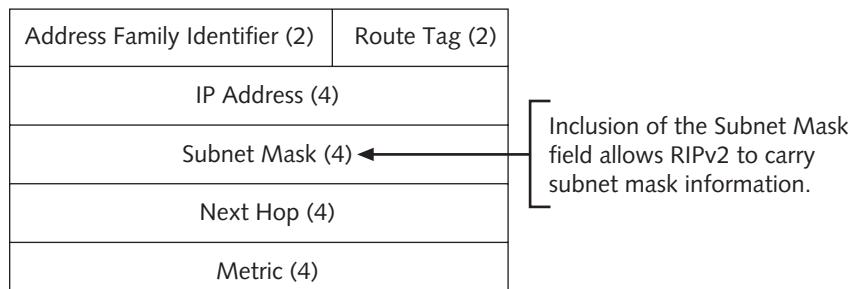
A long repeat count was used to show the effects of the dual routes.

Only 50% of the pings reach RouterA's F0/0 interface.  
The other half are incorrectly routed to RouterC.

```
RouterB#ping
Protocol [ip]:
Target IP address: 192.168.12.33
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.12.33, timeout is 2 seconds:
!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U!.!U
Success rate is 50 percent (50/100), round-trip min/avg/max = 28/28/28 ms
RouterB#
```

**Figure 8-6** Ping example

Classful routing protocols cannot adapt to work in an environment where discontiguous networks or VLSM exist. Instead, to allow dynamic routing in these networks, a classless routing protocol must be used. In essence, the major improvement offered by a **classless routing protocol** is the ability to carry subnet mask information in the routing table updates. RIPv2, EIGRP, OSPF, and BGP are classless routing protocols. Figure 8-7 shows RIPv2's route update message format.



**Figure 8-7** RIPv2 update message format

The four bytes set aside for the Subnet Mask field allow RIPv2 to send the full 32-bit subnet mask for each network configured on the router's interfaces. Figure 8-8 shows the commands to convert RouterB to RIPv2.

```
RouterB(config)#router rip
RouterB(config-router)#version 2 ←
RouterB(config-router)#no auto-summary ←
```

This command converts RIP to version 2.

Although RIPv2 can carry subnet mask information, by default it summarizes along major network boundaries. The no auto-summary command configures the router to use the subnet mask information in the update messages to configure its routing table.

**Figure 8-8** Configuring RIPv2

Converting from RIPv1 to RIPv2 is very simple. The version 2 command switches RIP to version 2 while the no auto-summary command overrides RIPv2's default behavior of summarizing to major network boundaries. Once all the routers in the example are converted to RIPv2, RouterB's routing table looks substantially different than before.

Figure 8-9 shows RouterB's routing table after the conversion. Instead of two equal cost routes to the major network 192.168.12.0, a route for each subnet exists. As a result, the extended ping command in Figure 8-10 works correctly every time.

A separate route entry per subnet now exists.

```

RouterB#sh 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, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      192.168.12.0/27 is subnetted, 2 subnets
R        192.168.12.64 [120/1] via 10.0.0.2, 00:00:09, Serial0/1
R        192.168.12.32 [120/1] via 172.16.0.2, 00:00:07, Serial0/0
C        172.16.0.0/16 is directly connected, Serial0/0
C        10.0.0.0/8 is directly connected, Serial0/1
RouterB#

```

**Figure 8-9** RouterB's routing table with RIPv2

Once the routing table has the correct entries, all pings are successfully sent.

```

RouterB#ping
Protocol [ip]:
Target IP address: 192.168.12.33
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.12.33, timeout is 2 seconds:
!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 28/28/40 ms
RouterB#

```

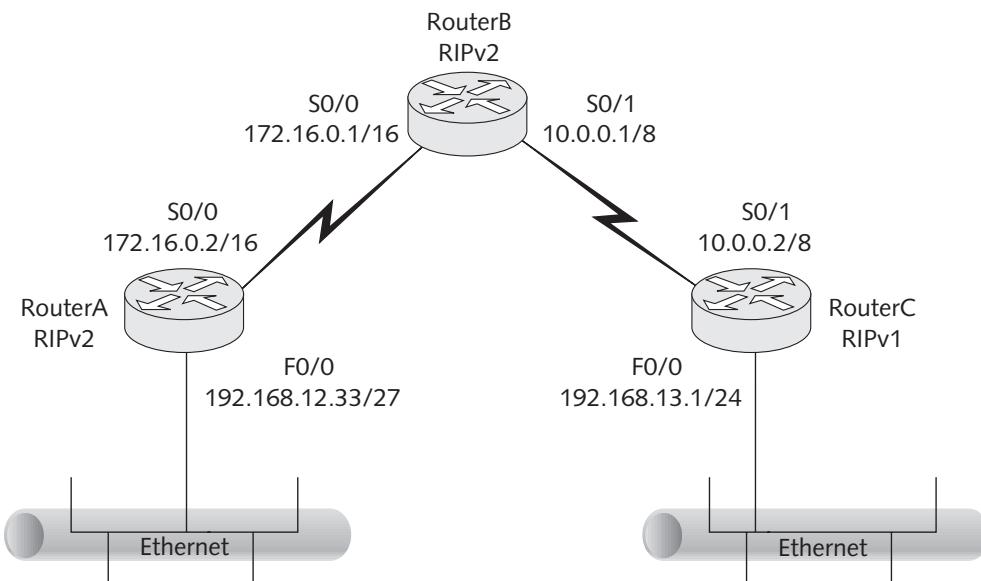
**Figure 8-10** Extended Ping attempt with RIPv2

In general, due to the complexity of modern networks and the use of VLSMs, which require subnet mask information to be sent with update messages, most networks use classless routing protocols.

## Routing Information Protocol version 2

RIPv2 is not a totally new protocol. In reality, it is a set of extensions to RIPv1. As such, it is still a distance-vector routing protocol that uses the normal measures of hold-down timers and split horizon to prevent routing loops. It also suffers from RIPv1's major drawback, in that it only supports a maximum of 15 hops. The major change is RIPv2's ability to carry subnet mask information and a difference in the way it sends out routing table updates. Unlike RIPv1, which broadcasts routing table updates every 30 seconds, RIPv2 multicasts its updates using the multicast address of 224.0.0.9. This feature saves bandwidth on the network, as devices not running RIPv2 do not have to process unnecessary broadcast traffic. Additionally, RIPv2 provides a way to authenticate routing peers to provide enhanced security to a network.

Configuring RIPv2 is a simple process. Figure 8-11 shows a sample network in which two of the three routers are running RIPv2 while a third router is running RIPv1. Figure 8-12 shows the commands necessary to configure RIPv2 on RouterA. The commands are basically the same as those for RIPv1, except for the inclusion of the `version 2` command and the `no auto-summary` command.



**Figure 8-11** RIPv2 example network

```

RouterA(config)#router rip
RouterA(config-router)#version 2
RouterA(config-router)#no auto-summary
RouterA(config-router)#network 172.16.0.0
RouterA(config-router)#network 192.168.12.0

```

Specifies RIPv2 as the routing process.

**Figure 8-12** RIPv2 configuration commands

Issuing the `show ip protocols` command displayed in Figure 8-13 shows that the current routing protocol is RIP and that routing updates for version 2 are being sent and received.

```
RouterA#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 4 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   Triggered RIP  Key-chain
    FastEthernet0/0    2      2
    Serial0/0        2      2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.12.0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.16.0.1        120          00:00:06
  Distance: (default is 120)

RouterA#
```

**Figure 8-13** Show IP protocols output with RIPv2

Additionally, RIPv2 maintains backward compatibility with RIPv1. Cisco routers running RIPv2 can be configured on a per-interface basis to either send or receive version 1 or 2 updates. Because of this per-interface basis, backward compatibility can be easily maintained as a network is migrated from RIPv1 to RIPv2. In our example network in Figure 8-11, RouterB must be configured to send and receive RIPv1 updates to RouterC. Figure 8-14 shows the commands necessary to correctly configure RouterB to share version 1 updates with RouterC. Once this configuration is complete, RouterA will learn via RIPv2 of the routes RouterC has advertised to RouterB. The result will be a network with proper routing throughout, even though all three routers are not running the same version of RIP.

```
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#router rip
RouterB(config-router)#version 2
RouterB(config-router)#no auto-summary
RouterB(config-router)#network 10.0.0.0
RouterB(config-router)#network 172.16.0.0
RouterB(config-router)#int s0/1
RouterB(config-if)#ip rip send version 1
RouterB(config-if)#ip rip receive version 1
RouterB(config-if)#^Z
RouterB#
```

**Figure 8-14** RouterB configuration for RIPv1 and RIPv2 support

## 208 Chapter 8 Advanced Routing Protocols

If RouterB had not been configured to send and receive version 1 updates, the `debug ip rip` command would have displayed errors such as the one shown in Figure 8-15. In this example, RouterB, which has not yet been configured to receive version 1 updates, receives an illegal update from RouterC. Once RouterB has been correctly configured, it will accept the version 1 update from RouterC and pass it on to RouterA as a version 2 update.

If RouterB had not been configured to receive version 1 updates, this output would appear in the `debug ip rip` output. In this example, RouterB ignored a v1 update from Router C.

```
RouterB#debug ip rip
RIP protocol debugging is on
RouterB#
3d00h: RIP: received v2 update from 172.16.0.2 on Serial0/0
3d00h:    192.168.12.32/27 via 0.0.0.0 in 1 hop
3d00h: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (172.16.0.1)
3d00h: RIP: build update entries
3d00h: 10.0.0.0/8 via 0.0.0.0, metric 1, tag 0
3d00h: RIP: sending v2 update to 224.0.0.9 via Serial0/1 (10.0.0.1)
3d00h: RIP: build update entries
3d00h: 172.16.0.0/16 via 0.0.0.0, metric 1, tag 0
3d00h: 192.168.12.32/27 via 0.0.0.0, metric 2, tag 0
% Type "show ?" for a list of subcommands
RouterB#
3d00h: RIP: ignored v1 packet from 10.0.0.2 (illegal version)
RouterB#
RouterB#
RouterB#
```

**Figure 8-15** `debug ip rip` output

Another enhancement of RIPv2 is its ability to authenticate routing peers. In the example network, authentication can be implemented between RouterA and RouterB because they are both running RIPv2. RIP authentication can occur either by passing the authentication keys in clear text or via MD5 authentication. RFC 1321 defines MD5 as an “algorithm [that] takes as input a message of arbitrary length and produces as output a 128-bit ‘fingerprint’ or ‘message digest’ of the input.” In short, using MD5 allows RIPv2 to authenticate a routing peer without sending the secret key (a text string) across the link between the two peers. Instead, it runs the MD5 algorithm against the secret key and sends the hash to the peer. A hash is a number generated by MD5 from the secret key. This number cannot be reverse-engineered easily enough for someone to guess the secret key. The hash is sent to the opposite peer, which runs MD5 against its configured secret key; if the two hashes match, then the two peers are considered authenticated.

Configuring RIPv2 authentication requires the following steps:

- Define a key chain.
- Define keys in the key chain.
- Enable authentication on the interface by specifying the key chain to be used.
- Enable either clear text or MD5 authentication.
- Manage the keys (optional key lifetimes).

Figure 8-16 shows authentication being configured on both RouterA and RouterB. If, by mistake, authentication was only configured on one of the two peers, the RIPv2 process would stop sharing routing updates between the peers, and the error shown in Figure 8-17 would be displayed.

```

RouterB(config)#
RouterB(config)#key chain caudle
RouterB(config-keychain)#key 1
RouterB(config-keychain-key)#key-string ducks←
RouterB(config-keychain-key)#interface s0/0
RouterB(config-if)#ip rip authentication key-chain caudle
RouterB(config-if)#ip rip authentication mode md5
RouterB(config-if)#

RouterA(config)#
RouterA(config)#key chain cannon
RouterA(config-keychain)#key 1
RouterA(config-keychain-key)#key-string ducks←
RouterA(config-keychain-key)#interface s0/0
RouterA(config-if)#ip rip authentication key-chain cannon
RouterA(config-if)#ip rip authentication mode md5
RouterA(config-if)#

```

The two key-strings must match. In essence, this is the shared secret password between the two routers. Of course, because MD5 authentication has been specified, this key will not be sent between the two peers. Only a message digest of the two will be sent.

8

**Figure 8-16** RIPv2 authentication commands

Because RouterB has been configured with MD5 authentication and RouterA has not, RouterB will not accept routing updates from RouterA.

```

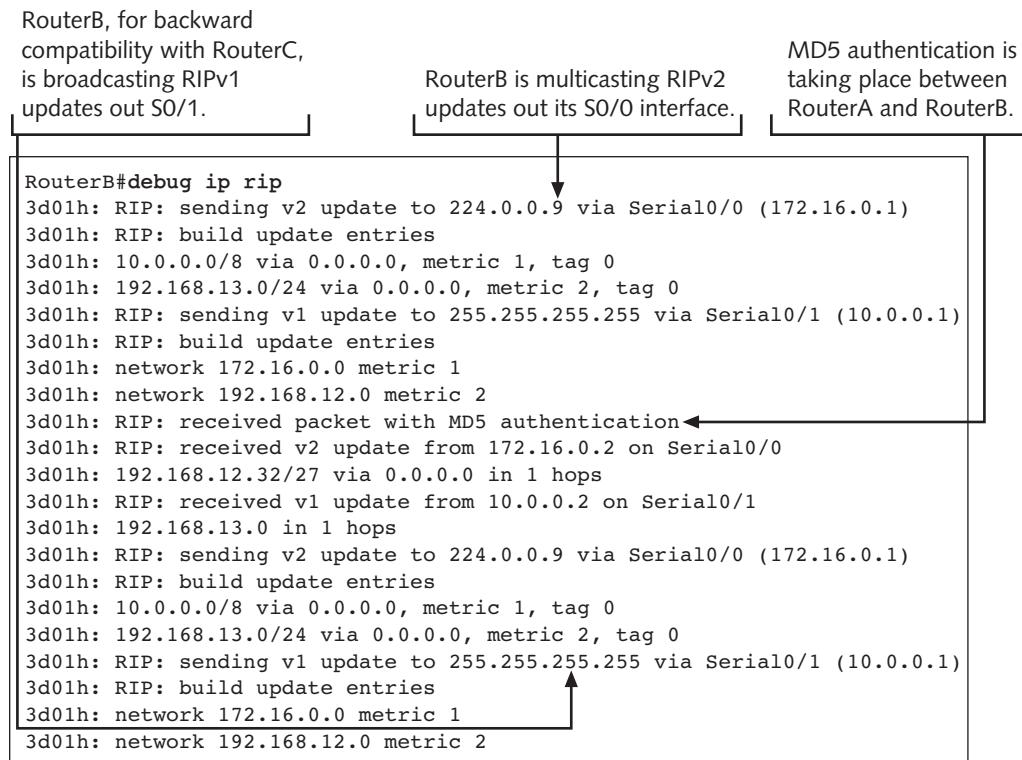
RouterB#debug ip rip
RIP protocol debugging is on
RouterB#
3d01h: RIP: ignored v2 packet from 172.16.0.2 (invalid authentication)
3d01h: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (172.16.0.1)
3d01h: RIP: build update entries
3d01h: 10.0.0.0/8 via 0.0.0.0, metric 1, tag 0
3d01h: 192.168.13.0/24 via 0.0.0.0, metric 2, tag 0
3d01h: RIP: sending v1 update to 255.255.255.255 via Serial0/1 (10.0.0.1)
3d01h: RIP: build update entries
3d01h: network 172.16.0.0 metric 1

```

**Figure 8-17** RIPv2 authentication failure

Once both routers have been configured with MD5 authentication, the `debug ip rip` command displays output similar to that shown in Figure 8-18. In this output, it is clearly visible that RouterB is accepting authenticated updates from RouterA via RIPv2 and unauthenticated updates from RouterC via RIPv1.

Figure 8-18 also shows the following features described in this section: RouterB multicasting RIPv2 updates via 224.0.0.9 to RouterA; RouterB broadcasting RIPv1 updates via 255.255.255.255; and MD5 authentication.



**Figure 8-18** RIPv2 authentication success

Although RIPv2 has many enhancements, its 15 hop-count limit and distance-vector qualities curtail its usefulness in large enterprise networks, where routing protocols such as Enhanced Interior Gateway Routing Protocol and Open Shortest Path First are better choices.

## Enhanced Interior Gateway Routing Protocol

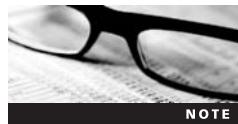
Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary protocol designed to overcome the limitations found in IGRP. Although it is often described as a hybrid protocol containing the features of both distance-vector and link-state protocols, EIGRP is still a distance-vector routing protocol at its core, albeit an advanced one. EIGRP is classless, whereas RIPv1 and IGRP are classful. Therefore, EIGRP can support VLSM and complex internetworks. EIGRP can also route IP, IPX, and AppleTalk. **Protocol Dependent Modules (PDMs)** allow EIGRP to carry these multiple routed protocols within their own native packet formats. Finally, EIGRP uses nonperiodic, partial, and bounded routing table updates. So, EIGRP does send route information to directly connected neighbors, but not on a periodic basis. Instead, updates are only sent when changes occur to the network. Also, the updates do not include the entire routing table; they are partial, meaning that only routes that have changed are sent. Additionally, the updates are sent only to the routers that need to learn them, not to all directly connected routers. These updates are therefore considered bounded. Finally, because network security is paramount in today's world, EIGRP, like RIPv2, supports authentication of routing peers.

EIGRP is more than the addition of a few features to IGRP. In fact, while still backward-compatible with IGRP, EIGRP is a significantly better routing protocol for use in large enterprise networks. EIGRP, like IGRP, makes use of a composite metric comprised of six different factors:

- *Hops*—Number of routers between source and destination networks
- *Load*—The load on a link in the path
- *Bandwidth*—The speed of the link (default)
- *Reliability*—Measures reliability of a link with a scale of 0 to 255
- *Delay*—The delay of a link (default)
- *MTU*—The maximum datagram size allowed on a link

By default, the formula used for metric calculation in EIGRP is:

$$\text{Metric} = [(K1 * \text{Bandwidth} + (K2 * \text{Bandwidth})/(256 - \text{load}) + K3 * \text{Delay}) * K5 / (\text{reliability} + K4)] * 256$$



The default values for the K variables are:

K1 = 1  
K2 = 0  
K3 = 1  
K4 = 0  
K5 = 0



Using these default values, the metric for EIGRP can be simplified to the following formula:

$$(\text{Bandwidth} + \text{Delay}) * 256$$

While changing the default K values is possible with EIGRP, doing so is not recommended unless a very specific problem arises that can only be solved by the values changing. Otherwise, for the stability of an EIGRP network, it is best for the values to stay at their defaults. Also, note that the Delay mentioned in the metric is the sum of all delays in a path to a network. On Cisco equipment, each type of interface has a default delay value assigned to it. Likewise, all interfaces have a bandwidth set based upon their type. In order to ensure the use of a correct bandwidth value, each interface should have its bandwidth set using the `bandwidth` command.

EIGRP uses the same metric as IGRP multiplied by 256. As a result, by simply multiplying or dividing metrics by 256, EIGRP can automatically share or redistribute routes between EIGRP and IGRP. This automatic redistribution of routes takes place between two routers if they are configured with the same autonomous system (AS) numbers. Figure 8-19 shows a network where EIGRP and IGRP automatic redistribution occurs. RouterB is configured with both EIGRP and IGRP using the autonomous system number of 52. As a result, the IGRP routes from RouterC are redistributed into EIGRP.

Figure 8-20 shows the routing table of RouterA. RouterA has a normal EIGRP route, flagged as “D” in the routing table, and external EIGRP routes, flagged as “D EX.” The redistribution of the 10.0.0.0/8 and 192.168.13.0/24 networks to RouterA via EIGRP required no extra configuration, apart from enabling both EIGRP and IGRP with the same autonomous system number on RouterB. This is unique, as redistribution of routing protocols normally requires additional work. With the discontinuation of IGRP in recent versions of the IOS, this automatic redistribution has lost much of its importance.

## 212 Chapter 8 Advanced Routing Protocols

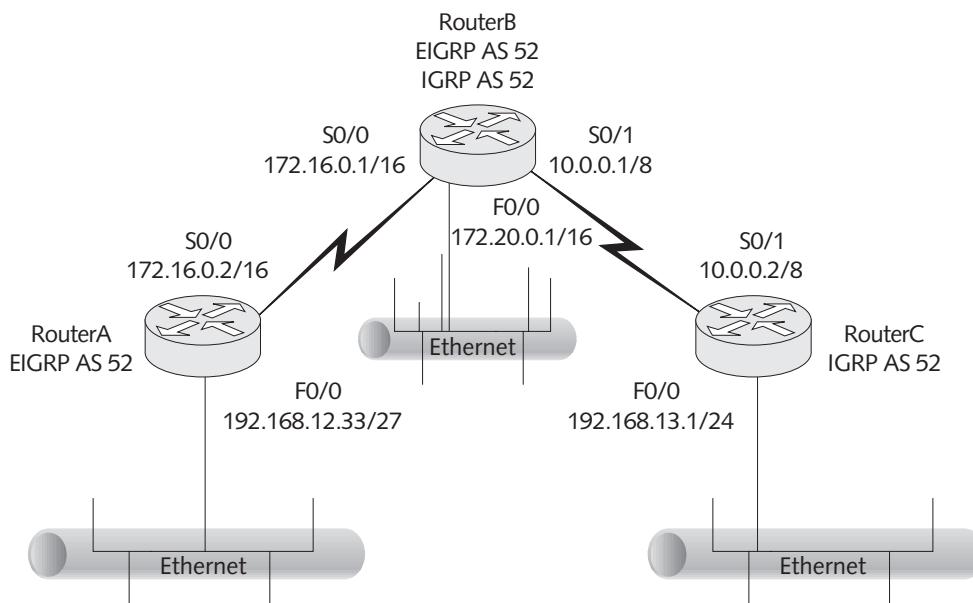


Figure 8-19 EIGRP example network

A "D" in the routing table signifies a route learned via an EIGRP neighbor.

EIGRP can see when a route has been redistributed from another routing protocol. Therefore, it marks the route as an external route learned from an EIGRP neighbor.

```

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, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      192.168.12.0/27 is subnetted, 1 subnets
      C 192.168.12.32 is directly connected, FastEthernet0/0
D EX 192.168.13.0/24 [170/21026560] via 172.16.0.1, 00:01:00, Serial0/0
C 172.16.0.0/16 is directly connected, Serial0/0
D 172.20.0.0/16 [90/20514560] via 172.16.0.1, 00:01:00, Serial0/0
D EX 10.0.0.0/8 [170/21024000] via 172.16.0.1, 00:01:00, Serial0/0
RouterA#

```

Figure 8-20 EIGRP/IGRP route redistribution

EIGRP continues to grow with each new iteration. EIGRP for IPv6 has been developed and will be ready for use once IPv6 becomes the standard.

## **EIGRP Components**

EIGRP is made up of four major components:

- Protocol Dependent Modules (PDM)
- Neighbor discovery and maintenance
- Reliable Transport Protocol
- Diffusing Update Algorithm (DUAL)

As mentioned earlier, Protocol Dependent Modules allow EIGRP to support multiple Network layer routed protocols such as IP, IPX, and AppleTalk. Each PDM is designed to allow EIGRP to provide any protocol-specific needs, such as packet formats. This discussion of EIGRP focuses on IP environments and therefore relies on the IP-EIGRP PDM.

Unlike other distance-vector protocols such as RIP and IGRP, which broadcast their entire routing table out to all interfaces, EIGRP must be able to keep updates bounded, sent only to those peers that need the information. To accomplish this task, EIGRP must build a neighbor table of directly connected peers. Neighbor discovery and maintenance allow EIGRP to discover neighbors and keep track of their status. EIGRP uses multicast address 224.0.0.10 to multicast Hello packets every five seconds on most networks of T1 speed or greater. On some slower WAN links (Frame Relay and multipoint links slower than T1 speed), Hello packets are sent as unicasts every 60 seconds to conserve bandwidth. The Hello packets allow EIGRP neighbors to determine if routing peers are still online and available. Once a Hello packet is received, a router determines a hold-down timer for its peer. By default, the hold-down timer is three times the Hello interval. So, on higher-speed connections such as Ethernet, the hold-down timer is 15 seconds. If a router does not hear a Hello from a neighbor before the expiration of the hold-down time, it marks the neighbor as unavailable and begins the process of recalculating routes. Unlike other routing protocols, EIGRP does not require all peer routers to have the same Hello and hold-down timers. As part of the Hello process, EIGRP neighbors inform one another of their currently configured timers. The timers are configurable on a per-interface basis. Still, unless a particular reason exists to change the default, the timers should be left at the defaults. Regardless of their interval, Hello packets use the Reliable Transport Protocol as their Transport layer protocol.

Because EIGRP is protocol-independent, it cannot use existing Transport layer protocols to carry its various packet types. Instead, Cisco developed an entirely new layer 4 protocol, the **Reliable Transport Protocol (RTP)**, for use by EIGRP. Reliable Transport Protocol is somewhat of a misnomer, as it can actually provide both reliable and unreliable delivery. For instance, the Hello packets are sent as unreliable multicasts. Having to acknowledge every Hello would be an enormous waste of bandwidth. Routing table updates are an example of an EIGRP packet type that uses reliable multicast via RTP. Reliable multicast is a feature of RTP that requests an acknowledgment via unicast to a multicast message. EIGRP uses reliable multicast to ensure that certain packets are

## 214 Chapter 8 Advanced Routing Protocols

acknowledged. In fact, EIGRP uses five packet types. Table 8-1 lists each packet type and its transport type:

| Packet Type     | Purpose                             | Transport Type                           |
|-----------------|-------------------------------------|------------------------------------------|
| Hellos          | Maintain neighbor status            | Multicast, unreliable                    |
| Acknowledgments | Reply to reliable multicast request | Unicast, unreliable                      |
| Updates         | Carry route information             | Unicast for update to single router      |
|                 |                                     | Multicast for update to group of routers |
|                 |                                     | Reliable delivery                        |
| Queries         | Used by DUAL to compute best paths  | Multicast or unicast, reliable delivery  |
| Replies         | Used by DUAL to compute best paths  | Unicast, reliable delivery               |

**Table 8-1** EIGRP packet types

The Diffusing Update Algorithm (DUAL) is the heart and soul of EIGRP, and is the reason that EIGRP can quickly recover from a link outage and route around network problems. In order to understand DUAL, you must understand several key terms associated with it:

- **Successor**—The best route to a destination; the next hop route to a network; stored in the EIGRP topology table and placed as the best route in the actual routing table
- **Feasible distance (FD)**—The lowest metric to a destination (determines which route becomes the successor)
- **Reported distance (RD)**—The distance a router advertises to a network; in other words, the distance from an advertising router to a network
- **Feasible successor**—A backup route to the successor route; must meet the feasibility condition for DUAL; stored as a backup in the topology table; does not get placed in the routing table until the successor fails
- **Feasibility condition**—Used to ensure that a backup route (i.e., a feasible successor) does not contain a loop; to become a feasible successor, a router's RD must be less than its neighbor's FD. The easiest way to remember the feasibility condition is:  
If  $RD < FD$  = feasible successor
- **Adjacency**—A relationship formed between EIGRP neighbors through the use of Hello packets

DUAL uses the EIGRP topology table to track the status of all links in a network. To better understand DUAL, it is best to observe it in action on a network. Figure 8-21 shows the network that will be used in this discussion. Each Cisco 1721 router is running EIGRP with an autonomous system number of 52. Each router creates a neighbor relationship with Hello packets. Figure 8-22 shows the output of the `show ip eigrp neighbors` command on RouterA. This command lists a router's EIGRP neighbors in the order they were discovered. Once neighbors have been discovered, EIGRP runs the DUAL algorithm to create the EIGRP topology table.

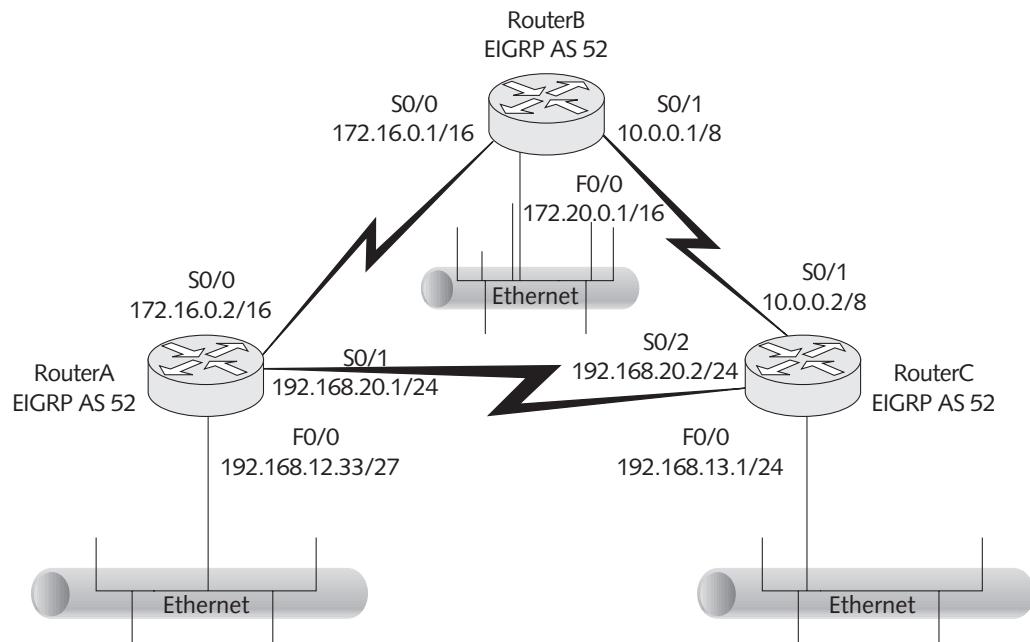


Figure 8-21 DUAL example network

Neighbors are listed in the order they are learned.

Neighbors' IP addresses are listed.

Interface column specifies the interface from which RouterA is receiving its neighbor's Hello packets.

| H | Address      | Interface | Hold<br>(sec) | Uptime   | SRTT<br>(ms) | RTO  | Q<br>Cnt | Seq<br>Num | Type |
|---|--------------|-----------|---------------|----------|--------------|------|----------|------------|------|
| 1 | 192.168.20.2 | Se1       | 11            | 01:03:49 | 647          | 3882 | 0        | 5          |      |
| 0 | 172.16.0.1   | Se0       | 13            | 22:44:45 | 395          | 2370 | 0        | 16         |      |

Figure 8-22 Output of the show ip eigrp neighbors command output

The EIGRP topology table contains information about all the networks a router can reach. Using the `show ip eigrp topology` command shown in Figure 8-23, you can display information garnered from the DUAL process. The output includes several items of particular interest. To begin, you can see that RouterA has two successors to the 10.0.0.0/8 network. This is possible because the routes are equal cost, which is apparent because the feasible distance (FD) via 192.168.20.2 and 172.16.0.1 is equal: 21024000.

Another item of interest is the single successor to the 192.168.13.0/24 network, even though Figure 8-21 clearly shows that another route via RouterB is available. Why does the second route not show up as a feasible successor? The answer lies in the feasibility condition. In order for a route to be a feasible successor, the advertising router's reported distance (RD) must be less than the receiving router's FD. Figure 8-23 shows that RouterA's FD to 192.168.13.0/24

## 216 Chapter 8 Advanced Routing Protocols

```

RouterA#show ip eigrp topology
IP-EIGRP Topology Table for AS(52)/ID(192.168.12.33)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/8, 2 successors, FD is 21024000
      via 192.168.20.2 (21024000/20512000), Serial0/1
      via 172.16.0.1 (21024000/20512000), Serial0/0
P 192.168.12.32/27, 1 successors, FD is 28160
      via Connected, FastEthernet0/0
P 192.168.13.0/24, 1 successors, FD is 20514560
      via 192.168.20.2 (20514560/28160), Serial0/1
P 192.168.20.0/24, 1 successors, FD is 20512000
      via Connected, Serial0/1
P 172.20.0.0/16, 1 successors, FD is 20514560
      via 172.16.0.1 (20514560/28160), Serial0/0
P 172.16.0.0/16, 1 successors, FD is 20512000
      via Connected, Serial0/0
RouterA#

```

**Figure 8-23** Output of the show ip eigrp topology command

is 20514560. Figure 8-24 displays the show ip eigrp topology command on RouterB. RouterB's FD to the 192.168.13.0 network is 20514560. The feasibility condition states that, to become a feasible successor, the RD of the neighbor must be less than the FD. In this case, RouterA's FD is 20514560 and RouterB's RD is 20514560. Because the RD is not less than the FD, the feasibility condition is not met, and no feasible successor exists in the EIGRP topology table for RouterA. If the link between RouterA and RouterC failed, the DUAL algorithm would run and the route through RouterB would then be installed in the routing table. In truth, the topology table does contain the link via RouterB. To see it, you must use the show ip eigrp topology all-links command, as shown in Figure 8-25.

RouterB's feasible distance is the distance it will advertise to RouterA as its reported distance (RD). In short, the RD is the best path a neighboring router has to the destination network.

```

RouterB#show ip eigrp topology
IP-EIGRP Topology Table for AS(52)/ID(172.16.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/8, 1 successors, FD is 20512000
      via Connected, Serial0/1
P 192.168.12.32/27, 1 successors, FD is 20514560
      via 172.16.0.2 (20514560/28160), Serial0/0
P 192.168.13.0/24, 1 successors, FD is 20514560 ←
      via 10.0.0.2 (20514560/28160), Serial0/1
P 192.168.20.0/24, 2 successors, FD is 21024000
      via 172.16.0.2 (21024000/20512000), Serial0/0
      via 10.0.0.2 (21024000/20512000), Serial0/1
P 172.20.0.0/16, 1 successors, FD is 28160
      via Connected, FastEthernet0/0
P 172.16.0.0/16, 1 successors, FD is 20512000
      via Connected, Serial0/0
RouterB#

```

**Figure 8-24** RouterB show ip eigrp topology command output

Only one successor exists for the 192.168.13.0 network, but EIGRP still keeps the second route in the topology table in case the primary route fails. This is one reason convergence is so fast with EIGRP.

```
RouterA#show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(52)/ID(192.168.12.33)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/8, 2 successors, FD is 21024000, serno 15
      via 192.168.20.2 (21024000/20512000), Serial0/1
      via 172.16.0.1 (21024000/20512000), Serial0/0
P 192.168.12.32/27, 1 successors, FD is 28160, serno 1
      via Connected, FastEthernet0/0
P 192.168.13.0/24, 1 successors, FD is 20514560, serno 16
      via 192.168.20.2 (20514560/28160), Serial0/1
      via 172.16.0.1 (21026560/20514560), Serial0/0 ←
P 192.168.20.0/24, 1 successors, FD is 20512000, serno 14
      via Connected, Serial0/1
P 172.20.0.0/16, 1 successors, FD is 20514560, serno 8
      via 172.16.0.1 (20514560/28160), Serial0/0
      via 192.168.20.2 (21026560/20514560), Serial0/1
P 172.16.0.0/16, 1 successors, FD is 20512000, serno 2
      via Connected, Serial0/0
```

8

**Figure 8-25** Output of `show ip eigrp topology all-links` command

In all the outputs showing the topology table for EIGRP, the routes are tagged as “P” or Passive. In EIGRP, passive is a good state, as it means all DUAL computations have been completed and the route is stable. A route marked passive can be installed in the routing table and used to route packets. If a neighbor becomes unavailable for some reason, the table may list a route as “A” or Active. If marked as active, DUAL is sending queries and replies in an attempt to find the FD and the successor. Occasionally, due to hardware errors or configuration errors, a route may become “stuck in active.” While in this state, the route cannot be passed for inclusion in the routing table and packets cannot be routed to that network via EIGRP.

Using the hold-down time in the neighbor table, EIGRP learns about down neighbors in as quickly as 15 seconds. The use of the topology table allows EIGRP to keep successors and feasible successors, or backup routes, that can be quickly installed in the event of a link failure. Ultimately, the routing table is the final destination for the information found via EIGRP’s extensive route selection process. Via DUAL and the three tables—the neighbor table, topology table, and routing table—EIGRP can converge quickly in the event of most network problems. For this reason, EIGRP is a commonly used protocol in Cisco-only networks.

## EIGRP Configuration

EIGRP configuration is nearly identical to IGRP configuration. Figure 8-26 shows the commands necessary to configure basic EIGRP on RouterA.

Notice that the `no auto-summary` command is used once again. Like RIPv2, EIGRP is classless, but it summarizes to classful network boundaries by default. The `no auto-summary` command turns off this default behavior. EIGRP configuration requires turning on the EIGRP process with the `router eigrp [process-id]` command. Each router will only share EIGRP information with other EIGRP routers configured with the same process id.

## 218 Chapter 8 Advanced Routing Protocols

```

RouterA>enable
RouterA#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#router eigrp 52
RouterA(config-router)#no auto-summary
RouterA(config-router)#network 192.168.20.0
RouterA(config-router)#network 172.16.0.0
RouterA(config-router)#network 192.168.12.0
RouterA(config-router)#^Z
RouterA#

```

**Figure 8-26** EIGRP configuration

The process-id is analogous to a workgroup name in Windows networking. The process-id is a number between 1-65535 that, when the same between two routers, allows them to share EIGRP routes.

It is also highly recommended that you use the bandwidth command to set the actual bandwidth on serial links. Otherwise, EIGRP will make path selections based on the default link speed for an interface. Because serial links on Cisco routers default to 1.544 Mbps, not setting the bandwidth on a 56K link could cause strange routing behavior. Adding the eigrp log-neighbor-changes command to your EIGRP configuration is also helpful. This command tracks neighbor state changes and will show you why neighbors have been reset. You must enter this command at the (config-router) # mode. Figure 8-27 shows EIGRP routes in the routing table of RouterA. All of the EIGRP routes in this table come from the EIGRP topology table.

The first number is the administrative distance and the second is the metric to the network. In this case, the two successors from the EIGRP topology table have been installed as equal cost paths in the routing table.

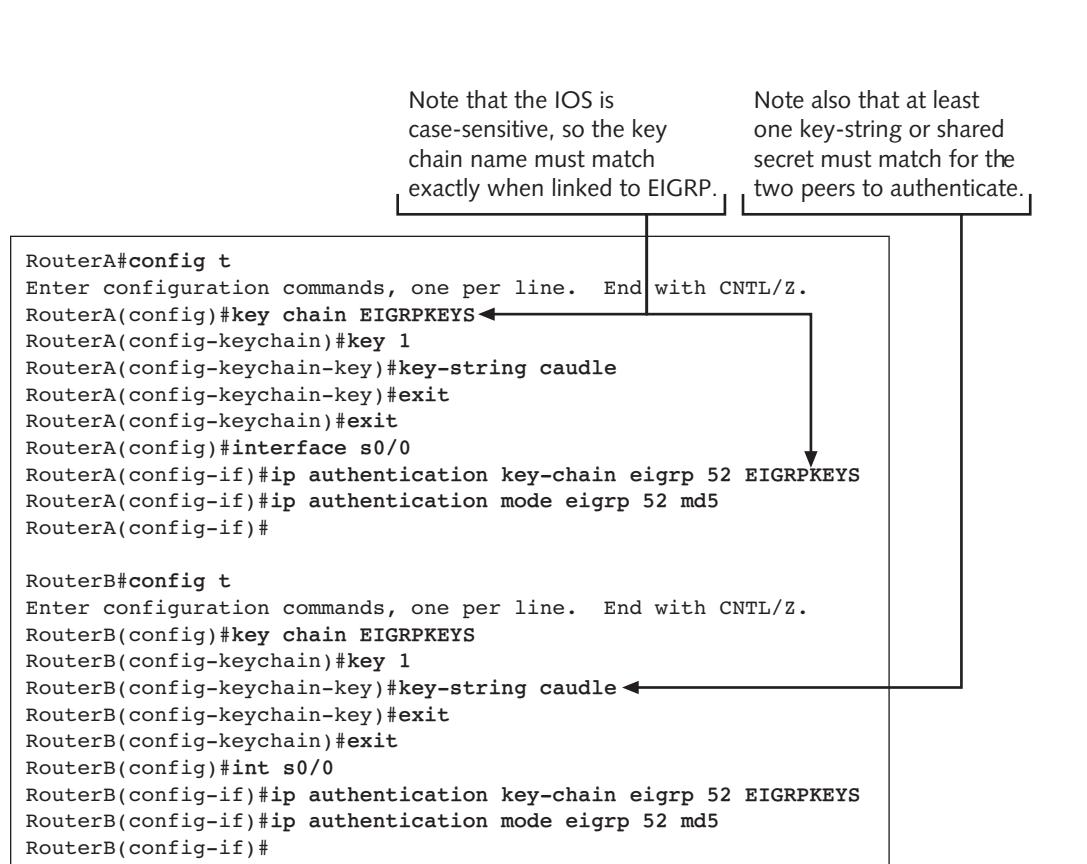
|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <pre> 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, ia - IS-IS inter area       * - candidate default, U - per-user static route, o - ODR       P - periodic downloaded static route  Gateway of last resort is not set        192.168.12.0/27 is subnetted, 1 subnets C        192.168.12.32 is directly connected, FastEthernet0/0 D        192.168.13.0/24 [90/20514560] via 192.168.20.2, 00:00:03, Serial0/1 C        172.16.0.0/16 is directly connected, Serial0/0 D        172.20.0.0/16 [90/20514560] via 172.16.0.1, 00:00:03, Serial0/0 C        192.168.20.0/24 is directly connected, Serial0/1 D        10.0.0.0/8 [90/21024000] via 192.168.20.2, 00:00:03, Serial0/1                                          [90/21024000] via 172.16.0.1, 00:00:03, Serial0/0 </pre> |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Figure 8-27** EIGRP routing table

EIGRP supports optional authentication of routing peers. Unlike RIPv2, however, it only supports MD5 authentication. Configuring EIGRP authentication requires the following steps:

- Define a key chain.
- Define keys in the key chain.
- Enable authentication on the interface by specifying the key chain to be used.
- Manage the keys (optional key lifetimes).

Figure 8-28 shows the commands necessary on RouterA and RouterB to configure authentication. The figure shows each router with matching key chain names. The key chain names do not have to match, but the routers must have a common key-string. In this case, both routers have a key-string of caudle and therefore will authenticate with one another. EIGRP is a powerful routing protocol that greatly enhances Cisco-only networks. However, because it is proprietary, many networks either will not or cannot use it. To provide robust routing services on multivendor networks, many system administrators turn to the open standards link-state protocol called Open Shortest Path First.



**Figure 8-28** EIGRP authentication

## Open Shortest Path First

Large networks consisting of equipment from multiple vendors cannot use the advanced features of the Cisco proprietary protocol EIGRP. Moreover, many corporations make open standards protocols a requirement in their networks. **Open Shortest Path First (OSPF)** is an open standards, link-state routing protocol that supports classless routing, variable-length subnet masks, and authentication.

Link-state routing protocols allow routers to share a common view of the entire network. Each router sends out link-state advertisements (LSAs) describing its attached links to all routers in an area. These LSAs are not periodic. Instead, they are sent only when a change occurs in the network. The nonperiodic nature of the updates saves network bandwidth. The downside of link-state routing protocols comes from the need for each router to hold a topological database of the entire area; this requirement increases CPU and memory demands on a router. Because OSPF creates an adjacencies database (basically a neighbor database similar to EIGRP), a topological database, and a routing table, it requires more memory to run than a simple protocol such as RIP, which only creates a routing table. OSPF parameters are also much more complex to configure. However, for the CCNA, configuring OSPF in a single area is the only exam objective. Complex configurations of OSPF in a multi-area environment are part of CCNP study.

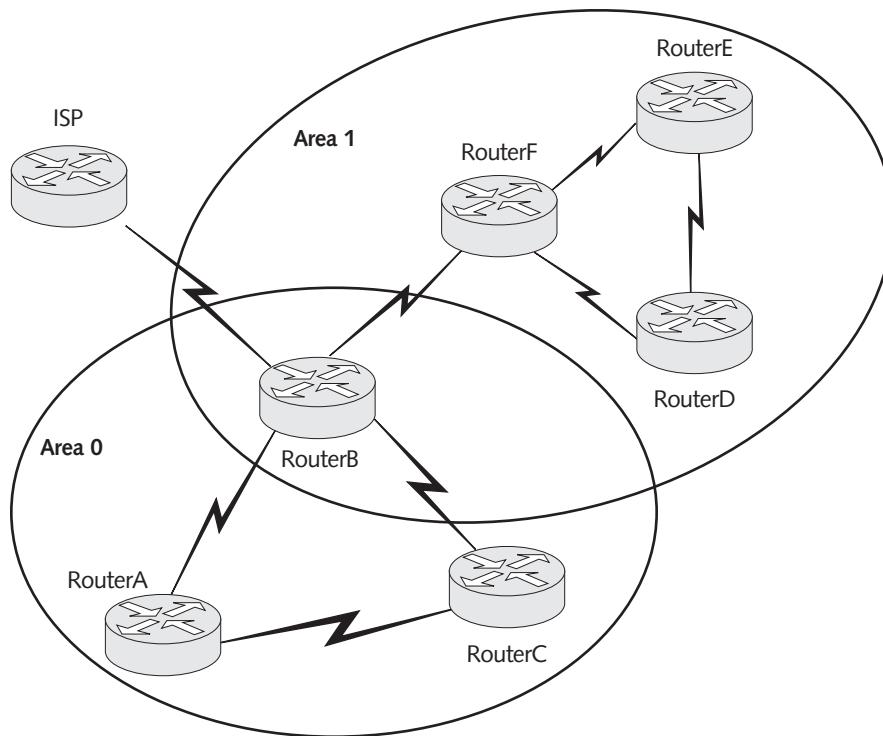
Table 8-2 summarizes the main differences between distance-vector and link-state routing protocols.

| Distance-vector                                                  | Link-state                                                                                                                                                                                      |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Periodically broadcasts entire routing table to neighbor routers | Multicasts links to all neighbor routers in the AS on startup; all other routing table updates contain only updated routes; typically, updates only occur when a network topology change occurs |
| Slow to converge                                                 | Fast to converge due to link-state advertisements                                                                                                                                               |
| Prone to routing loops because of routing by rumor nature        | Less prone to routing loops because all other routers share a common view of the network                                                                                                        |
| Easy to configure and administer                                 | Harder to configure; requires greater memory and processing power on each router                                                                                                                |
| Consumes relatively more bandwidth                               | Consumes relatively less bandwidth                                                                                                                                                              |

**Table 8-2** Major characteristics of distance-vector and link-state routing protocols

OSPF is ideally suited for large networks because it can use a concept known as areas to bound link-state advertisements. An **area** is the portion of a network within which LSAs are contained. All OSPF routers configured with the same area identification will accept LSAs from one another. Figure 8-29 shows an OSPF network that has been designed with two areas. Area 0 is the only required area in an OSPF network. In other words, all OSPF networks must have an area 0 configured. The significance of areas becomes apparent when you realize how LSAs are bounded within an area. In Figure 8-29, area 0 LSAs affect only routers A, B, and C. LSAs for area 1 only affect routers B, D, E, and F. Therefore, if a link on RouterA goes down, it will inform only RouterB and RouterC that the link has gone down. The ability to design OSPF in this bounded, hierarchical fashion is solely the result of the concept of areas.

In the sample network, network administrators may have placed routers B, D, E, and F in a separate area because of a known problem with route flapping or because those routers did not contain the memory needed to hold a topological database of the entire network. They may also have created the area simply as a way to logically group a set of routers in a geographical location. With OSPF, network designers have great flexibility. Still, as mentioned earlier, CCNAs only need to be able to configure single-area OSPF.



**Figure 8-29** OSPF areas

## OSPF Concepts

In order to configure OSPF, you must understand several main concepts associated with it:

- Link
- Link-state
- Area
- Cost
- Adjacencies database
- Topological database
- Designated router
- Backup designated router

A **link** in OSPF is a router's interface. So, a router has a link for each interface configured to run OSPF. **Link-state** is the status of a link on a router. An area defines the confines within which LSAs are contained. Areas, which were discussed in detail earlier, are responsible for allowing OSPF to use a hierarchical network design.

**Cost** is the default metric for OSPF. A link's cost is computed using the following formula:

$$\text{Cost} = (10^8 / \text{bandwidth of the link})$$

## 222 Chapter 8 Advanced Routing Protocols

Because the cost is computed using the bandwidth of the link, you must correctly set the bandwidth on serial interfaces using the `bandwidth [speed in kilobits]` command. If you do not set the bandwidth, OSPF will use the default speed of 1.544 Mbps on serial links, which may not be accurate. Table 8-3 shows Cisco's default OSPF costs for certain link types. As networks continue to increase in speed, OSPF will need to be modified to compute correct costs. Otherwise, Fast Ethernet, Gigabit Ethernet, and even 10-GB Ethernet will all have a cost of 1, even though their bandwidth specifications are different. This is because OSPF rounds off all fractions resulting from the cost formula to 1. Lower-cost routes are considered better in OSPF.

| Link Type                      | Cisco Default Cost |
|--------------------------------|--------------------|
| FDDI, Fast Ethernet and faster | 1                  |
| Ethernet                       | 10                 |
| E1 (2.048 Mbps)                | 48                 |
| T1 (1.544 Mbps)                | 64                 |
| 56 Kbps                        | 1785               |

**Table 8-3** Cisco's default OSPF costs for certain link types

To solve the problem of high-speed links and cost calculation, Cisco has introduced the idea of a reference-bandwidth to OSPF. By default, the reference-bandwidth for OSPF cost calculations is Fast Ethernet or 100 Mbps. Therefore, any link 100 Mbps or faster has a cost of 1. As shown in Figure 8-30, the `show ip protocols` command on a router running OSPF displays the current reference-bandwidth configured.

```
RouterA#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.12.33
  Number of areas in this router is 0.0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    Reference bandwidth unit is 100 mbps
    Routing Information Sources:
      Gateway          Distance      Last Update
      Distance: (default is 110)
```

OSPF cost calculation based on Fast Ethernet as the reference bandwidth.

**Figure 8-30** Determining OSPF reference bandwidth

If a network consists of predominately Gigabit or higher speed links, it may be appropriate to change the reference-bandwidth to 1000 Mbps or greater. Be careful when changing reference-bandwidth, however, as OSPF has a maximum cost of 65535. The command used to change the reference-bandwidth is:

```
RouterA(config-router)#auto-cost reference-bandwidth [1-4294967]
```

In a network with a wide variation of link speeds, setting the reference bandwidth too high can result in a link having a metric above 65535. For example, if the reference bandwidth is set to 10,000 Mbps, the auto cost calculation formula would change to  $10^{10}/\text{bandwidth}$ . Using this reference-bandwidth, a 56 Kbps link is not reachable:

$$100000000000/56000 = 178571 \text{ cost}$$

The cost of the 56 Kbps link using the modified reference-bandwidth exceeds the maximum cost for an OSPF metric. In a network of very fast links, however, link costs are more accurately reflected using the reference-bandwidth of 10,000 Mbps:

|                       |                                               |
|-----------------------|-----------------------------------------------|
| 10 GB Ethernet metric | $100000000000/10000000000 = 1 \text{ cost}$   |
| 1 GB Ethernet metric  | $100000000000/10000000000 = 10 \text{ cost}$  |
| Fast Ethernet metric  | $100000000000/10000000000 = 100 \text{ cost}$ |



Changes to the reference-bandwidth must be made to all routers running OSPF or the router in the internetwork will disagree on correct cost values for links.

**NOTE**



OSPF shares the concept of a neighbor table with EIGRP. In OSPF, the **adjacencies database** contains information about all OSPF peers with which a router has successfully exchanged Hello packets. Once two neighboring routers establish bidirectional communication via Hello packets, they add one another to their respective adjacency databases. Hellos are multicast to a special multicast address of 224.0.0.5. This address is reserved for all OSPF routers, and they will accept anything sent to the address. Hello intervals for OSPF are different depending on the network in use. On broadcast or multiaccess networks such as Ethernet, Hellos are sent every 10 seconds by default. On nonbroadcast networks such as Frame Relay, Hellos are sent every 30 seconds by default.

OSPF also makes use of a dead interval, similar to an EIGRP hold-down timer. The default dead interval is four times the Hello interval. Therefore, the default dead interval is 40 seconds on broadcast networks and 120 seconds on nonbroadcast networks. Unlike EIGRP, which does not require neighbors to have their timers configured the same to become adjacent, OSPF requires that the Hello and dead interval timers match. This is a common problem when trying to implement OSPF. Many vendors set their default timers to different defaults for various reasons. To manually change the timers on a Cisco router, you can use the `ip ospf hello-interval [seconds]` and `ip ospf dead-interval [seconds]` commands. Both are interface commands (see Figure 8-31). Always be careful when changing timers. If RouterB's neighbors do not have their default timers changed, RouterB will not be able to form adjacencies or participate in OSPF LSA exchange.

```
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#interface serial 0/0
RouterB(config-if)#ip ospf hello-interval 5
RouterB(config-if)#ip ospf dead-interval 20
RouterB(config-if)#

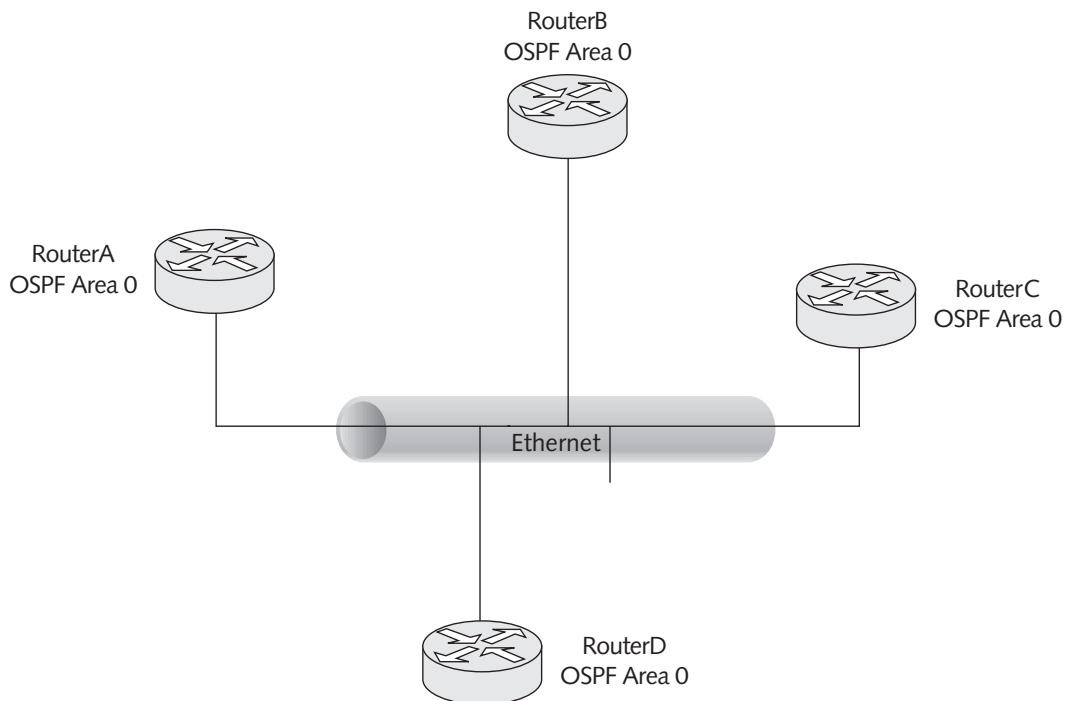
```

**Figure 8-31** Configuring OSPF timers

## 224 Chapter 8 Advanced Routing Protocols

OSPF also uses a **topological database**, which holds the common view of the network formed from the link-state advertisements that are received. The topological database allows the router to run the Shortest Path First algorithm and find the best path to a network.

The final OSPF concepts covered here are **designated routers (DRs)** and **backup designated routers (BDRs)**. On broadcast, multiaccess networks, OSPF elects a DR, which acts as a central point for LSAs. On multiaccess networks such as Ethernet, OSPF routers elect a DR and establish adjacencies with the DR only. This keeps each router from having to establish more adjacencies than necessary. In fact, the DR reduces the number of adjacencies and LSAs on a broadcast, multiaccess network. The reserved multicast address of 224.0.0.6 is used for all DRs and BDRs. In Figure 8-32, all the routers are connected to an Ethernet segment. A DR is elected on this network, and each router forms an adjacency with it. So, assume that RouterB is elected the DR. RouterA would then form an adjacency with just RouterB, the DR. If DRs were not used on broadcast, multiaccess networks, RouterA would need to form an adjacency with Routers B, C, and D, its directly connected peers. DRs allow fewer adjacencies to be needed. Likewise, RouterA will send all LSAs to the DR, and the DR will redistribute them back out to all OSPF routers using the reserved multicast address of 224.0.0.5, an address for all OSPF routers. The backup designated router has one purpose: It takes over if the DR fails.



**Figure 8-32** OSPF on a broadcast, multi-access network

The DR election occurs via the Hello process. Hello packets contain an OSPF **router ID**. This ID can be one of three things: the highest IP address configured on a loopback interface, the highest IP address on an active physical interface, or the ID set using the `ospf router-id [ip address]` command. By default, if an ID is configured using the `router-id` command, the ID will always represent that router for purposes of OSPF. The concept of a router ID is important because OSPF requires an ID to start. What is more, OSPF uses the router ID as a factor in determining which router becomes the DR or BDR. The DR election looks first at the OSPF priority of a link. By default, all links have a priority of 1. Therefore, if you want to guarantee that a router will become the DR, you can assign it the highest OSPF priority. The `ip ospf priority [0-255]` interface command allows the priority to be set from 0 to 255. The router with the second-highest priority will become the BDR. In the example network in Figure 8-32, you could ensure that RouterC becomes the DR by using the following commands:

```
RouterC(config)#interface f0/0
RouterC(config-if)#ip ospf priority 100
```

If the priorities are not changed and all the priorities are equal, the router with the highest router ID will become the DR and the router with the second-highest will become the BDR. As previously noted, the router ID is either the ID configured with the `router-id` command, the highest configured loopback, or the highest IP address on an active interface. Figure 8-33 displays the commands needed to configure a loopback address on RouterC.

```
RouterC#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterC(config)#interface loopback 0/1<-->
RouterC(config-if)#ip address 1.1.1.1 255.255.255.255
RouterC(config-if)#
```

The syntax for the loopback command is:  
**interface loopback [#].**

**Figure 8-33** Loopback address configuration

## OSPF Operation

OSPF goes through a series of steps to get a router up and running. First, an OSPF router forms adjacencies with neighbors. Routers exchange Hello packets and then place one another in their adjacency tables. Figure 8-34 shows the example network that will be used for the rest of this chapter. In this network, each router forms an adjacency with its neighbors. Figure 8-35 displays the `show ip ospf neighbor` command output from RouterB. It clearly shows that RouterB has RouterA and RouterC in its adjacency database.

## 226 Chapter 8 Advanced Routing Protocols

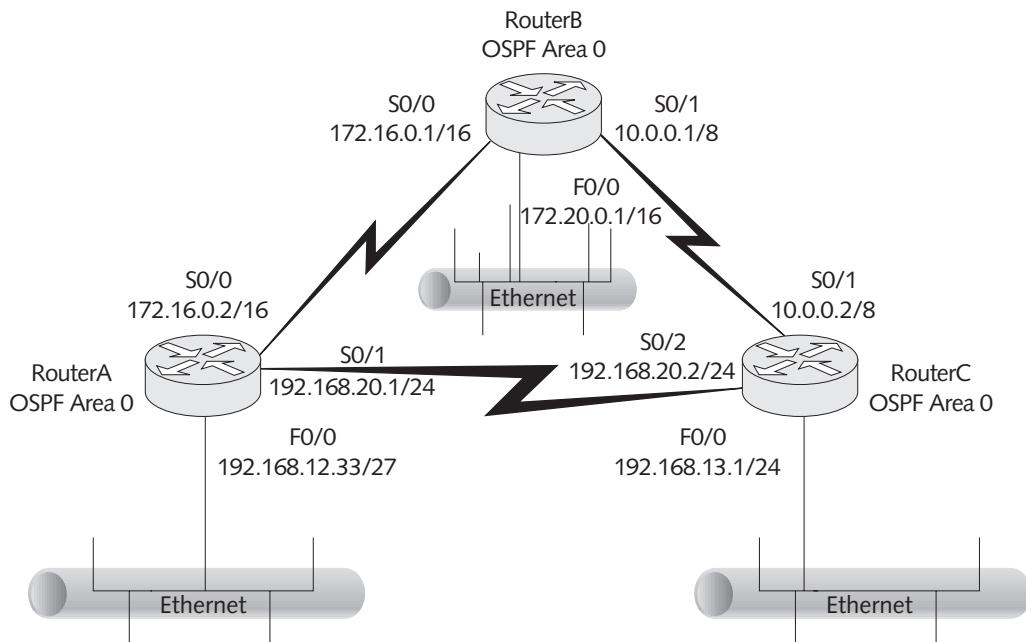


Figure 8-34 OSPF example network

The router ID is the highest IP address on an active interface on the neighbor router.

Once neighbors are in a FULL state, they have correctly formed adjacency with one another.

| RouterB#show ip ospf neighbor |     |         |           | Address    |  | Interface |  |
|-------------------------------|-----|---------|-----------|------------|--|-----------|--|
| Neighbor ID                   | Pri | State   | Dead Time |            |  |           |  |
| 192.168.20.2                  | 1   | FULL/ - | 00:00:30  | 10.0.0.2   |  | Serial0/1 |  |
| 192.168.20.1                  | 1   | FULL/ - | 00:00:32  | 172.16.0.2 |  | Serial0/0 |  |

Figure 8-35 Output of show ip ospf neighbor command

Next, a DR and BDR are elected in OSPF. Of course, the network must be broadcast and multiaccess for this election to occur. In our example, all links are point-to-point links. Therefore, no DRs or BDRs exist on the network because no election takes place.

Finally, the routers will flood their link-state advertisements and go through the process of selecting the best route to each network. OSPF uses **Dijkstra's Shortest Path First Algorithm** to find the best path. In essence, each router sees itself as the central point from which a loop-free, best-cost path to each network is determined. The SPF algorithm allows each router to quickly find the best path to a destination network. It is a complicated algorithm, however, and uses a large amount of CPU processing and memory on a router.

After routes are installed, they must be maintained. If a link fails, OSPF routers send out link-state updates to notify the network, the SPF algorithm is run to find a new route, and the new route is advertised.

During initialization and maintenance of the routing table, OSPF makes use of the five OSPF packet types described in Table 8-4.

| Type | Name                       | Function                                                                                       |
|------|----------------------------|------------------------------------------------------------------------------------------------|
| 1    | Hello                      | Neighbor discovery and adjacency maintenance                                                   |
| 2    | Database Description       | Summarizes topological database between routers during initialization of neighbor relationship |
| 3    | Link State Request         | Request Link State information from a neighbor's database                                      |
| 4    | Link State Update          | Advertises available links via network flooding                                                |
| 5    | Link State Acknowledgement | Response to flooded links sent via Link State Updates                                          |

**Table 8-4** OSPF Packet Types

## Single-Area OSPF Configuration

As with EIGRP, the concepts related to OSPF are much more difficult to master than the steps required to configure simple, single-area OSPF. In the real world, OSPF offers a huge number of configuration options, including multiple areas of different types. For the CCNA exam, you only need to know how to configure single-area OSPF. The commands to configure single-area OSPF on RouterB are shown in Figure 8-36.



```
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#router ospf 1
RouterB(config-router)#network 172.20.0.0 0.0.255.255 area 0
RouterB(config-router)#network 172.16.0.0 0.0.255.255 area 0
RouterB(config-router)#network 10.0.0.0 0.255.255.255 area 0
RouterB(config-router)#exit
RouterB(config)#

```

Once OSPF is turned on, you must then specify which networks will be advertised. Note that OSPF does not use subnet masks. Instead, it uses wildcard masks. Also, each network must be associated with an area (in this case, area 0).

OSPF is configured using the **router ospf [process id]** command.

**Figure 8-36** Single-area OSPF configuration

OSPF requires two key commands. The first command is **router ospf [process id]**, which turns on OSPF. Routers in the same area do not have to use the same process ID. The process ID is similar to a process on a server running Windows 2000 or Linux. The local router uses the process ID to keep up with the OSPF process running in memory. The other important command is the **network** command. OSPF uses wildcard masks in its network statements, which is dissimilar from all other protocols that have been discussed. Once these two commands are entered, the router begins the process of forming adjacencies and developing the topological database.

You may also want to configure default routing with OSPF. The **default-information originate** command allows injection of a default route into a network. This command must be used on the border router for the network. RouterB in Figure 8-29 would be considered

a border router. The commands to configure and inject a default route into our example network are shown in Figure 8-37.

```

RouterB(config-if)#ip route 0.0.0.0 0.0.0.0 serial0/1
RouterB(config-if)#router ospf 1
RouterB(config-router)#default-information originate
RouterB(config-router)#

```

This diagram shows a command box containing four lines of Cisco IOS configuration commands. A callout points from the first line to a note about setting a default route. Another callout points from the third line to a note about advertising the default route.

**Note:**

- The ip route command sets a default route that sends all traffic without an entry in the routing table out serial0/1.
- The default-information originate command causes RouterB to advertise its default route to the network.

Figure 8-37 Default route configuration in OSPF

## OSPF Authentication

Routing update authentication is a basic security requirement for all modern routing protocols. OSPF provides authentication of routing table updates via several methods. OSPF supports using no authentication (the default), authentication with passwords sent in clear text, or authentication using MD5 hashing of a shared secret key. Since authentication using clear text results in almost no advantage over no authentication at all, it will not be discussed in this text. Instead, the following discussion focuses on MD5 authentication.

To perform MD5 authentication of routing updates in OSPF, two steps must be completed:

- Configuration of authentication keys on each OSPF interface
- Configuration of area authentication

Figure 8-38 shows two routers that can be configured to run OSPF authentication via their serial interfaces.

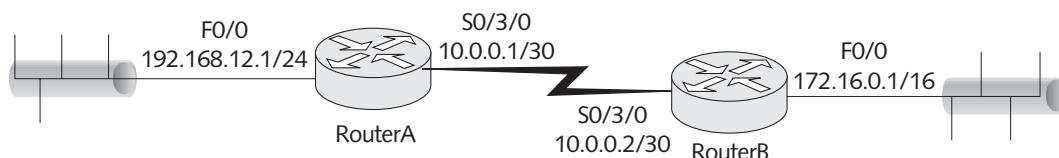


Figure 8-38 OSPF authentication example network

Configuring authentication on the interfaces is the first step to authenticate routing updates. Configuring authentication on RouterA and RouterB requires the commands shown in Figure 8-39.

```

RouterA(config)#int s0/3/0
RouterA(config-if)#ip ospf message-digest-key 1 md5 TiAspw34
RouterB(config)#interface s0/3/0
RouterB(config-if)#ip ospf message-digest-key 1 md5 TiAspw34
RouterB(config-if)#

```

This diagram shows a command box containing configuration commands for both RouterA and RouterB. A callout points from the second command on RouterA to a note about turning on MD5 authentication.

**Note:**

- Turns on MD5 authentication and sets the password to "secureme."

Figure 8-39 OSPF interface authentication commands

It is also necessary to add authentication commands for the area, as shown in Figure 8-40. The commands shown in the figure enable MD5 authentication for area 0. It is important to note that authentication is turned on for each area individually.

```
RouterA(config)#router ospf 1
RouterA(config-router)#area 0 authentication message-digest
RouterB(config)#router ospf 1
RouterB(config-router)#area 0 authentication message-digest
```

**Figure 8-40** OSPF routing protocol authentication commands

Finally, the show ip ospf command in Figure 8-41 displays information confirming that MD5 authentication has been configured on the router.

```
RouterA#sh ip ospf
Routing Process "ospf 1" with ID 192.168.12.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
    Area BACKBONE(0)
Number of interfaces in this area is 2
Area has message digest authentication
SPF algorithm last executed 00:00:57.676 ago
SPF algorithm executed 9 times
Area ranges are
Number of LSA 2. Checksum Sum 0x0113D3
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

**Figure 8-41** Verifying OSPF authentication

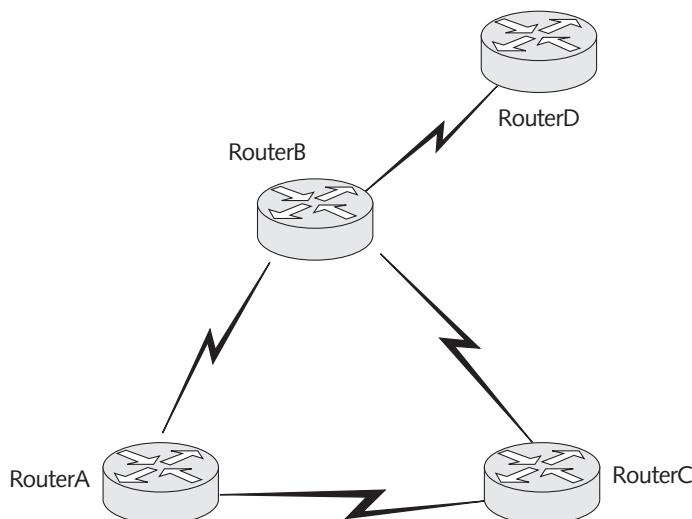
As a general rule, routing table authentication should be used on all modern networks. Likewise, when given the choice between clear text or MD5 authentication, you should use

MD5 authentication. Finally, even with MD5 authentication, it is imperative to choose good passwords for the shared secret key.

## Controlling Route Traffic

The `passive-interface` command is an important entry-level command for controlling route traffic. In the network shown in Figure 8-42, RouterD may need to learn of the RIP routes on the rest of the network, but the network does not need to know its routes because RouterB is configured to route to it statically. In short, you need a way for RouterD to hear RIP updates, but not send out updates. The `passive-interface` command allows this. To make the serial interface on RouterD passive, you must use the following commands:

```
RouterD(config)#router rip
RouterD(config-router)#passive-interface s0/0
RouterD(config-router)#+
```



**Figure 8-42** Passive-interface example

Unfortunately, this command disrupts the function of EIGRP and OSPF. The command causes a router to listen only on the passive interface. Therefore, if used with EIGRP or OSPF, the router will not send Hellos out the interface. The result is a link that is seen as having no neighbors on it, and therefore it will not be used to form adjacencies. EIGRP and OSPF do provide methods to control routing traffic, but they are beyond the scope of the CCNA and this book.

## Chapter Summary

- Large, complex internetworks using variable-length subnet masks require routing protocols that can handle the task. Several advanced routing protocols are in common use on networks today. These protocols are classless and carry subnet mask information in their routing table updates.

- RIPv2 is a classless routing protocol built as an extension to RIPv1. It supports modern networks' use of VLSM and authentication. In addition, it provides backward compatibility with RIPv1 when configured correctly. Still, RIPv2 suffers from all the pitfalls of distance-vector routing protocols.
- EIGRP is a Cisco proprietary protocol designed to incorporate some of the features of link-state routing protocols. It is, however, still a distance-vector routing protocol. EIGRP does support classless routing. Its use of neighbor, topological, and routing tables allows for quick convergence in the event of a link failure. In fact, for each destination network, EIGRP keeps a successor or best route, and if possible a feasible successor or backup route. Unfortunately, because it is proprietary, only all-Cisco networks can run EIGRP.
- The open standards protocol OSPF is the link-state protocol of choice in many networks; it supports VLSM, classless routing, and fast convergence. In OSPF, each router uses the Shortest Path First Algorithm to determine the best loop-free path to each network. Each router also uses an adjacency table, topological table, and routing table to pick the best route to a destination.

---

## Key Terms


**8**

**adjacencies database** The neighbor database in OSPF.

**adjacency** Bidirectional communication formed by EIGRP neighbors.

**area** An OSPF concept used to define the confines within which LSAs will propagate.

**backup designated router (BDR)** An OSPF router on broadcast, multiaccess networks that takes over if the DR fails.

**classful routing protocol** A dynamic routing protocol that does not carry subnet mask information in its routing table updates and consequently must summarize to major classful network boundaries.

**classless routing protocol** A dynamic routing protocol that carries subnet mask information in its routing table updates; allows support for discontiguous subnets and VLSM.

**cost** The default metric in OSPF, calculated with the following equation: Cost =  $(10^8 / \text{bandwidth of the link})$ .

**designated router (DR)** Used on broadcast, multiaccess OSPF networks as a central point for adjacencies and LSAs.

**Diffusing Update Algorithm (DUAL)** The algorithm used by EIGRP for path selection.

**Dijkstra's Shortest Path First Algorithm** A complex algorithm used by OSPF routers to determine a loop-free, lowest-cost path to a destination network.

**Enhanced Interior Gateway Routing Protocol (EIGRP)** A Cisco proprietary distance-vector protocol that uses some link-state features to improve performance.

**feasibility condition** A condition ( $RD < FD$ ) that allows a route to become a feasible successor.

**feasible distance (FD)** The lowest-cost metric to a destination.

**feasible successor** A backup route in the EIGRP topology table.

**link** An OSPF router interface.

**232** Chapter 8 Advanced Routing Protocols

**link-state** The status of an interface on an OSPF router.

**MD5** Message digest 5, an algorithm used to produce a secure hash of shared secret passwords.

**Open Shortest Path First (OSPF)** A classless link-state routing protocol that uses areas to provide for hierarchical network design.

**Protocol Dependent Modules (PDMs)** A component of EIGRP that allows it to support multiple routed protocols such as IP, IPX, and AppleTalk.

**Reliable Transport Protocol (RTP)** A Transport layer protocol used by EIGRP.

**reported distance (RD)** The distance an EIGRP router advertises to its neighbors for a network.

**router ID** A router identifier used in OSPF Hellos and updates; normally the highest configured loopback or interface address.

**successor** The best route to a destination in an EIGRP network.

**topological database** A database that holds the common view of the network formed from the link-state advertisements that are received. It allows the router to run the Shortest Path First algorithm and find the best path to a network.

## Review Questions

1. What command injects a default route into an OSPF network?
  - a. passive-interface
  - b. loopback default
  - c. router ospf
  - d. default-information originate
  
2. Classless routing protocols carry subnet mask information in their routing table updates. True or False?
  
3. The process ID must match on all routers in an OSPF network. True or False?
  
4. What command switches RIP to version 2?
  - a. router rip 2
  - b. version 2
  - c. rip version 2
  - d. ripv2 on
  
5. What command turns off automatic summarization to major network boundaries in both RIPv2 and EIGRP?
  - a. summarization off
  - b. no summary
  - c. no auto-summary
  - d. no ip classless

6. In what state are OSPF neighbors, when bidirectional communication has been established and adjacencies have been formed?
- Passive
  - Up
  - DR
  - FULL
7. Which type of authentication sends only a hash across the link between two authenticating peers?
- MD5
  - Clear text
  - Signed secret keys
  - Shared keys
8. What command places the 192.168.12.32/27 network into OSPF area 0?
- network 192.168.12.0 area 0
  - network 192.168.12.32 area 0
  - network 192.168.12.32 255.255.255.224 area 0
  - network 192.168.12.32 0.0.0.31 area 0
9. EIGRP uses the same metric as IGRP multiplied by \_\_\_\_\_.
10. What feature of OSPF allows it to use a hierarchical design?
- areas
  - auto summarization
  - wildcard masks
  - neighbor adjacencies
11. Cisco routers can be configured to send and receive RIPv1 updates on a per-interface basis. True or False?
12. What does the feasibility condition state?
13. What protocol is used by EIGRP to transport its routing protocol information?
- TCP
  - UDP
  - RTP
  - DR/BDR
14. Which of the following commands enables EIGRP on a router with an autonomous system number of 101?
- router eigrp
  - router eigrp 101
  - router 101 eigrp
  - as 101

**234** Chapter 8 Advanced Routing Protocols

15. What algorithm is used by OSPF for path selection?
  - a. DUAL
  - b. Open Path First
  - c. Shortest Path First
  - d. Default-information Originate
16. A backup route in EIGRP is a(n) \_\_\_\_\_.
17. OSPF timers must match for neighbors to form adjacencies. True or False?
18. EIGRP timers must match for neighbors to form adjacencies. True or False?
19. Which of the following commands would ensure that a router becomes the DR on a broadcast, multiaccess network?
  - a. ip ospf priority 256
  - b. ip ospf dr on
  - c. ip ospf priority 0
  - d. None of the above
20. What command displays the successors and feasible successors for EIGRP?
  - a. show ip route
  - b. show ip eigrp topology
  - c. show ip ospf topology
  - d. show ip topology
21. What command displays area authentication information?
  - a. show ip route
  - b. show ip ospf
  - c. show ip ospf authentication
  - d. show authentication
22. What OSPF priority range can be assigned to a router?
23. Clear text is the most secure authentication supported by OSPF. True or False?
24. Which of the following is used by EIGRP for path determination?
  - a. DUAL
  - b. Dijkstra's Shortest Path First Algorithm
  - c. wildcard masks
  - d. priority
25. What is the default OSPF cost for FastEthernet (assuming the default reference bandwidth)?
  - a. 40
  - b. 255
  - c. 0
  - d. 1

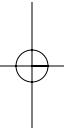
## Case Projects



CASE PROJECTS

1. Hogan Enterprises needs to implement a new TCP/IP addressing scheme using VLSM. They are currently running RIPv1 on a network consisting of seven routers, four of which are Cisco routers. After being told by another contractor that they would have to abandon RIP to use VLSM, Hogan contacted you for a second opinion. Create a short paper discussing their network and recommendations concerning the move to VLSM. What protocol do you recommend, and how would you achieve the upgrade?
2. Conner, Inc., a large think tank, currently runs IGRP on its 50-router network. They are considering upgrading to a more robust routing protocol. Write a short paper comparing and contrasting EIGRP and OSPF. In the end, you must recommend a protocol for the company and defend your position.
3. Recently, a rogue OSPF router was discovered on your network. The rogue router was feeding incorrect routing information to routers in your network. Management wants you to secure the routing infrastructure to ensure that this type of intrusion cannot happen again. Write a short paper discussing how you will secure the OSPF routers in your network to protect against rogue routers. Your paper should contain example router configurations to back up your plan.







chapter 9

# Network Services

**After reading this chapter and completing the exercises, you will be able to:**

- Understand the purpose and operation of network address translation (NAT)
- Understand and configure static NAT, dynamic NAT, and PAT
- Understand and configure Dynamic Host Configuration Protocol (DHCP)
- Understand and configure Domain Name Services (DNS)
- Configure network services using Cisco's Security Device Manager (SDM)

**This chapter explains the concepts of network services, such as the** various flavors of NAT, DHCP, and DNS. The chapter also provides instructions on how to configure these services using Cisco's SDM.

## Network Address Translation

Network address translation (NAT) allows many home users, corporations, and organizations around the world to connect far more computers to the Internet than they would otherwise be able to connect. NAT is defined in RFC 3022, which describes methods for connecting private (internal) IP addresses to the Internet. In Chapter 4, you learned that the private IP addresses specified in RFC 1918 could not be routed on the Internet. However, NAT uses a one-to-one mapping or one-to-many mapping method to allow one or more private IP clients to gain access to the Internet by mapping the private IP addresses to public IP addresses. The private addresses are shown in Table 9-1.

| Class | Private Address Range   |
|-------|-------------------------|
| A     | 10.x.x.x                |
| B     | 172.16.x.x – 172.31.x.x |
| C     | 192.168.x.x             |

**Table 9-1** RFC 1918 private address ranges

Using private addressing with NAT has several advantages over public IP addressing. First, it conserves public IP addresses. Networks can make use of the private IP address ranges and NAT to either a single external public IP or a smaller pool of public IP addresses. It also hides your internal IP addressing scheme from the outside world, greatly enhancing network security. Finally, it allows for easy renumbering of your IP addresses. For example, if you use all public IP addresses and suddenly decide to change ISPs, you must change all of your internal IP addressing. Using NAT, the internal network uses private IP addresses, which need not change. You would only need to change your outside NAT addresses if you decided to change ISPs.

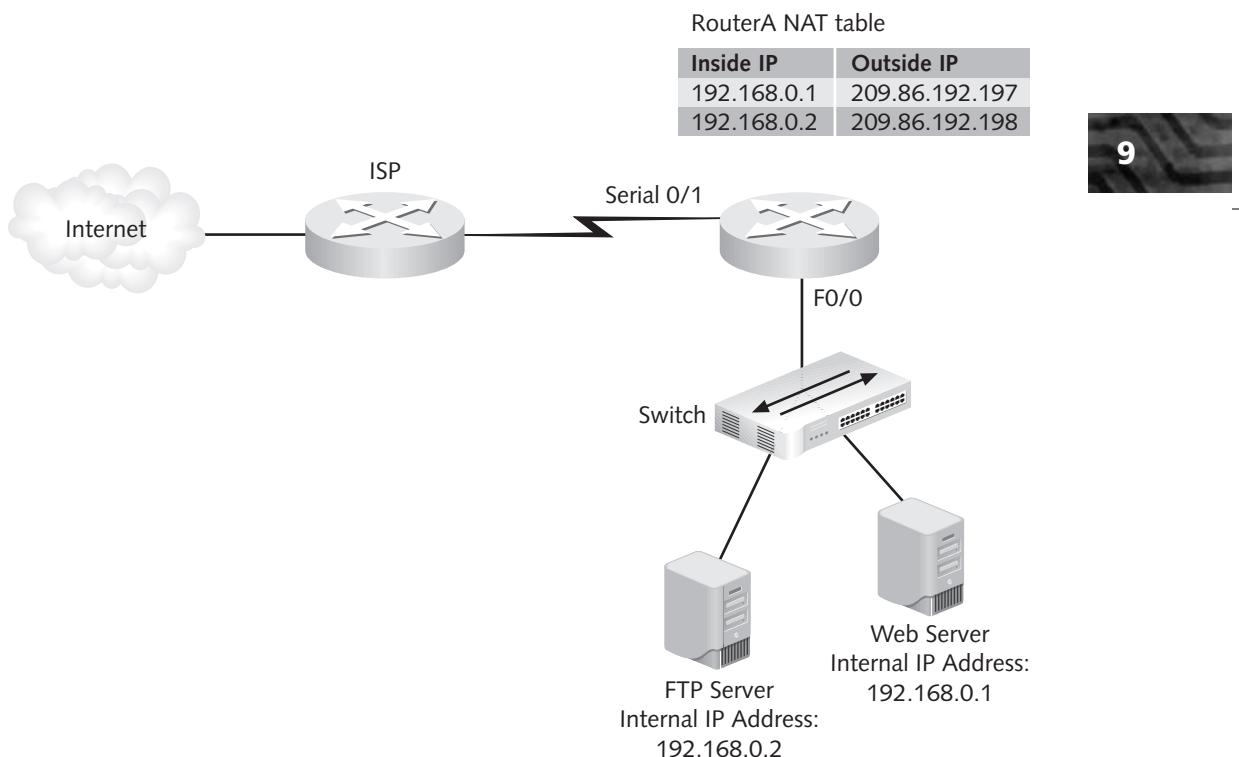
NAT does present some disadvantages, however. NAT introduces a small amount of delay into your network because the NAT router has to create and maintain the NAT table, which is a table of inside addresses and the associated outside addresses. In addition, due to the translation of the source IP address, end-to-end IP traceability is lost. While it is still possible to track a packet back to the NAT device, finding the actual original host is difficult. Finally, some applications fail due to NAT, although this was more of a problem when NAT was first implemented. Today, most modern applications expect NAT to be present on a network.

Cisco developed NAT, and today the technology is used by routers, firewalls, and even individual computers with multiple network connections. NAT is available in three forms:

- Static NAT
- Dynamic NAT
- Port address translation (PAT)

## Static NAT

Static NAT is the simplest form of NAT, in which a single private IP address is mapped to a single public IP address. For example, a router could be configured to translate all communications from the internal 192.168.0.1 address to the address 209.86.192.197. In this way, when the host 192.168.0.1 accesses the Internet, the router will translate its IP address to 209.86.192.197. The router will then translate communications between that host and any system on the Internet. Therefore, all Internet devices will communicate with host 209.86.192.197, but the actual packets will be forwarded by the NAT router to host 192.168.0.1 on the local network. In order for the NAT router to translate communications between the internal and external network, it must maintain a table in memory that maps internal IP addresses to addresses presented to the Internet (external addresses). With static NAT, the mapping is one-to-one. For example, internal address 192.168.0.1 maps to 209.86.192.197, address 192.168.0.2 maps to 209.86.192.198, and so on. Figure 9-1 shows a network with static NAT between the internal IP address of an FTP and Web server and a defined public address. Static NAT must be used if you want clients outside your network to access services on your servers.



**Figure 9-1** Static NAT table

The network configuration for NAT is quite simple in a small network because the NAT router will be the default gateway for all clients. In a larger network, the NAT router might be one of many routers. Routers would have to be configured to use the NAT router for Internet communications. NAT should be configured on the border router of a large network. In other words, as shown in Figure 9-1, NAT is needed on the router that connects directly to the ISP.

When the local host 192.168.0.1 communicates with other hosts on the internal network (intranet), NAT will not be involved. For example, when host 192.168.0.1 sends packets to host 192.168.0.2, the packets will not go through the router. This is also true if the local host communicates with other hosts on different networks or subnetworks as long as those destination networks are within the intranet.

## Dynamic NAT

Dynamic NAT means that the NAT router automatically maps a group of valid local IP addresses to a group of Internet IP addresses, as needed. This means that the network administrator is not concerned about which IP address the internal clients use, just that they can get an address. The network administrator also does not have to spend any time defining specific one-to-one mappings between the private and public IP addresses. Any private IP address will automatically be translated to one of the available Internet IP addresses by the NAT router. Addresses for dynamic NAT are pulled out of a predefined pool of public addresses. The administrator must define the pool and then state which internal private addresses can use the pool. Actual NAT configuration is covered later in this chapter.

## Port Address Translation

Port address translation (PAT), also known as **overloading**, is a special form of dynamic NAT. PAT allows multiple internal, private IP addresses to use a single external registered address. To differentiate between the connections, PAT uses multiple public TCP and UDP ports to create unique sockets that map to internal IP addresses. The socket, as you learned earlier, is a combination of the IP address and port. For example, you may communicate with a Web server with IP address 209.120.178.205 over TCP port 80. The socket for that communication is 209.120.178.205:80, representing the IP address and port. When that Web server contacts your hosts, it will call your local IP address and the TCP socket you indicated in your three-way handshake, as you learned in Chapter 3. Now, assume that you have five clients on your LAN, all communicating with different Web servers, but your NAT router only has one valid Internet IP address. How can the NAT router keep track of where the packets should be sent? The simple answer is by using PAT, which maps internal addresses and ports to the same external address but with different communication ports.

Consider the following example while referring to the sample NAT mapping table (see Table 9-2). Assume an organization has five internal clients—Hosts A–E with IP address

| Host                   | Source Local Socket | Source Translated Socket | Destination Remote Socket |
|------------------------|---------------------|--------------------------|---------------------------|
| A                      | 192.168.0.1:1025    | 209.86.192.198:1025      | 209.120.178.205:80        |
| B                      | 192.168.0.2:1027    | 209.86.192.198:1026      | 209.120.178.205:80        |
| C                      | 192.168.0.3:1025    | 209.86.192.198:1027      | 209.120.178.205:80        |
| D                      | 192.168.0.4:1512    | 209.86.192.198:1049      | 64.247.37.221:21          |
| D                      | 192.168.0.4:1513    | 209.86.192.198:1050      | 64.247.37.221:20          |
| E                      | 192.168.0.5:1025    | 209.86.192.198:1029      | 64.46.108.24:80           |
| Internal<br>Web server | 192.168.0.100:80    | 209.86.192.198:80        | 72.13.15.24:1099          |

**Table 9-2** NAT mapping table

ranges 192.168.0.1 to 192.168.0.5. The organization also has a Web server at 192.168.0.100 hosting connections from Internet clients. The NAT server uses **port forwarding** to send connections from external clients to the Web server on the internal network. Hosts A, B, and C are communicating with a Web server that has the address 209.120.178.205 over port 80, which is socket 209.120.178.205:80. Host D is communicating with an FTP server with IP address 64.247.37.221 over TCP ports 21 and 20. Host E is connected to a Web server at 64.46.108.24. Each internal host had to supply one or more ports when it established communications. The organization only has one Internet IP available: 209.86.192.198.

In Table 9-2, you can see how the NAT router would keep track of these unique, individual connections. The local sockets will always be unique because the local hosts have unique IP addresses, even though they may end up using similar port numbers. Remote sockets may be the same because multiple internal hosts can call the same external host. The only item that the NAT router has to make unique is the translated socket. The NAT router does this by not duplicating a port number for the unique IP addresses that it is configured to use. In the preceding example, the NAT router is configured to use a single IP address, making sure there is no port number duplication in the translated sockets. However, many NAT routers can be configured to use multiple public addresses and would therefore just have to ensure that the translated sockets were unique. For example, if the NAT router had IP addresses 209.86.192.198 and 209.86.192.199 as public addresses, it could use dynamic port 1027 twice: once in socket 209.86.192.198:1027, and again in socket 209.86.192.199:1027.

**Overlapping** Overlapping occurs when the internal network has been incorrectly configured for an IP range that actually exists on the Internet (registered to another entity) or when two companies merge and each company was using the same private IP address range. This problem usually occurs only when uninformed network engineers configure a network using arbitrary addresses. Sometimes the thought is that a connection to the Internet will never be required. In this case, the organization cannot connect directly to the Internet because it has an IP range registered to someone else. This overlapping problem can be solved using NAT because NAT hides the incorrectly configured internal IP scheme. The NAT router must be configured to translate the internal IP addresses to a valid external address or address range. This is really no different than previous forms of NAT except that the organization's internal IP address range actually belongs to someone else. The "someone else" just does not know about it because those addresses are never exposed to the Internet, thanks to NAT. Most companies do not run into this problem because their network engineers and designers know to use one of the private IP address ranges (10.x.x.x, 172.16.x.x–172.31.x.x, and 192.168.x.x.) when configuring a private internal TCP/IP network.

## Configuring Network Address Translation

You can configure NAT as static NAT, dynamic NAT, or PAT. These three methods are described in the following sections.

### Configuring Static NAT

As mentioned previously, static NAT is a one-to-one mapping of private IP addresses to public IP addresses. Configuring static NAT is a two-step process:

- Define the static mapping between the inside address and the outside address.
- Define the NAT router's interfaces as inside or outside.

The static mapping is defined with the following command:

```
ip nat inside source static [inside ip] [outside ip]
```

In the example network shown in Figure 9-1, the commands to map the Web server's internal IP to the public IP address 209.86.192.197 would be:

```
RouterA(config)#ip nat inside source static 192.168.0.1  
209.86.192.197
```

The only other necessary commands are the definition of interfaces as either inside or outside. In this example, the private addresses are located on F0/0 and the public addresses on Serial 0/1. So, F0/0 must be defined as inside and Serial 0/1 as outside. The syntax for identifying interfaces as inside or outside is:

```
ip nat [inside | outside]
```

The commands to correctly identify the interface for the network in Figure 9-1 are as follows:

```
RouterA(config)#int f0/0  
RouterA(config-if)#ip nat inside  
RouterA(config-if)#int serial 0/1  
RouterA(config-if)ip nat outside
```

After these commands are configured, the NAT router has a static one-to-one mapping of 192.168.0.1 to 209.86.192.197. The `show ip nat translations` command will now display the static NAT mapping.

## Configuring Dynamic NAT

Configuring dynamic NAT is a more involved process than setting up static NAT. Still, it can be broken down into four easy-to-remember steps:

- Configure a standard access control list to define what internal traffic will be translated.
- Define a pool of addresses to be used for dynamic NAT allocation.
- Link the access list to the NAT pool.
- Define interfaces as either inside or outside.



This section shows only the syntax necessary to configure a standard access list for use with NAT. The entire definition and syntax for access lists are presented in Chapter 10.

**NOTE**

To define the standard access list, you must use the following syntax:

```
RouterA(config)#access-list [1-99] permit [inside IP network(s)]  
[wildcard mask]
```

Continuing to use Figure 9-1 as an example, assume that the network administrator adds 10 hosts to the network and wants to use dynamic NAT to support them. The access list to allow those 10 clients (and any others who are not defined by static NAT) to use NAT is:

```
RouterA(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

The administrator also obtains the public address range of 209.86.192.200 to 209.86.192.240 for use as his dynamic NAT pool. The second step defines the NAT pool. The syntax for this command is:

```
ip nat pool [pool name] [start ip] [end ip] netmask [netmask]
```

Because the administrator has a range of addresses to use, the pool can be defined as follows:

```
RouterA(config)#ip nat pool PoolExample 209.86.192.200  
209.86.192.240 netmask 255.255.255.0
```

The pool must then be linked to the access list. The syntax for the command is:

```
ip nat inside source list [access list number] pool [pool name]
```

The command necessary to link the access list and NAT pool in our example is as follows:

```
RouterA(config)#ip nat inside source list 1 pool PoolExample
```

Two very important items must match in this command. First, the access list number you place in the command must match the list number you created in the first step. Second, the pool name must be an exact match for the pool you create. Cisco routers are case sensitive, so placing `poolexample` instead of `PoolExample` in the command would result in NAT not functioning correctly. This command states that all 192.168.0.0 internal IP addresses (as defined in access list 1) must be translated to the addresses found in `pool`, `PoolExample`: 209.86.192.200-209.86.192.240.

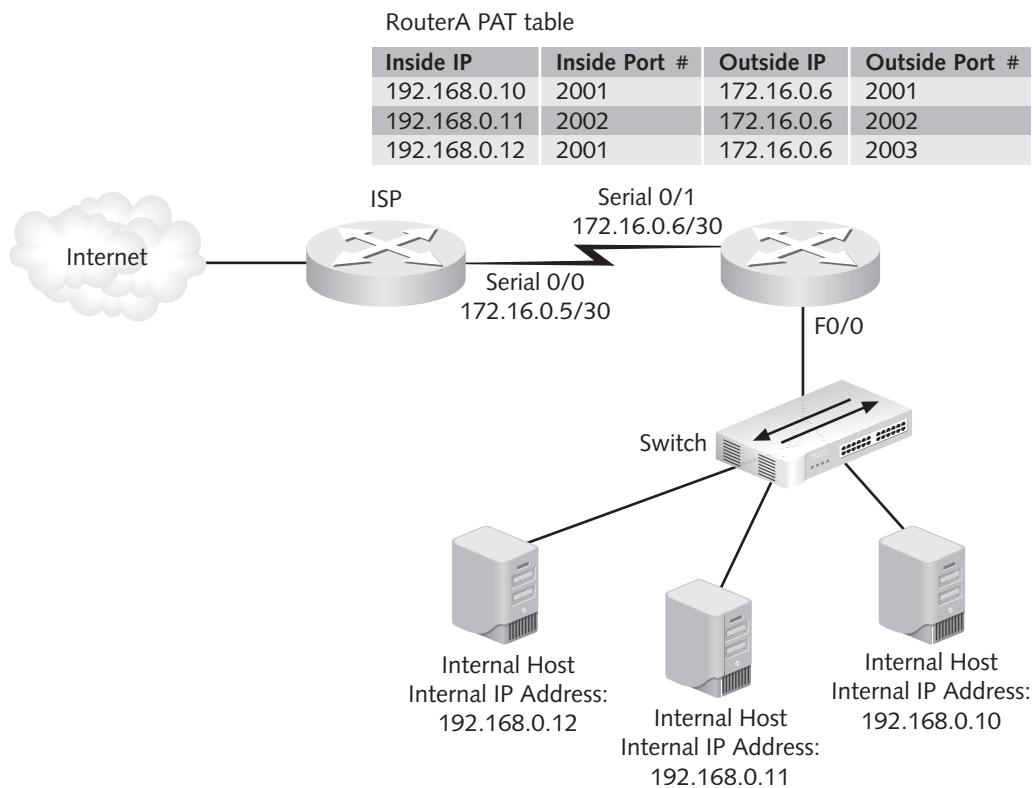
Finally, you must define the interfaces as either inside or outside. These commands are exactly the same as those shown in the static NAT example:

```
RouterA(config)#int f0/0  
RouterA(config-if)#ip nat inside  
RouterA(config-if)#int serial 0/1  
RouterA(config-if) ip nat outside
```

**Configuring Port Address Translation** On smaller networks, the ISP may be unwilling to provide multiple IP addresses to be used for NAT, or the company may not want to pay for additional IP addresses. When these situations occur, you can configure port address translation to allow the IP address of a single outside interface to be used for translation. Figure 9-2 shows a network where the single outside IP address that is assigned to Serial 0/1, 172.16.0.6/30 is also used for PAT. As the clients on the inside attempt to reach the Internet via the ISP, the internal source IP and source port are translated to the external IP address and an external source port. The PAT router attempts to use the same external source port as the original inside port number. The example in Figure 9-2 shows this occurring with the first two PAT table entries. If, however, the original inside source port number is already in use, as is the case in the third entry in the table, the PAT router will use the next unassigned outside port number.

Configuring PAT is a three-step process:

- Configure a standard access list to define what internal traffic will be translated.
- Link the access list to the interface to be used for PAT.
- Define interfaces as either inside or outside.



**Figure 9-2** Port address translation example

In the example from Figure 9-2, a standard access list must be configured that permits 192.168.0.0/24 networks to be translated. Then, this list must be linked to interface serial 0/1. Finally, Serial 0/1 must be defined as outside and F0/0 as inside. The commands to accomplish all of these tasks are:

```

RouterA(config)#access-list 1 permit 192.168.0.0 0.0.0.255
RouterA(config)#ip nat inside source list 1 interface
serial 0/1 overload
RouterA(config)#interface serial 0/1
RouterA(config-if)#ip nat outside
RouterA(config-if)#interface f0/0
RouterA(config-if)ip nat inside

```

## Domain Name Service

Most people prefer to use names, not IP addresses, when communicating with network devices. That is why Domain Name Service (DNS) is such a popular and important naming service. Based on the client/server model, DNS translates names into IP addresses. Without this capability, we would have to know the IP address of every host with which we wanted to communicate. In Chapter 6, you learned that you could use the `ip host` command to provide this name resolution on a Cisco router by typing in the command with the mapping for every

device which might need a name. This static naming method is much too time-consuming to implement on large networks. While you may want to use the `ip host` command to configure a few IP-to-name mappings, it is easier to configure your router to point to a DNS server somewhere on the network. Then, whenever you want to Telnet to or ping a device, you can simply use the name in the command instead of the IP address.

By default, a Cisco router will try several times to find an IP address for a name if you enter one. This automatic translation is called a **lookup**; if no DNS server has been configured, the router will broadcast for the information. Some people find this process annoying; if you make a typo while entering a command, you have to wait while the router attempts to look up an IP address that matches your error. Figure 9-3 displays the router output when `SwitchA` is entered as the command. The router thinks this is a Telnet attempt and tries to find the IP address for `SwitchA` by broadcasting for a domain name server. The router tries three times and then gives up. If you are prone to typing errors, you may want to use the `ip host` command to statically configure the name table on the router. Then, you could turn off the lookup feature by using the `no ip domain-lookup` command.

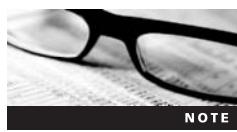
```
RouterA#SwitchA
Translating "SwitchA"...domain server (255.255.255.255)

Translating "SwitchA"...domain server (255.255.255.255)
(255.255.255.255)
Translating "SwitchA"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
```

**Figure 9-3** Output with no name server configured

9

**Configuring DNS Lookup** As previously mentioned, if you have a DNS server on your network, you can configure it on the router. From that point on, all name-to-IP translation requests that are not provided by a static IP host configuration will be forwarded to the DNS server. The command to configure a DNS lookup on a Cisco router is `ip name-server`. Figure 9-4 illustrates the configuration of a name server and the subsequent lookup of `SwitchA`. The `ip domain-lookup` command enables DNS if it has previously been disabled. The IP name-server `10.0.0.3` points the router to the DNS server on the network. The server's IP address is `10.0.0.3`. The `ip domain-name` command is optional, but provides a domain suffix for the names. In this example, the suffix is `cannon.com`. Just as before, when `SwitchA` is entered on the command line, the router thinks this is a Telnet attempt. This time, however, the router asks the DNS server at `10.0.0.3` for help and it resolves `SwitchA`'s name to IP address `10.0.0.2`. The connection is opened and the router operator is Telnetted to `SwitchA`.



Windows Internet Name Service (WINS) servers are also supported by Cisco routers.

NOTE

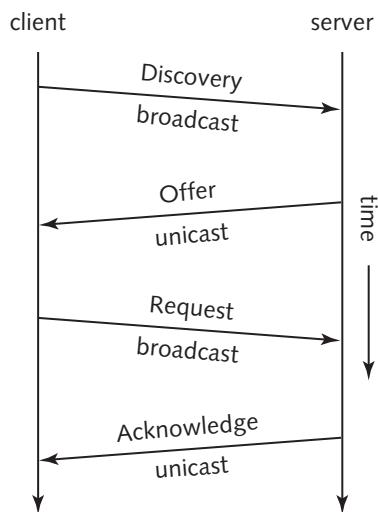
```
RouterA(config)#ip domain-lookup
RouterA(config)#ip name-server 10.0.0.3
RouterA(config)#ip domain-name cannon.com
RouterA#SwitchA
Trying SwitchA (10.0.0.2)... Open
SwitchA>
```

**Figure 9-4** Output when name server is configured

# Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) provides IP configuration information to hosts on bootup. This functionality is much like that provided by older protocols RARP and BOOTP. But unlike DHCP servers, RARP and BOOTP servers issue IP configuration information based on a host's MAC address and require manual preconfiguration for each host. In addition, RARP servers can provide only limited information and can serve only a single LAN. Unlike its predecessors, DHCP is a truly dynamic way to configure IP hosts. In addition to the IP address itself, DHCP servers can provide other parameters, such as the WINS and DNS server addresses, and the default gateway address.

DHCP manages addressing by leasing the IP information to the hosts. This leasing allows the information to be recovered when not in use and reallocated when needed. When hosts are configured to use DHCP, they broadcast a **DHCP DISCOVER** message on the network. DHCP servers that hear the broadcast will send a unicast **DHCP OFFER** message back to the host. Because a network can have more than one DHCP server, the host may receive more than one offer. In this case, the host broadcasts a **DHCP REQUEST** to inform the other DHCP servers that the host has chosen a configuration from a particular server. Finally, the chosen DHCP server sends a unicast acknowledgment (**DHCP ACK**) to the host. This DHCP process is illustrated in Figure 9-5.



**Figure 9-5** DHCP process

You can configure your Cisco router to be a DHCP server. The router can also be configured to forward the request to other DHCP servers if it cannot satisfy a DHCP request. This forwarding of a DHCP request is known as a **DHCP relay**. An advantage of using the router as the DHCP server is that you can configure multiple subnets on the same device. That means that if parameters change in the future, you only need to reconfigure one device.

**Configuring the Router to Be a DHCP Server** The first step in configuring DHCP is to enable the service. This is usually unnecessary because DHCP is enabled by default in the Cisco IOS. If you want to make sure it is enabled, use the `service dhcp` command at the global configuration mode prompt. Cisco's DHCP server implementation prefers to save

the IP configuration parameters it has sent to a particular host. These are called bindings. If you are going to use this feature, you will need a place to store the DHCP bindings database. Typically, an FTP or TFTP server is used for this function. The following command configures the router to store the database on the TFTP server running on host 10.0.0.3. The database filename in this example is dhcp-file.

```
RouterA(config)# ip dhcp database tftp://10.0.0.3/dhcp-file
```

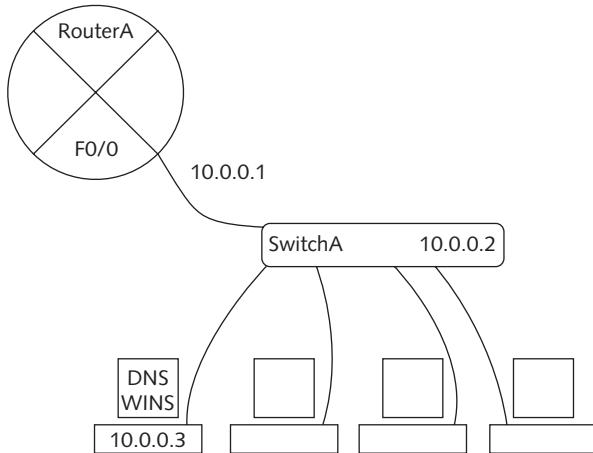
If you choose not to use a server to save the DHCP bindings, you will need to disable the recording of address conflicts on the router. The command to disable this logging is:

```
RouterA(config)# no ip dhcp conflict logging
```

After you complete these routine steps, you can begin the actual DHCP configuration. This configuration involves the same parameters used when configuring DHCP on a server rather than on a router. You will need to complete the following steps:

- Define the pool of addresses.
- Configure any optional IP configuration parameters.
- Exclude any statically configured addresses.

The optional configuration parameters usually include the default-gateway, DNS and WINS server addresses, and a domain name. Figure 9-6 illustrates a sample DHCP configuration for the network shown. In this example, the name of the pool of addresses is RouterA.



```

RouterA>en
RouterA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#ip dhcp pool RouterA
RouterA(dhcp-config)#network 10.0.0.0 255.255.255.0
RouterA(dhcp-config)#default-router 10.0.0.1
RouterA(dhcp-config)#domain-name cannon
RouterA(dhcp-config)#dns-server 10.0.0.3
RouterA(dhcp-config)#netbios-name-server 10.0.0.3
RouterA(dhcp-config)#ip dhcp excluded-address 10.0.0.1 10.0.0.3
RouterA(config)#^Z
RouterA#
  
```

**Figure 9-6** DHCP service on RouterA

The addresses are defined as the valid IP addresses on network 10.0.0.0 using a mask /24 mask. This defines the range of valid IP addresses to be distributed as 10.0.0.1 to 10.0.0.254. The hosts also receive additional optional information. This includes the default gateway and the domain name cannon as well as pointers to the DNS and WINS servers, both at address 10.0.0.3. Finally, the IP address range 10.0.0.1 to 10.0.0.3 is excluded from the pool because 10.0.0.1 was statically assigned to the RouterA interface, 10.0.0.2 was configured on SwitchA, and 10.0.0.3 is the DNS and WINS server address.

**Monitoring DHCP** The best way to check the bindings is to execute the `show ip dhcp binding` command on the router. Figure 9-7 shows the output from this command. In this example, the only IP address configuration assigned is for the 10.0.0.4 address. This address as well as the other optional information has been leased to the host with the MAC address 0100.e0b8.cbff. For information on the specific DHCP address pool, use the `show ip dhcp pool` command, as shown in Figure 9-8. Notice there are 254 total addresses in the pool and that only one from the pool has been assigned. The previous `show ip dhcp binding` command output revealed that 10.0.0.4 is the assigned address. Therefore, the next available address is 10.0.0.5.

```
RouterA#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/          Lease expiration      Type
10.0.0.4        0100.e0b8.cbff    Mar 02 1993 12:21 AM  Automatic
```

**Figure 9-7** Output from the `show ip dhcp binding` command

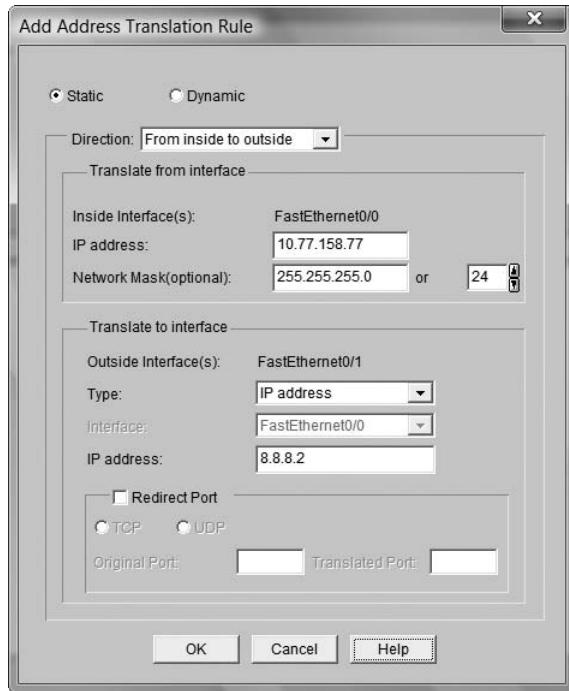
```
RouterA#show ip dhcp pool
Pool RouterA :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                 : 254
  Leased addresses                : 1
  Pending event                   : none
  1 subnet is currently in the pool :
    Current index           IP address range          Leased addresses
    10.0.0.5                10.0.0.1 - 10.0.0.254      1
```

**Figure 9-8** Output from the `show ip dhcp pool` command

## Security Device Manager

In Chapter 6, you were introduced to Cisco's new Security Device Manager (SDM), which is a Web-based tool for advanced configuration on Cisco routers. In addition to advanced security features, SDM can be used to configure the NAT, DNS, and DHCP services discussed in this chapter. It is important to note that network administrators typically do not use SDM to configure these services as they are relatively easy to configure using the command-line interface. However, since SDM is now a part of the Cisco CCNA exam, SDM examples and labs for these services are included in this book.

**Using SDM to Configure NAT** When you launch the SDM program, you see the Home tab. To see all of the parameters that can be configured, click the Configure button. NAT is one of the options displayed. Once you click the NAT button, you will be able to edit the current NAT configuration (if one exists) and/or configure static and dynamic NAT as well as PAT. Figure 9-9 displays the Add Address Translation Rule dialog box for the NAT section of SDM. In this example, Static NAT has been selected. The Direction box displays From inside to outside. This is the default setting and implies that the network administrator wants to translate inside private addresses to outside public ones. The inside interface is Fast Ethernet 0/0, and the address to be translated is 10.77.158.77/24. This private address will be translated to address 8.8.8.2 /24. This is a static mapping, which means that the host at 10.77.158.77 will always indicate the address 8.8.8.2 when its traffic is outside of the private network.

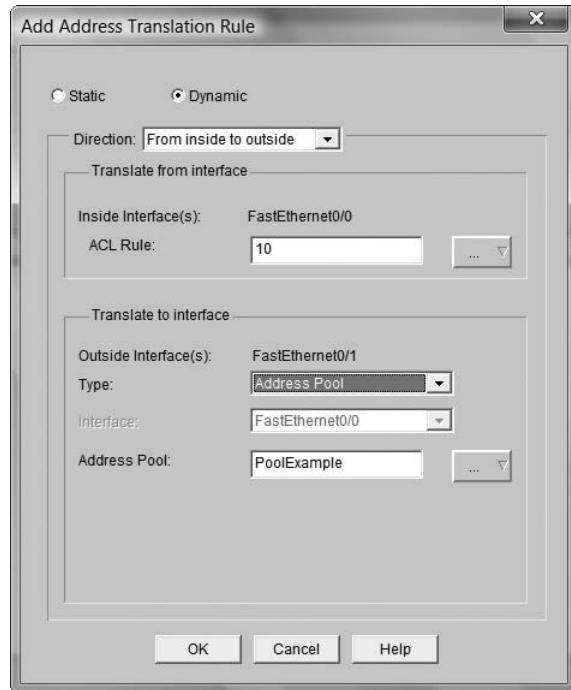


**Figure 9-9** Using SDM to configure static NAT

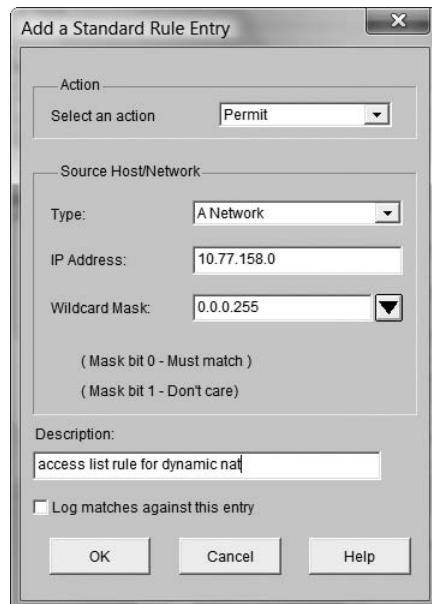
In the case of dynamic NAT, an access list must be created to define the inside addresses, and a pool of addresses must be created to define the outside addresses. This inside list and outside pool are then linked. Figure 9-10 illustrates a dynamic NAT example. Notice that a reference to access-list 10 is displayed for the inside interface, which is Fast Ethernet 0/0. This access list was created by clicking the button to the right of the list number and navigating to the dialog box shown in Figure 9-11. Notice in this figure that the list is a permit list and defines the inside addresses as all valid addresses defined by 10.77.158.0. The mask used in access lists is a wild-card mask, also known as an inverse mask. Compared to masks you have used previously, an inverse mask looks backwards or flipped. You will learn more about access lists and their associated masks in Chapter 10. Figure 9-10 defines the outside interface as Fast Ethernet 0/1 and indicates that the outside addresses are defined by a pool named PoolExample. The Add Address

## 250 Chapter 9 Network Services

Translation Rule dialog box shown in Figure 9-10 effectively links the inside addresses defined by the access list to the outside public addresses defined by the pool.

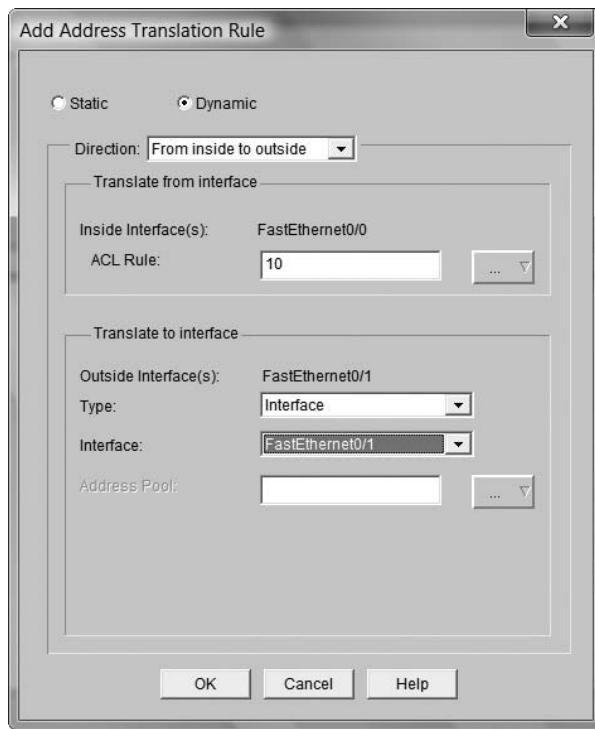


**Figure 9-10** Using SDM to create an access list for dynamic NAT



**Figure 9-11** Using SDM to create an access list for dynamic NAT

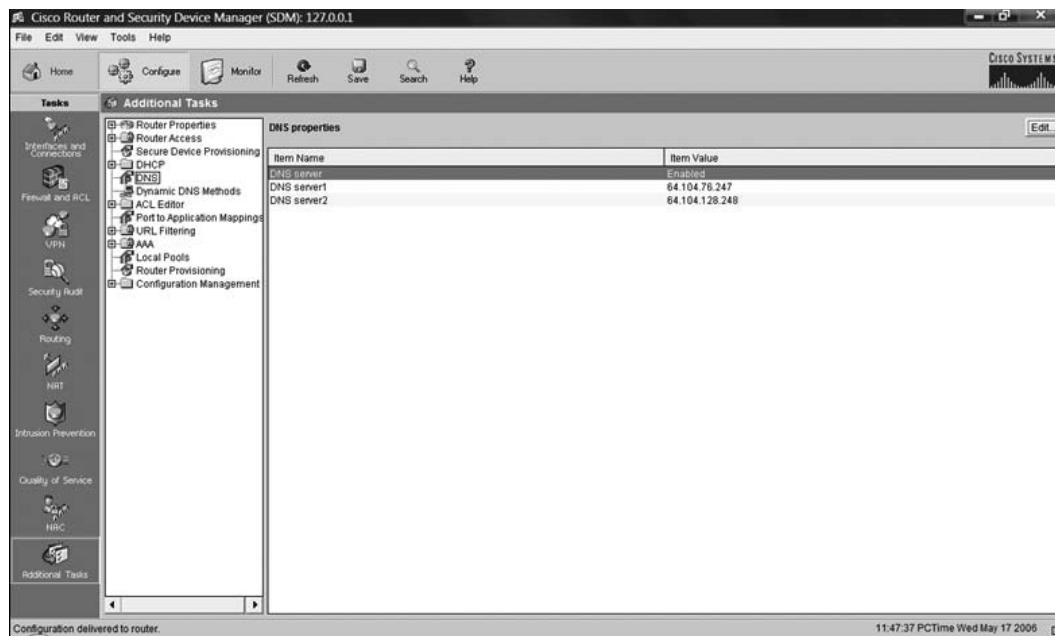
The only difference between using SDM to configure dynamic NAT versus PAT is that in the Add Address Translation Rule dialog box, you choose to translate to a single outside interface rather than a pool of addresses. Figure 9-12 illustrates an example of PAT. Notice that Dynamic is selected, because PAT is really just a type of dynamic NAT. The access list rule that defines the inside traffic is still used in the same way. But, since PAT translates all inside private addresses to a single outside address, the Translate to interface Type: selected is Interface and the Fast Ethernet 0/1 interface address is selected as the one to use for all translations. This use of a single outside address means the router must use port numbers to keep track of the connections.



**Figure 9-12** Using SDM to configure PAT

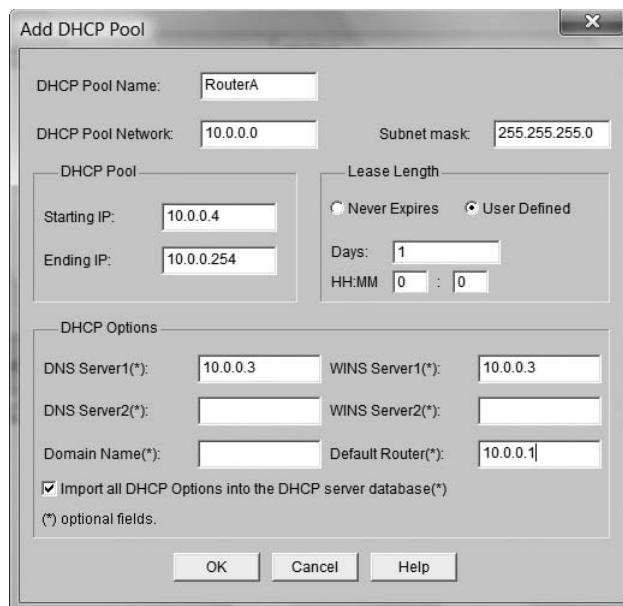
**Using SDM to Configure DNS** As previously discussed in this chapter, you can point your router to a DNS server for name resolution simply by configuring the `ip name-server` command, which would be the most efficient way to do it. However, if you are planning to use SDM for more than just advanced configurations, you can configure the DNS server pointer(s) as well. You access this area of the SDM by clicking on the Additional Tasks button in the lower left pane. When the Additional Tasks pane opens, click DNS. Figure 9-13 displays the DNS area in the SDM. If you enable DNS, you can configure two DNS server addresses. In this example, the router will look first to 64.104.76.247 for name resolution queries and then to 64.104.128.248 if the first DNS server fails to respond.

## 252 Chapter 9 Network Services



**Figure 9-13** Using SDM to point to DNS servers on the network

**Using SDM to Configure DHCP** You access the DHCP configuration area using the Additional Tasks button, just as you access DNS. Figure 9-14 displays the Add DHCP Pool dialog box. In this example, the name of the pool of addresses is RouterA. The valid IP addresses that will be leased by the router are defined by the 10.0.0.0 network with a /24 subnet mask.



**Figure 9-14** Using SDM to configure DHCP

The starting IP address is 10.0.0.4 and the last address to be leased is the last valid address on the network, which is 10.0.0.254. This effectively excludes addresses 10.0.0.1, 10.0.0.2, and 10.0.0.3, presumably because they are being used by other devices. You can change the default lease time of 1 day. Finally, you can point to two DNS servers, two WINS servers, and the default router. The default router will be defined by the interface on the router used to reach networks outside of the LAN. This is actually the default gateway and will be configured as such by the clients.

## Chapter Summary

- NAT is a technology that allows organizations to map valid external addresses to private or unregistered internal addresses. This allows organizations to maintain a separation between the Internet and the intranet (internal network) while still providing access to the Internet.
- Organizations can use NAT to allow many more people to access the Internet by sharing one or more valid public addresses.
- Static NAT involves mapping each internal IP address to a separately defined outside IP address. The mapping never changes.
- Dynamic NAT involves the mapping of inside addresses to a smaller pool of outside addresses. The allocation is done dynamically, so the mapping may change.
- PAT allows an organization to map more than one internal private IP address to a single outside IP address by using port numbers to identify the separate connections. This NAT method conserves public IP address space.
- The Domain Name Service (DNS) is used to provide an IP address-to-name mapping so that users can refer to hosts by name rather than address.
- The Dynamic Host Configuration Protocol provides IP configuration information such as address, subnet mask, default-gateway, DNS and WINS server location, and domain name to hosts on the network. When the hosts boot up, they broadcast for this information and a DHCP server or router on the network provides it. In cases where there is no DHCP server, the router can be configured to relay the request to another network.
- SDM is a Web-enabled Cisco product that allows advanced router configuration without using the command-line interface. SDM can be used to configure NAT, DNS, and DHCP on the router in lieu of using the command-line interface.

9

## Key Terms

**bindings** IP to MAC address mappings that are found in the DHCP database.

**DHCP ACK** A unicast acknowledgement sent by the DHCP server to the client.

**DHCP DISCOVER** A packet that is broadcast on bootup by a client when that client has no IP information or incomplete IP information.

**DHCP OFFER** A unicast reply by a DHCP server to a client that has broadcast a DHCP DISCOVER packet.

**DHCP relay** If no DHCP service is found on the network, the router can be configured to relay the request to a DHCP server on a different network.

**DHCP REQUEST** A formal request for IP configuration information intended for a specific DHCP server but broadcast so that all servers can see the association.

**DNS** Domain Name Services provides name-to-IP address translation so that users can use names instead of addresses in commands.

**DHCP** Dynamic Host Configuration Protocol provides IP configuration information to clients when they bootup.

**dynamic NAT** A type of network address translation in which the valid external IP addresses to be mapped to internal addresses are floating or not fixed. The NAT router can then dynamically assign any of the available external addresses to any of the hosts on the internal network.

**lookup** The process of retrieving an IP address for a given name and providing it to the client that requested it.

**network address translation (NAT)** A method for using a router to separate an internal network from an external network (usually the Internet), which is defined in RFC 3022. Internal hosts with private or unregistered IP addresses can effectively use one or more public registered IP addresses to communicate with external systems.

**overlapping** When an organization wants to connect to the Internet, but its internal addressing scheme is registered to another entity. Instead of renumbering the internal network, the organization uses NAT to translate its internal addressing scheme to the addresses that it was assigned by the ISP.

**overloading** A type of NAT that allows multiple internal hosts to use one or more external IP addresses. The NAT router uses a table to keep track of the IP addresses and ports of each host, dynamically mapping each internal socket to a valid external socket.

**port address translation (PAT)** A process used in overloading that allows multiple internal, unregistered IP addresses to use a single external registered address.

**port forwarding** A method for sending packets from an external host system through a firewall or NAT router to an internal device. In this way, the internal device IP address is hidden from the external network, yet the internal device can still service requests from the external network.

**static NAT** A type of network address translation (NAT) that allows for a one-to-one mapping of internal to external addresses. One internal address is mapped to one specific external address.

## Review Questions

1. What is used on routers to hide intranet IP addresses from the Internet?
  - a. PAP
  - b. CHAP
  - c. NAT
  - d. FRAT
  
2. Which flavor of NAT maps multiple internal IP addresses to a single external address?
  - a. PAP
  - b. CHAP

- c. NAT
  - d. PAT
3. How does overlapping occur?
- a. The network administrator does not plan for Internet connectivity.
  - b. The network administrator uses registered IP addresses without getting permission.
  - c. Both a and b
  - d. None of the above
4. When would it be most appropriate to configure static NAT?
- a. when you want to guarantee that a particular device is always associated with the same public IP address
  - b. when you do not care what public IP address is used by a device
  - c. when the inside-to-outside IP address mapping is not important
  - d. when you want every inside IP address to translate to a single public address
5. What is the purpose of the `ip nat inside` command?
- a. to tell the router to use static NAT
  - b. to tell the router to use dynamic NAT
  - c. to tell the router to enter NAT configuration mode
  - d. to tell the router that the current interface is to be considered the inside interface
6. The DNS service is required in order to browse the web. True or False?
7. Which of the following commands statically maps a name to an IP address?
- a. `ip name-server`
  - b. `ip host`
  - c. `ip address`
  - d. `ip name`
8. Which of the following commands disables the default DNS lookup function on a Cisco router?
- a. `no ip domain-lookup`
  - b. `no lookup`
  - c. `no ip-lookup`
  - d. `no ip domain-name lookup`
9. Which of the following commands directs the router to a DNS server for IP-to-name resolution?
- a. `ip host`
  - b. `ip address`
  - c. `ip name`
  - d. `ip name-server`

**256** Chapter 9 Network Services

10. If you have disabled the lookup function on your Cisco router, you will have to re-enable it if you want to use a DNS server to resolve names on your router. True or False?
11. Which of the following is *not* a DHCP packet type?
  - a. DHCP OFFER
  - b. DHCP SYN
  - c. DHCP REQUEST
  - d. DHCP ACK
  - e. DHCP DISCOVER
12. What is the purpose of the service dhcp command?
  - a. starts monitoring the DHCP service
  - b. turns off DHCP debugging
  - c. enables DHCP
  - d. disables DHCP
13. Where is the DHCP database typically stored?
  - a. on the router
  - b. on a server
  - c. on a CD or DVD
  - d. The database is not stored.
14. Which of the following are optional when configuring your router to be a DHCP server? (Choose all that apply.)
  - a. default gateway
  - b. IP address
  - c. subnet mask
  - d. DNS server address
  - e. WINS server address
  - f. domain name
15. Which of the following monitoring commands displays any IP addresses leased by the DHCP server and the corresponding MAC address of the host?
  - a. show ip dhcp pool
  - b. show dhcp
  - c. show ip dhcp binding
  - d. show binding
16. Which of the following monitoring commands displays DHCP pool specific information?
  - a. show ip dhcp pool
  - b. show dhcp
  - c. show ip dhcp binding
  - d. show binding

17. Cisco's SDM can be used to configure network services such as DNS and DHCP. True or False?
18. What is the difference between configuring dynamic NAT and PAT on a Cisco router using the SDM?
  - a. The access list that defines the inside addresses will be different.
  - b. You will select overload instead of dynamic in the Add Address Translation Rule dialog box.
  - c. The direction selected for PAT will be From outside to inside rather than From inside to outside.
  - d. You will translate to an interface rather than to a pool of addresses.
19. It is easier to configure a pointer to a DNS server using the command-line interface rather than the SDM. True or False?
20. What is another name for a wildcard mask?
  - a. inverse mask
  - b. obtuse mask
  - c. backwards mask
  - d. flip mask

**9**

---

## Case Projects



1. The Americanus Corporation wants to use RFC 1918 addresses on its LAN. They understand that NAT will have to be configured on the router but do not really understand how NAT works. Briefly explain the three types of NAT to them.
2. What are the essential commands when configuring your Cisco router to be a DHCP server? What are some optional commands that you will probably want to configure and why?
3. Explain why IP-to-name resolution is important and list and describe the function of the ip host, ip name-server, and dns-server commands.





# 10

chapter

## Access Lists

**After reading this chapter and completing the exercises, you will be able to:**

- Describe the usage and rules of access lists
- Establish standard IP access lists
- Produce extended IP access lists
- Apply access lists to interfaces
- Monitor and verify access lists
- Create named access lists
- Use Security Device Manager to create standard and extended IP access lists
- Use Security Device Manager to create a router firewall

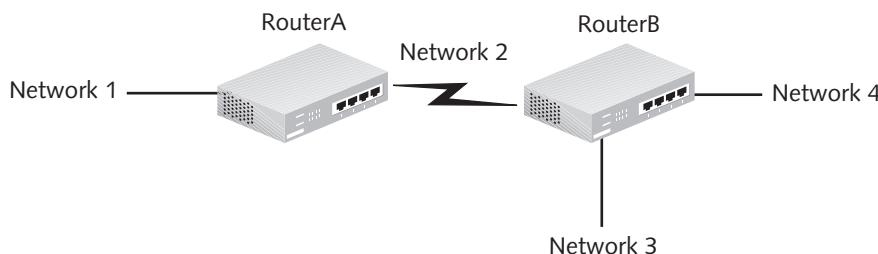
**In this chapter, you will learn how to create and apply access lists to control both traffic flow and network security.** In the process, you will review the use and rules of access lists. The chapter introduces the creation of standard and extended IP access lists and explains how to apply them to router interfaces. This chapter also describes how to monitor and verify access lists, create named access lists, and configure access lists via Security Device Manager.

## Access Lists: Usage and Rules

Smart network engineers pay close attention to network traffic flow and security when they design and manage their networks. Access lists, which are built into the Cisco IOS, solve many problems associated with traffic flow and security. **Access lists** are permit or deny statements that filter traffic based on the source address, destination address, protocol type, and port number of a packet. They are available for IP, IPX, AppleTalk, and many other protocols.

### Access List Usage

You can create a standard access list that examines a packet for the packet's source header information. For instance, RouterA can use an access list to deny access from Network 4 to Network 1; both networks are shown in Figure 10-1. If a packet from Network 4 arrives at the interface where you placed the access list, the router examines the packet and uses the access list to determine if it needs to discard the packet.



**Figure 10-1** Sample network

With the following conceptual syntax, you create the standard access list to block access from Network 4 to Network 1:

- access-list 1 deny Network 4
- access-list 1 permit any

The access list ends with an **implicit deny any statement**, which blocks all packets that do not meet the requirements of the access list. This statement exists even though it is not shown as part of the access list. Some administrators, in order to avoid confusion, configure the **deny any** statement to make it more obvious, but this is unnecessary. Access list 1, if applied to the interface of RouterA connected to Network 1, blocks only the traffic coming from Network 4 to Network 1. If you wanted to deny traffic from Network 3 and Network 4, the conceptual access list syntax would look like this:

```

access-list 1 deny Network 3
access-list 1 deny Network 4
access-list 1 permit any
  
```



The previous access-list statements are not the exact Cisco IOS syntax for the `access list` command. Actual IOS syntax will be covered later in the chapter.

**NOTE**

The final `permit any` statement is necessary because all access lists in the Cisco IOS end with an implicit `deny any`. If you apply the access list to the interface of RouterA that is connected to Network 1, it blocks traffic from Networks 3 and 4, while allowing all other network traffic to access Network 1.

With careful planning, you can create access lists that control which traffic crosses particular links, and which segments of your network will have access to others. In other words, you can control traffic flow and security. Security is enhanced because you can permit or deny particular networks access to parts of your network. In the preceding example, Network 4 may be a student network, and Network 1 may be an administrative network. The first list stops students on Network 4 from accessing any resources in Network 1, the administrative network.



Although access lists can help with network security, they do not take the place of more advanced security measures, such as firewalls. Access lists, combined with dedicated firewalls at the edge of your network, provide the greatest security.

**NOTE**

## Problems with Access Lists

Lack of planning is one of the most common problems associated with access lists. Before you begin configuring access lists on your router, you must plan exactly what needs to be filtered and where it needs to be filtered. Careful planning prior to the configuration of lists can cut down on simple logic mistakes, which commonly occur when you do not think through the effects of your actions.

10

The need to enter the list sequentially into the router also presents problems. You cannot move individual statements once they are entered. When making changes, you must remove the list, using the `no access-list [list number]` command, and then retype the commands. Many network administrators simplify this time-consuming process by creating their access lists in a simple word processor, such as Notepad, and then copying and pasting the access list into the router configuration. Using this method, an administrator can create a perfect access list (free of typos) and then apply the list to any single router or a group of routers. This allows a type-once, use-many scenario that reduces errors and the time necessary to configure a router.

Finally, many new network administrators find themselves in trouble when they telnet into a router and begin applying an access list. Access lists begin working the second they are applied to an interface. It is very possible that many new administrators will find themselves inadvertently blocked from the very router on which they are applying an access list. While this is not a serious problem when the router is in the same building as the administrator, it is a serious problem when the router is in another city and thus physically inaccessible.

Fortunately, the `reload` command can save you from a long car ride or an embarrassing phone call to a local administrator to explain the problem. With the `reload` command, an administrator can schedule the router to reload in a certain number of minutes, hours, or even days. For access list configuration, you probably want to schedule the reload to the granularity of minutes or hours. The syntax for the `reload` command is `reload in [hh: mm]` (reloads in a certain number of hours or minutes) or `reload at hh:mm [month day] / day month`

(reloads at a certain time on a certain date). For example, before modifying or adding access lists to a remote router, an administrator could type the following command:

```
RouterB#reload in 30
```

If an access list locks the administrator out, the router would reload in 30 minutes with a running-config that did not contain the access list that blocked the administrator's access. Note, however, that in this case, the `reload` command will only work if you do not copy the running-config to the startup-config while working with the access lists. If you create and apply the lists and they have the intended results, you can cancel the scheduled reload with the `reload cancel` command.

## Access List Rules

You must follow certain rules when creating standard or extended access lists. For instance, you must create and apply access lists sequentially. Also, as stated previously, access lists always end with an implicit deny.

The following example shows the structure of a standard IP access list. The router applies each line in the order in which you type it into the access list:

```
RouterA(config)#access-list 1 deny 172.22.5.2 0.0.0.0
RouterA(config)#access-list 1 deny 172.22.5.3 0.0.0.0
RouterA(config)# access-list 1 permit any
```

The previous example is a standard IP access list that denies the hosts 172.22.5.2 and 172.22.5.3, while allowing all other traffic. The list is applied sequentially from the top down as the router checks the packets arriving at the interface where this access list is applied, in order to check if the packets match the `permit` and `deny` statements.

In the process of applying access lists, the router first checks an arriving packet to determine if it matches the `deny 172.22.5.2 0.0.0.0` statement. If it does, the router discards the packet. If it does not, the router applies the second statement, `deny 172.22.5.3 0.0.0.0`. If the packet matches the second statement, the router discards the packet. Once again, if the packet does not meet the rules of the first two lines, the router applies the final `permit any` statement, and the packet is forwarded through the interface.

If you want to add another deny line to this list, you can go back into global configuration mode and do so. Because all new lines are added to the end of the list, adding the line

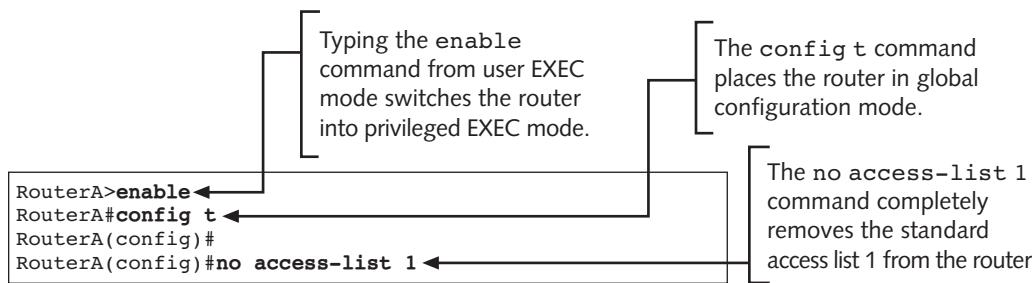
`RouterA(config)# access-list 1 deny 172.22.5.5 0.0.0.0` will produce the following list:

```
access-list 1 deny 172.22.5.2 0.0.0.0
access-list 1 deny 172.22.5.3 0.0.0.0
access-list 1 permit any
access-list 1 deny 172.22.5.5 0.0.0.0
```

The new line is appended to the end of access list 1. The router checks the packet against the first three statements. Once the packet matches one of the statements, the router discards or forwards it based on that match. Because the third statement says that all packets are permitted

and can be forwarded, the existence of the fourth line has no effect; a packet from 172.22.5.5 would be forwarded before it ever reached the `deny 172.22.5.5 0.0.0.0` statement. To fix this problem, you must remove the access list completely and re-create it using the correct sequence.

The `no access-list [list #]` command is used to remove an access list. For example, to remove the preceding list, you enter global configuration mode and type the `no access-list 1` command. Figure 10-2 shows the correct procedure for typing this command.



**Figure 10-2** The `no access-list` command

This command will remove the entire list; you cannot remove a particular line in an access list. As a general rule, the lines with the most potential matches should be first in the list so that packets will not undergo unnecessary processing. You should also avoid unnecessarily long access lists. A very long access list will consume large amounts of CPU processing time and could cause the router to act as a bottleneck on your network.

As previously mentioned, to ease the administrative load associated with access lists, Cisco recommends using a text editor to create them. You can then easily make changes to the list and apply it to the router configuration using copy and paste. You should place a `no access-list [list #]` command as the first line of the text file, which allows you to completely remove an access list from a router. If you do not use this command, the lines of the access list in the text file will be appended to the end of the existing list when you paste it into the configuration.

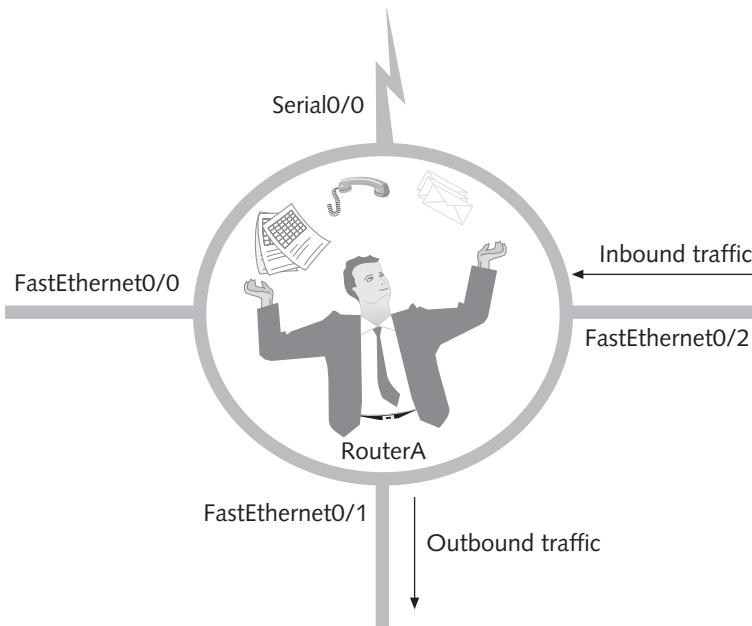
After you create access lists, you must apply them to interfaces so they can begin filtering traffic. You apply a list as either an outgoing or an incoming filter. To determine how to apply the list, you have to look through the eyes of “the man in the router.” Traffic coming in to the man in the router, through any of the interfaces, is considered **inbound** and needs to be filtered using incoming traffic filters, as shown in Figure 10-3.

To apply the access list to an interface, you use the following command:

```
ip access-group 1 in
(The one in this example represents the access list numbered 1.)
```

Once traffic gets to “the man in the router,” he must push it out to one of the interfaces. Access lists to block his outward delivery must be applied as **outbound** filters. The following command sets an outbound access list filter:

```
ip access-group 1 out
(Again, the 1 specifies that you are applying access list 1 to the interface.)
```



**Figure 10-3** The man in the router

The final rule that access lists must follow states that an interface cannot have more than one inbound or outbound list, per protocol, assigned to it. This means that a router can have no more than one inbound IP access list and one outbound IP access list applied at the same time. Multiple lists are allowed only if the lists are different protocols.

In summary, all access lists follow these rules:

- Routers apply lists sequentially in the order in which you type them into the router.
- Routers apply lists to packets sequentially, from the top down, one line at a time.
- Packets are processed only until a match is made, and then they are acted upon based on the access list criteria contained in access list statements.
- Lists always end with an implicit deny. Routers discard any packets that do not match any of the access list statements.
- Access lists must be applied to an interface as either inbound or outbound traffic filters.
- Only one list, per protocol, per direction can be applied to an interface.
- Access lists are effective as soon as they are applied; however, you must use the `copy run start` command to save the list after configuration if you want it to survive a router reload.

Now that you understand the basic rules of access lists, the next section describes standard and extended IP lists.

## Standard IP Access Lists

Standard IP access lists filter network traffic based on the source IP address only. Using a standard IP access list, you can filter traffic by a host IP, subnet, or a network address. To configure standard IP access lists, you must create the list and then apply it to an interface using the following syntax:

```
access-list [list #] [permit/deny] [source address]
[source wildcard mask]
```

The brackets in each command syntax are not part of the command; they group items that are replaced within each specific entry. The following list explains each element of the standard IP access list configuration syntax:

- *[list #]*—Standard IP access lists are represented by a number in the range of 1–99 (in IOS versions 11.2 and greater, they can also be represented by text names).
- *[permit|deny]*—Used to specify the nature of the access list line. It is either a permit or a deny statement.
- *[source address]*—The IP address of the source.
- *[source wildcard mask]*—A **wildcard mask**, or **inverse mask**, applied to determine which bits of the source address are significant.

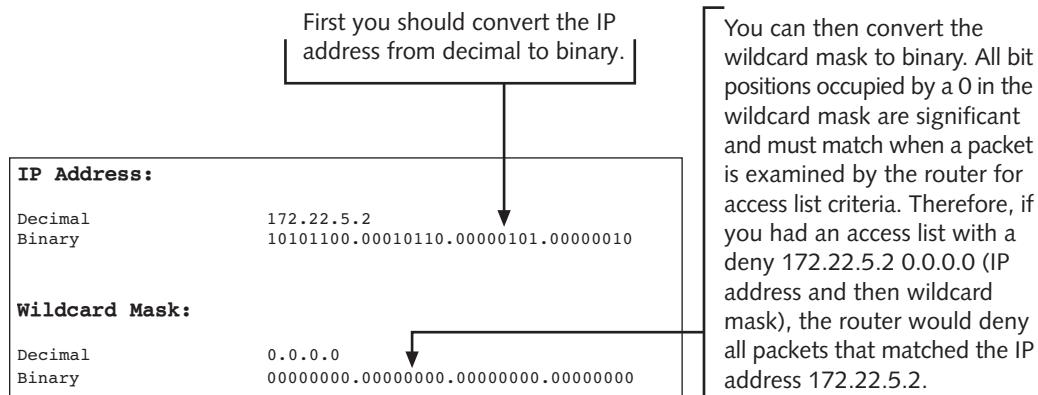
Wildcard masks are one of the most important concepts in IP access lists. Routers use them to determine which bits in an address will be significant. Unlike subnet masks, 0s are placed in bit positions deemed significant, and 1s are placed in positions that are not significant. In other words, where there is a 0 in the mask, the corresponding bit in the incoming packet (either 0 or 1) must match the bit in the IP address in the access list. If there is no match, the packet passes to the next line in the access list. Consider the addresses and wildcard masks shown in Table 10-1.

10

| IP Address | Wildcard Mask | Result                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 172.22.5.2 | 0.0.0.0       | All bit positions must match exactly. Therefore, the access list line will only be applied to host 172.22.5.2. For a match, the incoming packet must have an IP address of exactly 172.22.5.2.                                                                                                                                                                                                                                                 |
| 172.22.5.0 | 0.0.0.255     | Bit positions in the first three octets must match exactly, but the last octet can be any valid number. The access list line will apply to all hosts in the 172.22.5.0 subnet.                                                                                                                                                                                                                                                                 |
| 172.22.1.0 | 0.0.254.255   | The first two octets must match exactly, as must the least significant bit position in the third octet, which in this case is a 1. The last octet can be any valid number. This mask would allow you to permit or deny odd-numbered subnets from the 172.22.0.0 major network because odd subnets will always have a 1 in the final bit position of the third octet. The example assumes a subnet mask of 255.255.255.0 for a Class B network. |

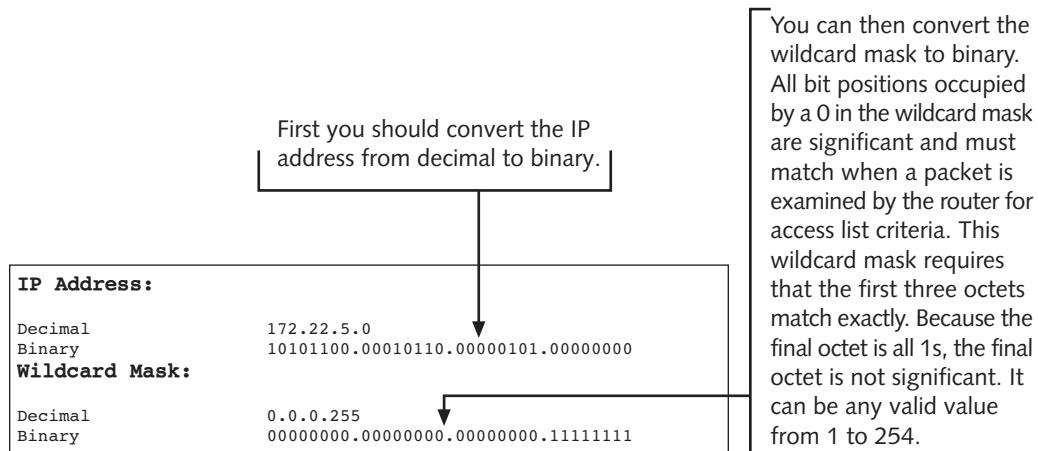
**Table 10-1** Wildcard mask examples

To understand wildcard masking, you may find it helpful to examine the addresses in binary format. Consider the example in Figure 10-4, which shows a wildcard mask that forces the packet to match all four octets of the source address.



**Figure 10-4** Wildcard masking example matching a single host

Because 0s represent significant bits, you can see that in Figure 10-4, a wildcard mask of 0.0.0.0 requires that the source address match exactly. The second example, in Figure 10-5, shows how to permit or deny an entire subnet.



**Figure 10-5** Wildcard masking example matching a complete subnet

Again, recalling that 0s represent significant bits, you see that the first three octets must match. The final octet of the wildcard mask consists of 1s and signifies that the value of the fourth octet is not significant.

Deciphering wildcard masks is relatively easy when an entire octet is either all 0s (zero) or all 1s (255). It is more difficult when some bits in an octet are 0s and some bits are 1s. This mixing of 0s and 1s in an octet is called **partial masking**.

The final example of wildcard masking is a bit more complex and requires examining two IP addresses to fully understand it. Figure 10-6 illustrates the first address, an odd subnet.

This wildcard mask requires that the first two octets and the final bit position of the third octet match the IP address in the access list. The values in the last octet are not significant. Because the final bit positions in the third octet of the IP address in the access list are turned on (set to 1), all packets that the access list will permit or deny must have a 1 in the final bit position of the third octet.

| <b>IP Address:</b>                   |                                     |
|--------------------------------------|-------------------------------------|
| IP address in access list in decimal | 172.22.1.0                          |
| IP address in access list in binary  | 10101100.00010110.00000001.00000000 |
| <b>Wildcard Mask:</b>                |                                     |
| Decimal                              | 0.0.254.255                         |
| Binary                               | 00000000.00000000.11111110.11111111 |

**Figure 10-6** Wildcard masking example using partial masking

In this example, the first two octets must match exactly. Also, the final bit place in the third octet must match; it must be a 1. Therefore, an access list that states `access-list 1 permit 172.22.1.0 0.0.254.255` will allow traffic from any odd-numbered subnet to pass. Even-numbered subnets are blocked because their last bit position in the third octet is a 0.

If you use a source of 172.22.1.0 and a wildcard mask of 0.0.254.255, any packet that the list will act upon must have a 1 in the least significant bit position of the third octet. If a packet with the IP address of 172.22.2.1 is examined by the access list in the previous paragraph, the router ignores it because the least significant bit of the third octet is a 0, not a 1. Figure 10-7 shows why this is true.

This wildcard mask requires that the first two octets and the final bit position of the third octet match the IP address in the access list. The values in the last octet are not significant. Because the final bit position in the third octet of the examined IP address and the IP address in the access list do not match (one is a 0 and the other is a 1), any line in an access list with a `permit 172.22.1.0 0.0.254.255` would not apply to the address 172.22.2.1. In fact, no even subnet could be affected because all even subnets would have a value of 0 in the last bit position of the third octet.

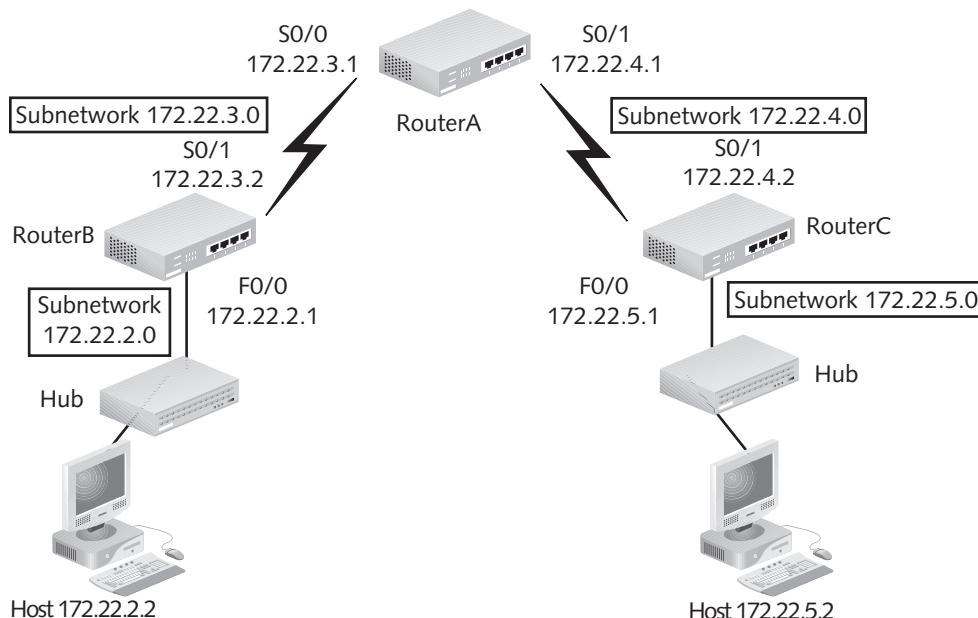
|                                |                                     |
|--------------------------------|-------------------------------------|
| Decimal of examined IP address | 172.22.2.1                          |
| Binary of examined IP address  | 10101100.00010110.00000110.00000001 |
| IP address in access list:     | 10101100.00010110.00000001.00000000 |
| Wildcard mask:                 | 00000000.00000000.11111110.11111111 |

**Figure 10-7** Wildcard masking example without match

Because the least significant bit positions do not match, any address within the subnet 172.22.2.0 is out of the required range of the access list and is thus discarded (or ignored, depending on the function of the access list).

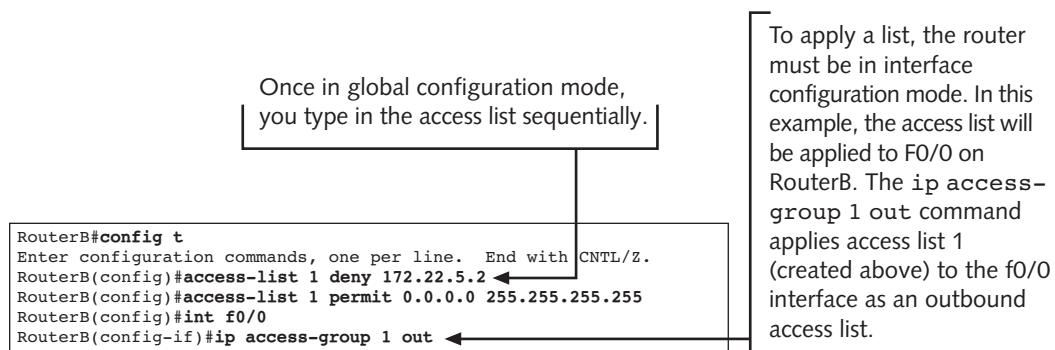
## Standard IP Access List Examples

Standard IP access lists permit or deny packets based only on the source address. These addresses can be a single host address, a subnet address, or a full network address. Consider the IP network in Figure 10-8.



**Figure 10-8** Sample IP network

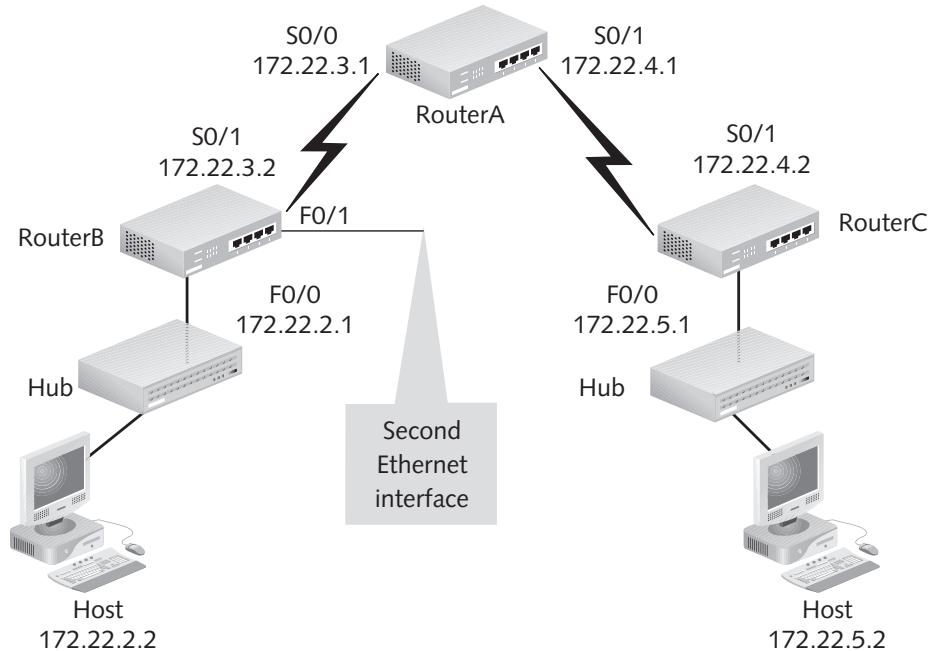
Using the sample network in Figure 10-8, you can create a standard IP access list that blocks host 172.22.5.2 from accessing subnet 172.22.2.0. Figure 10-9 shows the commands you would enter on RouterB to accomplish this task.



**Figure 10-9** Creating a standard IP access list

In global configuration mode, you add each line of the access list sequentially and then apply the list to an interface to cause it to take effect. In this example, the deny statement does not include a source wildcard mask because the default mask for standard IP access lists is 0.0.0.0, which is the exact mask needed in the example. It is also possible to replace the 0.0.0.0 255.255.255.255 entry, which represents all hosts and all networks, with the **any** keyword. Once the list is applied to RouterB's FastEthernet0/0 interface, packets from 172.22.5.2 will be blocked from going out the interface.

Correct placement of a list is imperative. If the list were placed on RouterB's S0/1 interface as an inbound list, it would work with the sample network. However, if RouterB had another Fast Ethernet interface, as shown in Figure 10-10, placing the access list on S0/1 would inadvertently block traffic to the second Fast Ethernet interface, F0/1.



**Figure 10-10** Sample IP network with two Ethernet interfaces on RouterB

Applying the previous list as an inbound access list on S0/1 blocks all traffic from host 172.22.5.2 to other ports on RouterB. Because you only want to block access to subnet 172.22.2.0, this is not the correct way to apply the list; you should apply the standard IP access list as close to the destination as possible. Otherwise, you will inadvertently block access to portions of your network.

To view the access lists defined on your router, use the `show access-lists` command. Because this is an IP access list, you could also use the `show ip access-lists` command. Figure 10-11 shows the correct procedures to type both commands.

RouterB has one standard IP access list defined on it. To view which interfaces have IP access lists set, use the `show ip interface` command. Your router will return a list of all interfaces and details about which access lists are applied, inbound and outbound. For the sake of brevity, only FastEthernet0/0 is displayed in Figure 10-12.

## 270 Chapter 10 Access Lists

```

RouterB#show access-lists
Standard IP access list 1
deny 172.22.5.2
permit any
RouterB#

RouterB#show ip access-lists
Standard IP access list 1
deny 172.22.5.2
permit any
  
```

The `show access-lists` command displays all access lists currently configured on the router. In this example, a single standard IP access list is on the router. If other types of access lists, such as IPX standard or extended, were on the router, this command would display them.

The `show ip access-lists` command displays all IP access lists currently configured on the router.

**Figure 10-11** The `show access-lists` and `show ip access-lists` commands

```

RouterB#show ip interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 172.22.2.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Multicast reserved groups joined: 224.0.0.9
  Outgoing access list is 1
  Inbound access list is not set
  Proxy ARP is enabled
  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 disabled
  IP multicast fast switching is enabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  --More--
  
```

The `show ip interface` command shows what IP access lists are applied on an interface.

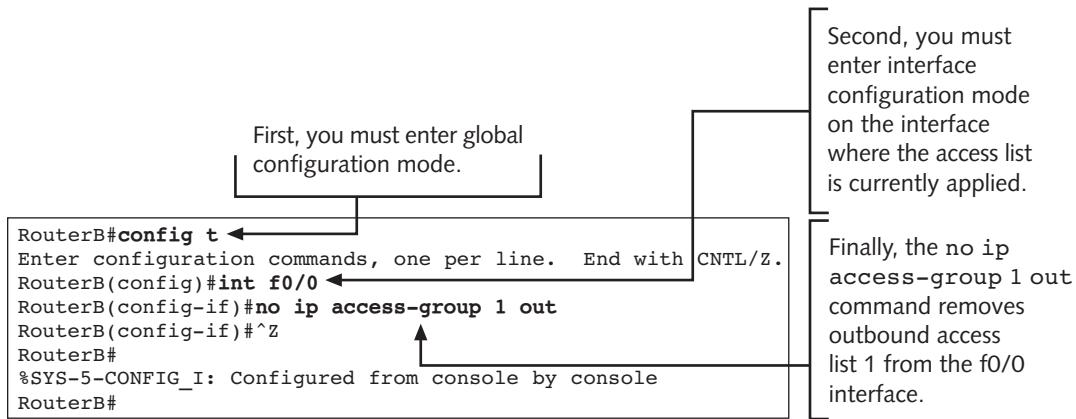
An outbound access list, access list 1, is set. No inbound list is set.

The `--More--` statement at the end of router output signifies that more output is available. Pressing the spacebar will display another page of output. Pressing the Enter key will display another line of output.

**Figure 10-12** The `show ip interface` command

If you decide that an access list needs to be removed from an interface, you can remove it with the `no ip access-group [list #]` command, as shown in Figure 10-13.

If you type the `show ip interface` command, it will show that access list 1 is no longer an outbound access list. Figure 10-14 displays the results of the `show ip interface` command after you type the `no ip access-group 1 out` command.

**Figure 10-13** Removing an IP access list from an interface

```

RouterB#show ip interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 172.22.2.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Multicast reserved groups joined: 224.0.0.9
  Outgoing access list is not set ←
  Inbound access list is not set
  Proxy ARP is enabled
  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 disabled
  IP multicast fast switching is enabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
--More--

```

An outbound list is no longer set on f0/0.

**10**

**Figure 10-14** Results of the show ip interface command after removal of access list 1 from f0

Access lists are not effective until they are applied to an interface. If a list is created and not applied, or if a list is applied and then the list itself is removed, the commands will be executed, but all traffic will be permitted in and out.

Now assume that instead of blocking a single host from subnet 172.22.5.0, you want to block all traffic from this subnet to subnet 172.22.2.0, using a standard IP access list. Once again, you need to create the access list in global configuration mode and apply the list to an interface in interface configuration mode. In this example, you will apply the list as an outbound filter on RouterB's FastEthernet0/0 interface, as this is closest to the destination as possible. (Recall that Figure 10-8 shows the network that contains RouterB.) Both parts of the task

## 272 Chapter 10 Access Lists

can be accomplished at the same time; the router output in Figure 10-15 shows both the creation of the list and the application of the list as an outbound filter on FastEthernet0/0.

```

RouterB con0 is now available
Press RETURN to get started.

RouterB>en
Password:
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#access-list 1 deny 172.22.5.0 0.0.0.255 ←
RouterB(config)#access-list 1 permit any
RouterB(config)#int f0/0
RouterB(config-if)#ip access-group 1 out ←
RouterB(config-if)#^Z
RouterB#
%SYS-5-CONFIG_I: Configured from console by console
RouterB#

```

From global configuration mode, you enter the commands for the access list.

In interface configuration mode, you apply the access list to the f0/0 interface as an outbound list.

**Figure 10-15** Creation and application of standard IP access list

You can use the `show access-lists` or `show ip access-lists` command followed by the `show ip interface` command to verify that the list has been entered and applied correctly. Figure 10-16 shows the results of these two commands after the procedures in Figure 10-15 have been performed.

```

RouterB#show access-lists
Standard IP access list 1 ←
    deny    172.22.5.0, wildcard bits 0.0.0.255
    permit any
RouterB#

RouterB#show ip interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 172.22.2.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Multicast reserved groups joined: 224.0.0.9
  Outgoing access list is 1 ←
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable messages are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP multicast fast switching is enabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
--More--

```

Access list 1 has been correctly added to RouterB.

Access list 1 has been correctly applied to interface FastEthernet0/0 on RouterB.

**Figure 10-16** The `show access-lists` and `show ip interface` commands

Finally, assume that you want to block access to the 172.22.2.0 subnet from all hosts on subnets 172.22.4.0 and 172.22.5.0. You can accomplish this task by entering the commands shown in Figure 10-17.

```

RouterB>en
Password:
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#access-list 1 deny 172.22.4.0 0.0.0.255
RouterB(config)#access-list 1 deny 172.22.5.0 0.0.0.255
RouterB(config)#access-list 1 permit any
RouterB(config)#int f0/0
RouterB(config-if)#ip access-group 1 out
RouterB(config-if)#^Z
RouterB#
%SYS-5-CONFIG_I: Configured from console by console
RouterB#

```

**Figure 10-17** Access list that blocks multiple subnets

Again, you can use the `show ip access-lists` or `show access-lists` commands to verify that the access list was entered correctly. The `show ip interface` command will show all IP interfaces. To view a specific interface, you can use `show ip interface [interface#]`. For instance, throughout these examples, the `show ip interface f0/0` command could be used to view just the FastEthernet0/0 interface.

10

## Monitoring Standard IP Access Lists

Three main commands are available for monitoring access lists on your router. The first two, `show access-lists` and `show ip access-lists`, display the exact syntax of all access lists and IP access lists, respectively. The `show interfaces` or `show ip interface` command is used to verify that an access list has been successfully applied to an interface. It is a good idea to run each of these commands after creating and applying access lists, to visually inspect and verify that statements were typed correctly and that the lists will function as entered. Use the `no access-list [list #]` command to remove the list and the `no ip access-group [list #] [direction]` command to remove the application of the list.

---

## Extended IP Access Lists

As previously noted, standard IP access lists are limited to filtering by source IP addresses only. Extended IP access lists, on the other hand, can filter by source IP address, destination IP address, protocol type, and application port number. This granularity allows you to design extended IP access lists that permit or deny a single type of IP protocol, such as TCP, and then filter by a particular port of a particular protocol, such as port 21 or FTP.

To configure extended IP access lists, you must create the list and then apply it to an interface using the following syntax. A detailed explanation of each element follows the example.

```

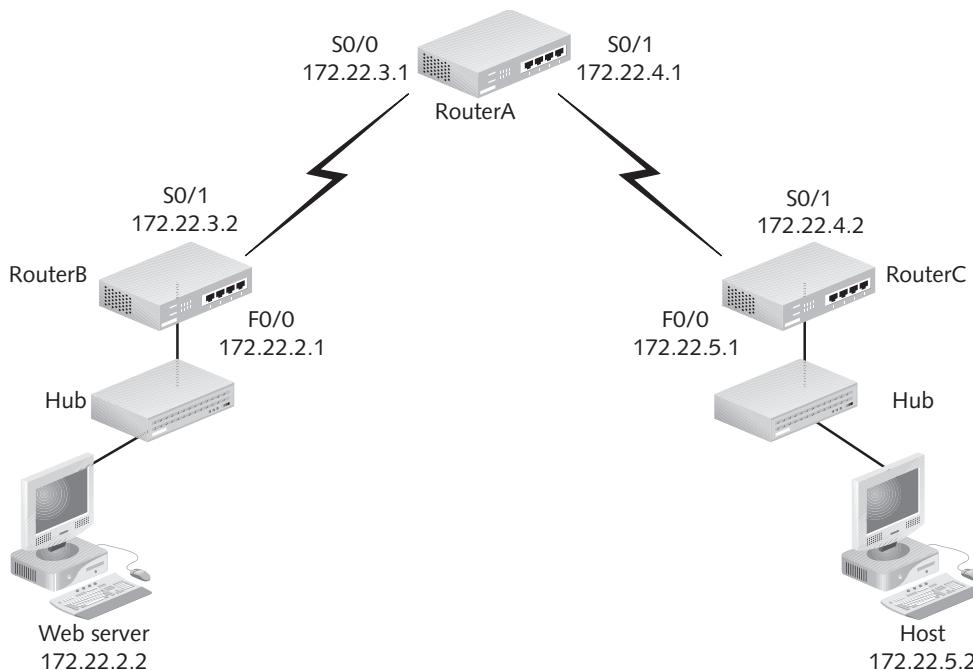
access-list [list #] [permit/deny] [protocol] [source IP address]
[source wildcard mask] [operator] [port] [destination IP address]
[destination wildcard mask] [operator] [port] [log]

```

- *[list #]*—Extended IP access lists are represented by a number in the range of 100–199 (in IOS versions 11.2 and greater, they can also be represented by text names).
- *[permit|deny]*—Used to specify the nature of the access list line. It is either a permit or a deny statement.
- *[protocol]*—The IP protocol to be filtered can be IP (which includes all protocols in the TCP/IP suite), TCP, UDP, ICMP, or others.
- *[source IP address]*—The IP address of the source.
- *[source wildcard mask]*—A wildcard mask, or inverse mask, applied to determine which bits of the source address are significant.
- *[destination IP address]*—The IP address of the destination.
- *[destination wildcard mask]*—A wildcard mask, or inverse mask, applied to determine which bits of the destination address are significant.
- *[operator]*—Can contain lt (less than), gt (greater than), eq (equal to), or neq (not equal to). It is used if an extended list filters by a specific port number.
- *[port]*—If necessary, the port number of the protocol to be filtered. Alternatively, a service using TCP, such as www or ftp, can be specified.
- *[log]*—Turns on logging of access list activity.

## Extended IP Access List Examples

Using Figure 10-18 as an example, this section discusses how to block host 172.22.5.2 from accessing Web services on server 172.22.2.2. The extended IP access list example shows how to block www access using the context-sensitive, built-in Help features in the Cisco IOS that display all available IOS options.



**Figure 10-18** Sample IP network with a Web server

The configuration begins when you type the enable command to enter privileged mode on RouterC. Typing ? at the privileged mode prompt shows all available commands. Figure 10-19 displays all the commands required to create the extended IP access list. The figure also displays the different access list groupings and their number ranges.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Typing the ? command displays all commands available from this prompt. Notice that <b>access-list</b> is the second command on the list.</p> <pre> RouterC&gt;enable Password: RouterC#config t Enter configuration commands, one per line. End with CNTL/Z. RouterC(config)#? Configure commands:     aaa                               Authentication, Authorization and Accounting.     access-list                      Add an access list entry     alias                            Create command alias     arp                             Set a static ARP entry     async-bootp                     Modify system bootp parameters     banner                          Define a login banner     boot                           Modify system boot parameters     bridge                         Bridging Group.     buffers                        Adjust system buffer pool parameters     busy-message                   Display message when connection to host fails     cdp                            Global CDP configuration subcommands     chat-script                    Define a modem chat script     clock                           Configure time-of-day clock     config-register               Define the configuration register     default-value                 Default character-bits values     dialer-list                   Create a dialer list entry     dnsix-dmdp                    Provide DMDP service for DNSIX     dnsix-nat                     Provide DNSIX service for audit trails     downward-compatible-config   Generate a configuration compatible with older software     enable                         Modify enable password parameters --More -- </pre> | <p>You then enter the <b>access-list</b> command to begin typing the access list. Again, the ? command reveals correct syntax for the command and possible number ranges for different access lists.</p> <pre> RouterC(config)#access-list ? &lt;1-99&gt;      IP standard access list &lt;100-199&gt;    IP extended access list &lt;1000-1099&gt;  IPX SAP access list &lt;1100-1199&gt;  Extended 48-bit MAC address access list &lt;1200-1299&gt;  IPX summary address access list &lt;200-299&gt;    Protocol type-code access list &lt;700-799&gt;    48-bit MAC address access list &lt;800-899&gt;    IPX standard access list &lt;900-999&gt;    IPX extended access list </pre> | <p>Because this list is an extended IP address, it will be designated with the number 100.</p> <pre> RouterC(config)#access-list 100 ? </pre> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|

**Figure 10-19** Extended IP access list example

Unlike standard IP access lists, extended access lists do not have a default wildcard mask of 0.0.0.0. Therefore, you must specify the wildcard mask for the source IP address. You can use either the typical wildcard mask, as previously defined, or you can use shortcuts, as in the example in Figure 10-20. The **host** keyword is short for a wildcard mask of 0.0.0.0; in other

## 276 Chapter 10 Access Lists

```
RouterC(config)#access-list 100 deny tcp host 172.22.5.2 host 172.22.2.2 ?
eq      Match only packets on a given port number
established Match established connections
gtc     Match only packets with a greater port number
log     Log matches against this entry
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
range   Match only packets in the range of port numbers
tos     Match packets with given TOS value
<cr>
```

At this point, you have specified your protocol and the source and destination addresses. You must now configure the operator and port. The example list should block WWW and therefore must contain an "equal to" operator and the WWW port number or name.

You place the port number or name and press Enter to add the line to the access list.

The next line you must add is a line that will permit all other IP traffic. If you do not, the implicit deny any at the end of the access list will block all other traffic. Notice that the any keyword is used twice; the first instance corresponds to any source, and the second corresponds to any destination.

|                                                                               |  |
|-------------------------------------------------------------------------------|--|
| RouterC(config)#access-list 100 deny tcp host 172.22.5.2 host 172.22.2.2 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 (used infrequently, 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)                                    |  |
| 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)                                                 |  |

```
RouterC(config)#access-list 100 deny tcp host 172.22.5.2 host 172.22.2.2 eq www
RouterC(config)#access-list 100 permit ip any any
RouterC(config)#

```

**Figure 10-20** Extended IP access list example continued

words, the line will only be applied to packets that match the one source address specified with the host keyword. Figure 10-20 shows a continuation of the access list started in Figure 10-19; note the use of the host keyword. Notice also that the host keyword is placed before the IP address rather than after it, like the wildcard mask would be.

Once an extended IP access list is created, it must be applied to an interface, just like a standard list. The difference is the placement of the list. Standard IP access lists examine the source address only. As a result, you must place them as close to the destination as possible to avoid blocking traffic bound for another interface or network. On the other hand, extended IP access lists are able to filter based on source and destination. Therefore, they are placed as close to the source as possible.

In our sample network, the list is best placed as an inbound filter on the FastEthernet0/0 interface of RouterC. Traffic from host 172.22.5.2 destined for the Web server at 172.22.2.2 will be blocked before it has a chance to even enter the network. Because of their placement, extended access lists create less traffic across the internetwork. Figure 10-21 displays the proper commands for adding the extended access list as an inbound list on interface FastEthernet0/0.

```
RouterC(config)#int f0/0
RouterC(config-if)#ip access-group 100 in
RouterC(config-if)#^Z
RouterC#
%SYS-5-CONFIG_I: Configured from console by console
RouterC#
```

Once in interface configuration mode, you use the ip access-group [list #] [in | out] command to add the list to the interface.

**Figure 10-21** Applying an extended IP access list to an interface

10

To remove a list from an interface, you enter interface configuration mode and use the no ip access-group [list #] [in/out] command, as shown in Figure 10-22.

```
RouterC#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterC(config)#int f0/0
RouterC(config-if)#no ip access-group 100 in
RouterC(config-if)#^Z
RouterC#
%SYS-5-CONFIG_I: Configured from console by console
RouterC#
```

Once in interface configuration mode, you use the no ip access-group [list #] [in | out] command to remove a list from the interface.

**Figure 10-22** Removing an extended IP access list from an interface

## The “Established” Parameter

Very often, network administrators want to block all TCP/IP traffic outside their network from coming into the network. However, if you use deny statements to deny all traffic coming in, no one will be able to browse the Web, get e-mail, ping, or perform other networking activities that involve a response to a request. For example, if you attempt to view the Web page at [www.cisco.com](http://www.cisco.com), a DNS server somewhere has to resolve [www.cisco.com](http://www.cisco.com) to an IP address and provide that address to your computer. This usually requires traffic from outside your network coming into your network. If all traffic coming in were blocked by an

access list, DNS and other network activities that we take for granted could not be accomplished. The easiest way to get around this problem is to use an extended IP access list with the **established** parameter. Review the following access list line:

```
fffaccess-list 100 permit tcp any 15.0.0.0 0.255.255.255 established
```

This command would permit traffic from any host on any network to any destination on the 15.0.0.0 network, as long as the traffic was in response to a request initiated inside network 15.0.0.0. In other words, a TCP connection must already be established in order for the outside traffic to be let in.

## Monitoring Extended IP Access Lists

The same commands used to monitor standard IP access lists are used to monitor extended IP access lists. If you want to view the access lists configured on your router, you use the **show access-lists** or **show ip access-lists** command. To see if the list has been applied to an interface, use the **show interfaces** or **show ip interface** command. The **show ip access-lists** command is shown in Figure 10-23.

```
RouterC#show ip access-lists
Extended IP access list 100
    deny tcp host 172.22.5.2 host 172.22.2.2 eq www
    permit ip any any (450 matches) ←
RouterC#
```

Extended access lists show the number of matches per line of the access list. The **deny** statement in list 100 has not been used in this example. No attempts have been made by host 172.22.5.2 to access the Web server.

450 packets have matched the **permit ip any any** statement.

**Figure 10-23** The **show ip access-lists** command

As shown in the figure, extended IP lists keep track of the number of packets that pass each line of an access list. These matches or counters can be reset to zero for troubleshooting purposes. The **clear access-list counters [list #]** command (see Figure 10-24) clears the counters. The **no access-list [list#]** command removes the list and the **no ip access-group [list#] [direction]** command removes the application of the list.

```
RouterC#clear access-list counters 100
RouterC#show ip access-list
Extended IP access list 100
    deny tcp host 172.22.5.2 host 172.22.2.2 eq www
    permit ip any any (9 matches) ←
RouterC#
```

Notice that the number of matches on access list 100 has dropped from the previous 450 matches in Figure 10-23 to 9 because the counters were cleared to 0 (zero).

**Figure 10-24** The **clear access-list counters** command

## Using Named Lists

In Cisco IOS versions 11.2 and above, names instead of numbers can be used to identify lists. These are known as **named access lists**. You cannot use the same name for multiple access lists; even different list types cannot have the same name. For example, you could not specify a standard list named Cannon if you already had an extended list named Cannon. To name a standard IP access list, use the following syntax:

```
RouterC(config)#ip access-list standard [name]
```

To name an extended IP access list, use the following syntax:

```
RouterC(config)#ip access-list extended [name]
```

Once the list is named, the permit or deny statement is entered. The commands follow the same syntax as unnamed lists, but the beginning part of the command is not included. For example, the syntax for a deny or permit statement for a standard IP named list would be:

```
RouterC(config-std-nacl)#deny{source [source-wildcard] | any}
```

or

```
RouterC(config-std-nacl)#permit{source [source-wildcard] | any}
```

To apply a standard IP named list to an interface, the syntax would be:

```
RouterC(config-if)#ip access-group [name] [in | out]
```

The naming feature allows you to maintain security by using an easily identifiable access list. It also removes the limit of 100 lists per filter type. In addition, with named access lists lines can be selectively deleted in the ACL. This feature does not allow you to add lines to the ACL; any lines added to a named ACL are applied to the end of the list. Named ACLs provide greater flexibility to network administrators who work in environments where large numbers of ACLs are needed, such as a large ISP.

10

## Controlling VTY Line Access

As previously discussed, access lists are used for both traffic flow and security. One useful security feature of access lists is restricting access to telnet on your router by controlling VTY line access. For example, imagine that you want to allow access to the VTY lines from a management station at the IP address 192.168.12.12/24 only. You must first create a standard IP access list that permits the management workstation. The access-list command to permit the workstation is:

```
fRouterA(config)#access-list 12 permit 192.168.12.12 0.0.0.0
```

The access list can also be created using the host keyword instead of the 0.0.0.0 wildcard mask:

```
RouterA(config)#access-list 12 permit host 192.168.12.12
```

Because the single host wildcard mask is the default for standard IP access lists, the command could be written without either the 0.0.0.0 mask or the host keyword.

Once the access list is created, it must be applied to the VTY lines via the access-class command. The syntax for this command is:

```
access-class [acl #] in | out
```

To apply access list 12 to the VTY lines, you would use the following command:

```
RouterA(config)#line vty 0 4
RouterA(config-line)#access-class 12 in
```

While it is possible to restrict access to the VTY lines to a particular host, as shown in the example, you can also restrict access to a subnet or network. To accomplish this, you must modify the access list to specify either a subnet or network. The commands to restrict access to the VTY lines to network 192.168.12.0/24 only are:

```
ffRouterA(config)#access-list 13 permit 192.168.12.0 0.0.0.255
ffRouterA(config)#line vty 0 4
ffRouterA(config-line)#access-class 13 in
```

This configuration allows VTY access from hosts on the 192.168.12.0/24 network only.

## Using Security Device Manager to Create Access Control Lists

The Cisco Security Device Manager (SDM), introduced in Chapter 6, provides a GUI-based configuration tool for Cisco devices. Using the SDM, an administrator can accomplish all the tasks that formerly required use of the CLI interface. SDM allows you to easily create a standard or an extended access list or, as it is known in the SDM, an Access Control List (ACL).

To begin creating an ACL, you start at the Home Page of SDM, as shown in Figure 10-25. The Home page, described in Chapter 6, displays a quick summary of the router model

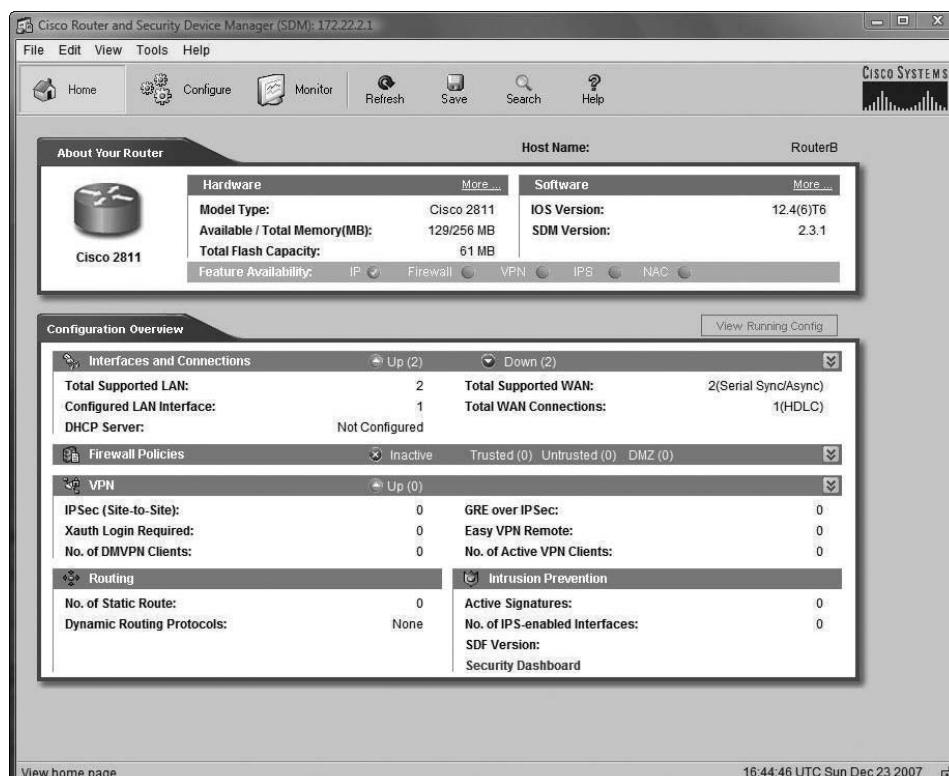
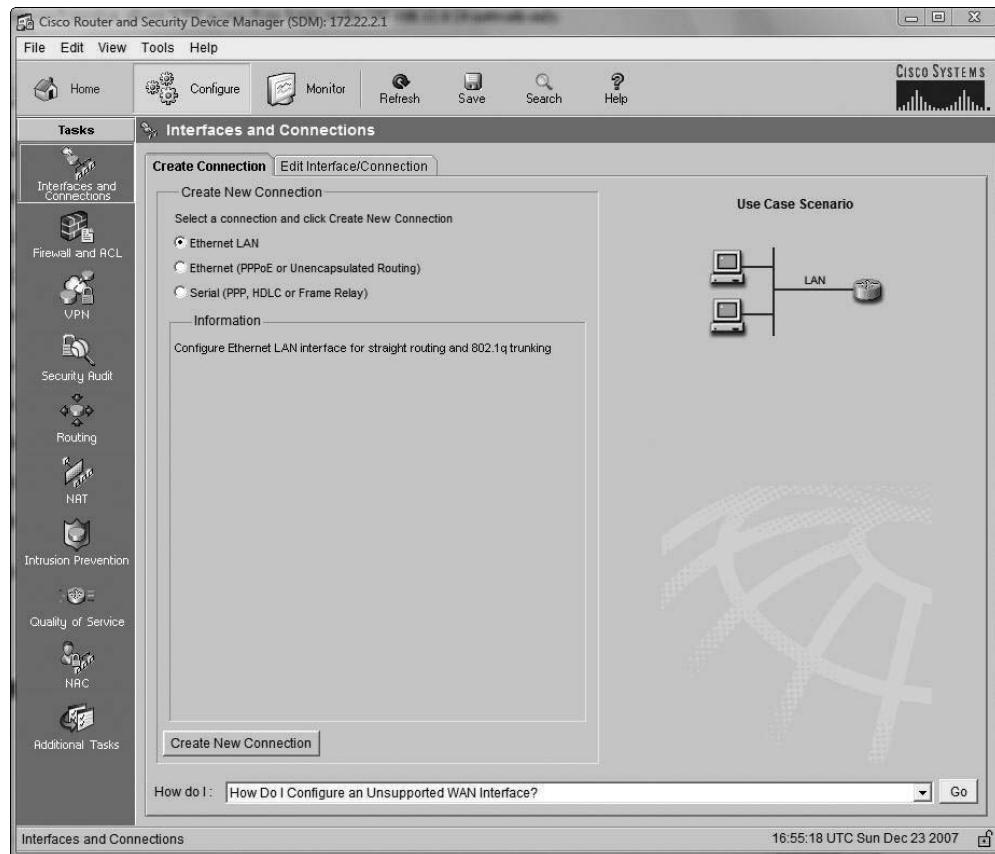


Figure 10-25 Home window

number, IOS version, configured interfaces, firewall settings, VPN settings, Routing protocols and Intrusion Prevention statistics. At the Home Page, click Configure to move to the Interfaces and Connection screen shown in Figure 10-26.



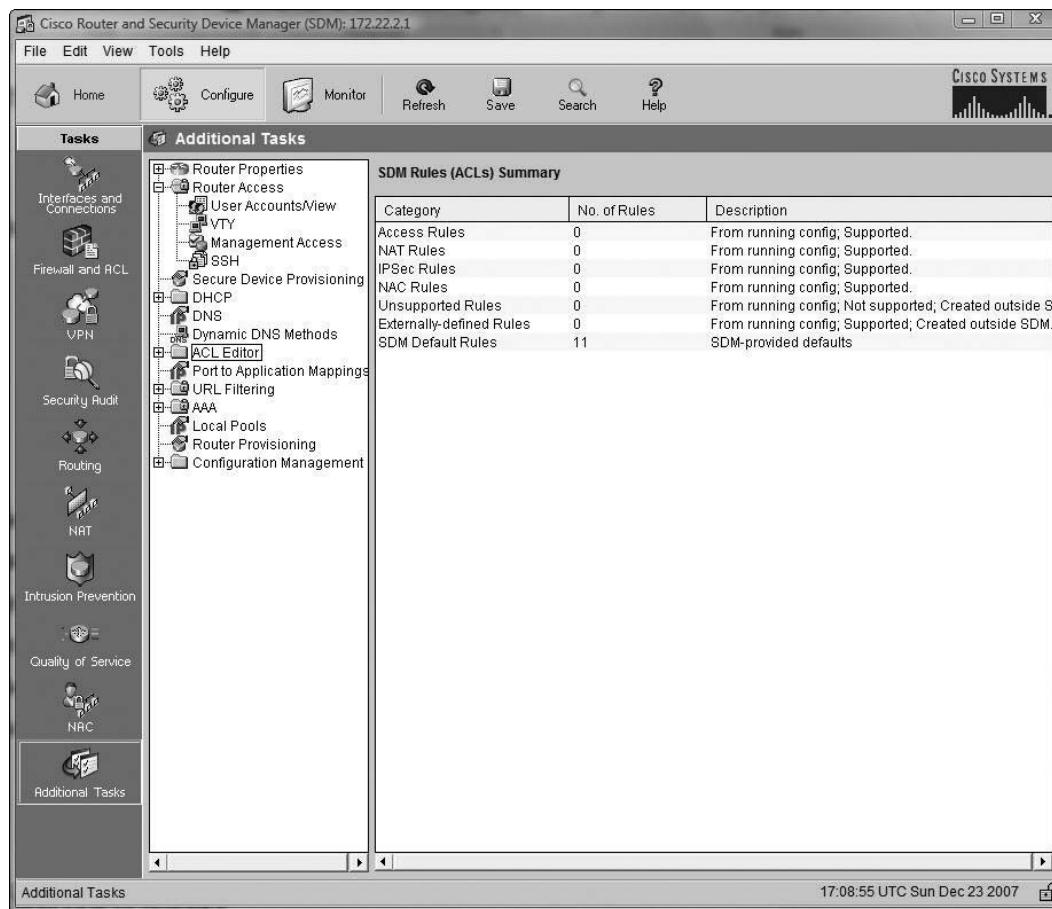
**Figure 10-26** Interfaces and Connection window

On the Interfaces and Connection screen, you can perform tasks related to:

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

## 282 Chapter 10 Access Lists

To get started on a particular task, click the relevant icon in the Tasks panel (the left-most part of the SDM window). To create standard and extended ACLs, you might think that you would start by clicking the Firewall and ACL icon in the Tasks panel. However, that option opens a wizard for configuring the router as a firewall. (Note that the router must have an IOS version that supports the firewall feature set.) Instead, to configure standard and extended ACLs, click the Additional Tasks icon in the Tasks panel. This opens the Additional Tasks window shown in Figure 10-27.

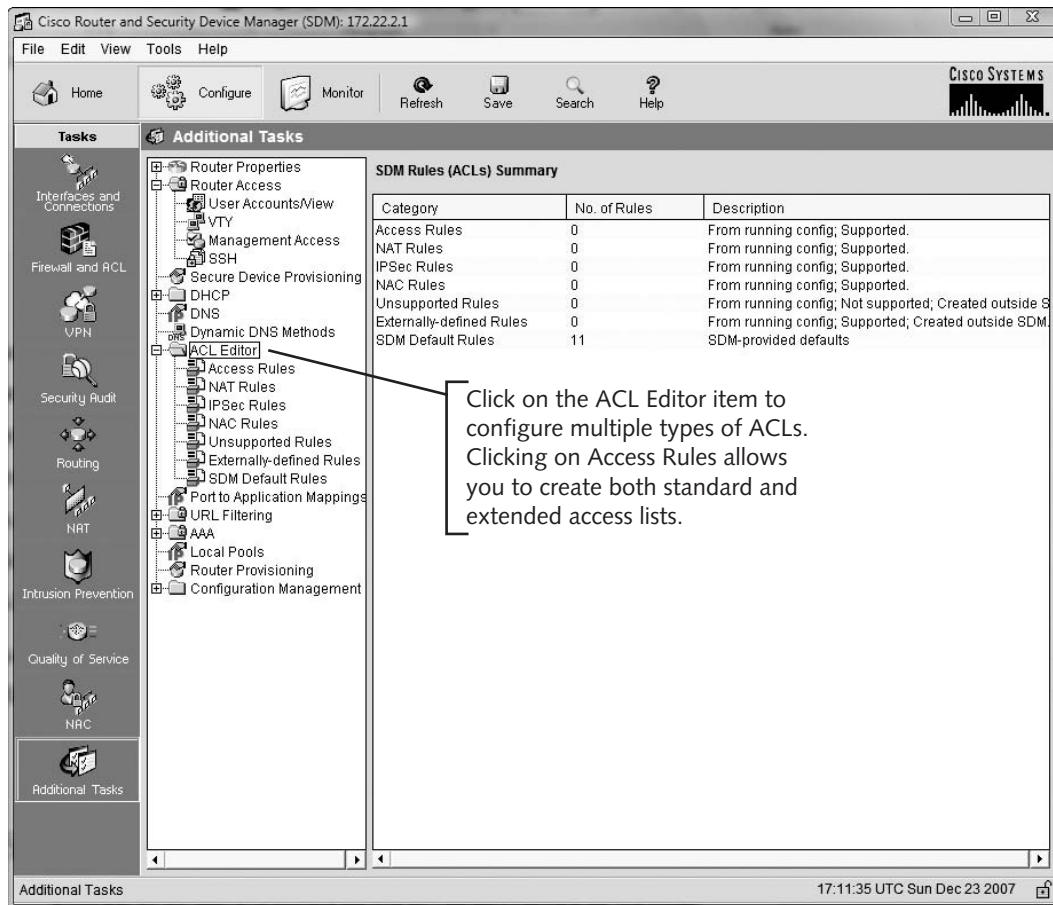


**Figure 10-27** Additional Tasks window

Within the Additional Tasks window, expanding the ACL Editor as shown in Figure 10-28 allows you to add many types of ACLs, such as:

- Access Rules
- NAT Rules
- IPsec Rules

- NAC Rules
- Unsupported Rules
- Externally-defined Rules
- SDM Default Rules



**Figure 10-28** ACL Editor screen

Once in the ACL Editor, you can begin to create a standard or extended ACL. To get started, right-click Access Rules, and then click Add item. The Add a Rule dialog box opens, as shown in Figure 10-29.

To create a standard ACL, click the Type list arrow, click Standard Rule, and then click the Add button under Rule Entry. The Add a Standard Rule Entry dialog box opens, as shown in Figure 10-30, providing options to configure a standard ACL. Figure 10-31 shows the settings required to create an access list that permits only traffic from the network 192.168.12.0/24.

## 284 Chapter 10 Access Lists

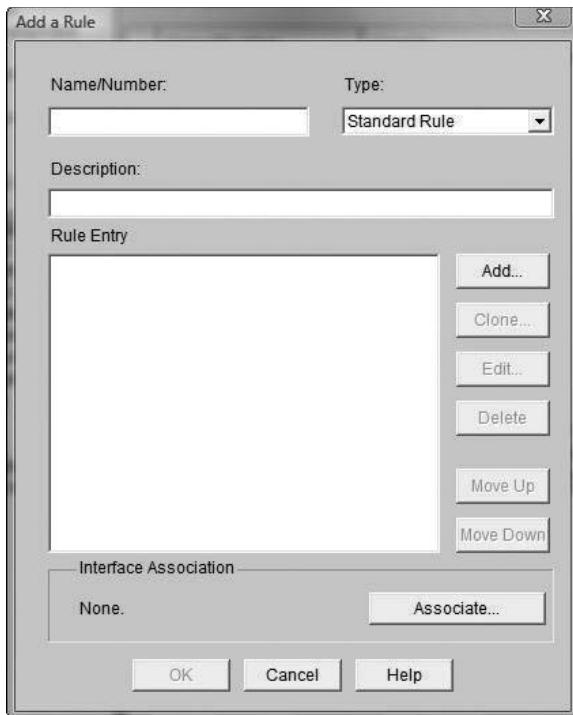


Figure 10-29 Add a Rule dialog box

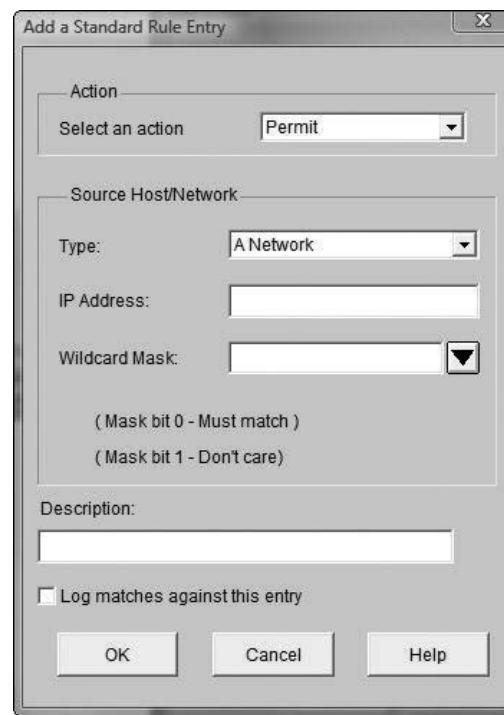


Figure 10-30 Add a Standard Rule Entry

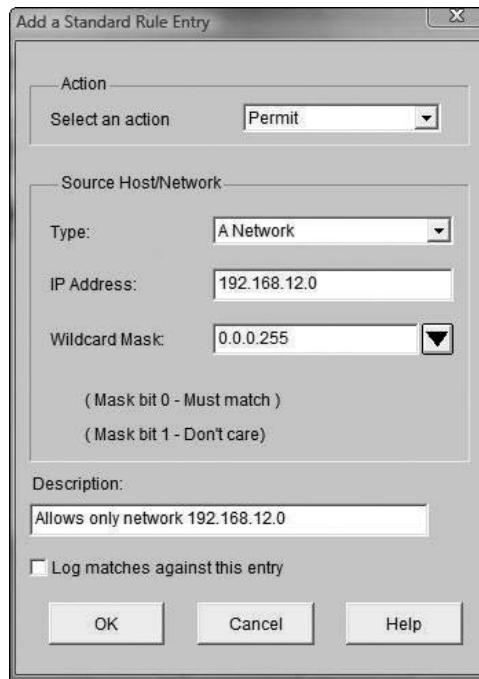
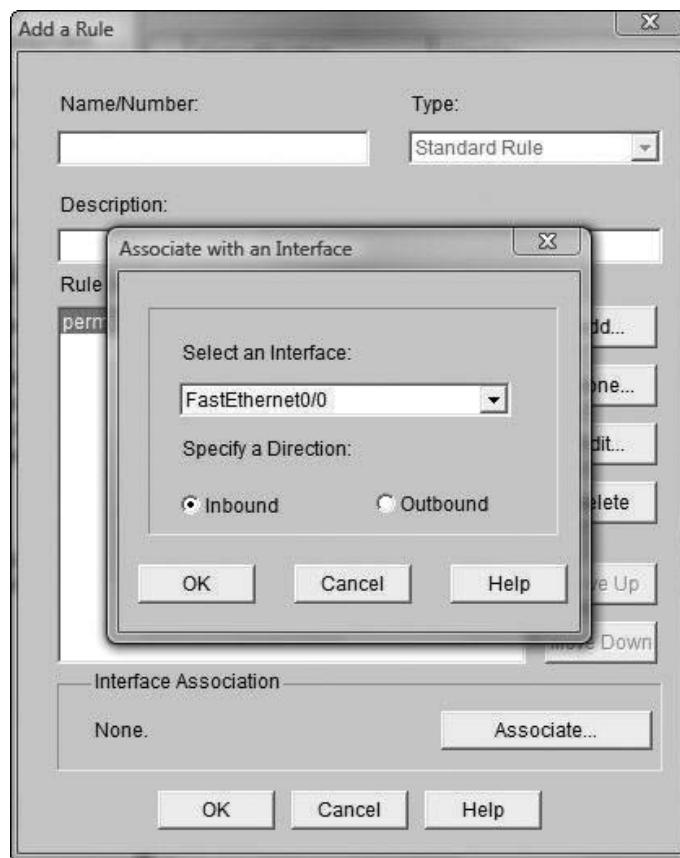


Figure 10-31 Standard ACL Configuration

Next, you need to associate the ACL with an interface. To do this, click the OK button to return to the Add a Rule dialog box, and then click the Associate button to open the Associate with an Interface dialog box. Figure 10-32 shows the settings required to associate the standard access list from Figure 10-31 with a FastEthernet interface in the inbound direction.



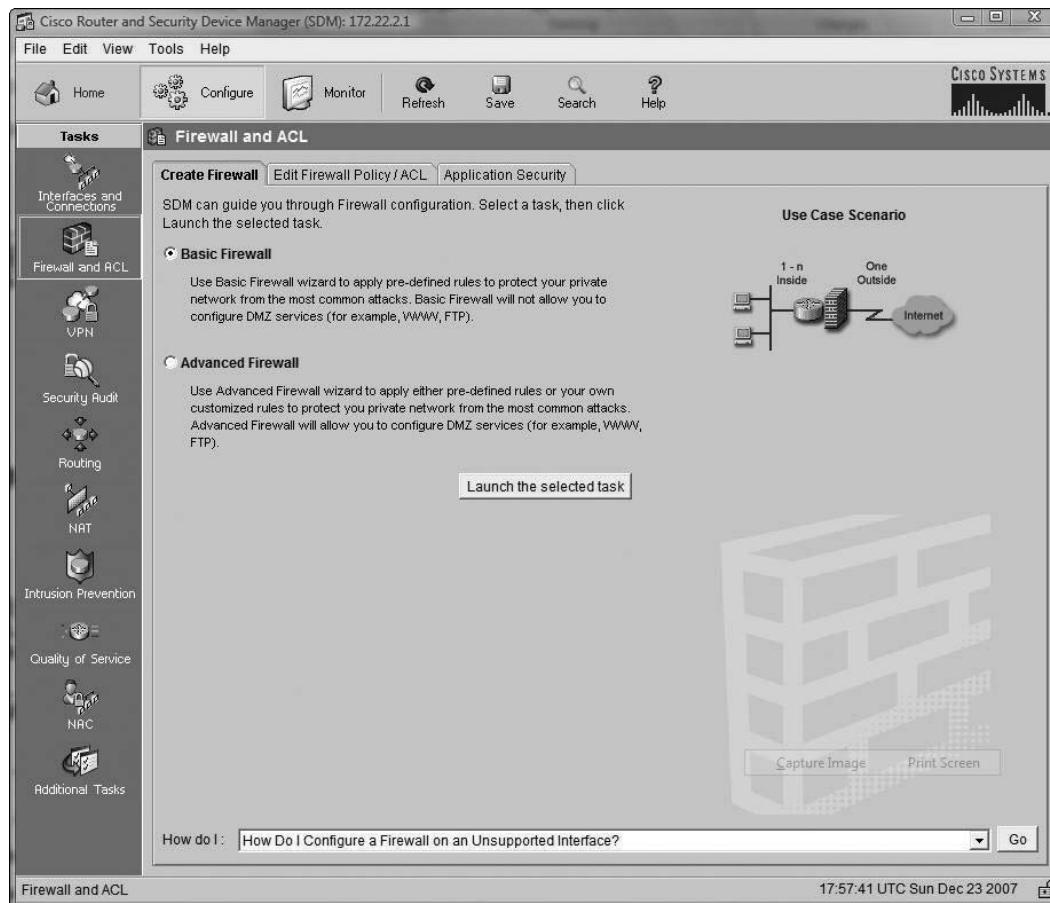
**Figure 10-32** Associating ACL with an Interface

Once applied, the standard ACL will act exactly like an ACL configured from the CLI. You can create an extended ACL by following the same steps as when creating a standard ACL, but selecting Extended in the Rule using the Type list box in the Add a Rule dialog box (shown earlier in Figure 10-29). Also, just as with extended rules in the CLI, in the SDN you must specify source address, destination address, and protocol.

The SDM may seem simpler than CLI because it gives administrators the option to work in a GUI, but you still need to understand basic CLI commands and features in order to use the SDM effectively.

## Using Security Device Manager to Create a Router Firewall

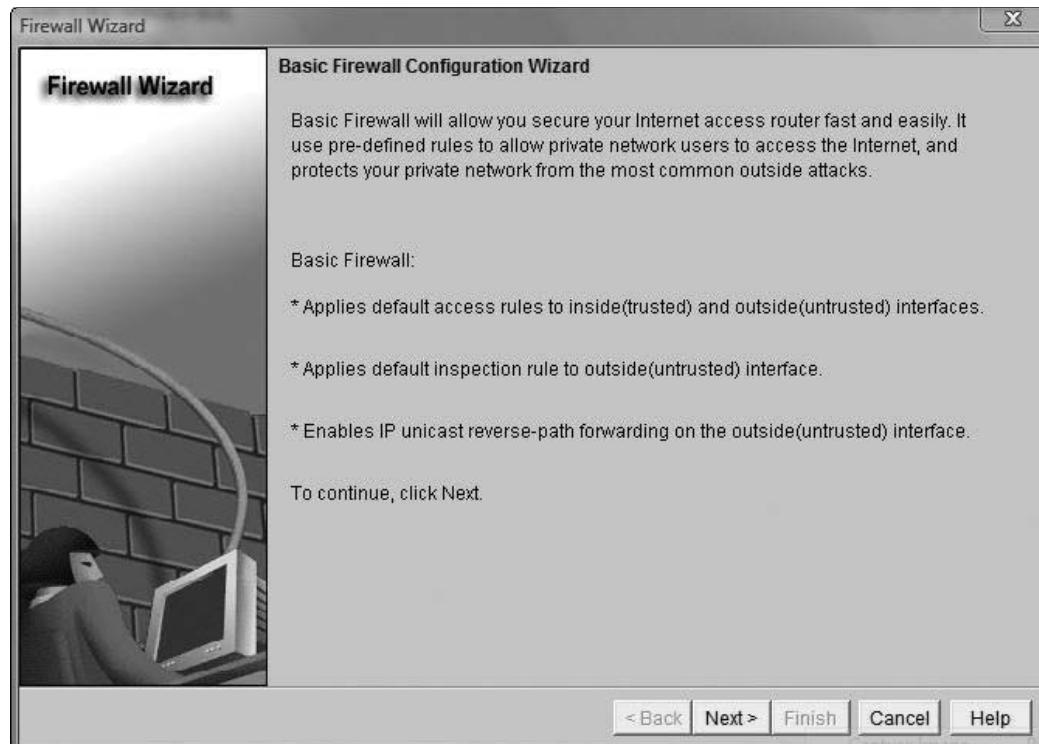
As you have learned, the SDM does not allow you to perform any ACL-related tasks that cannot be performed in the CLI. However, unlike the CLI, the SDM does allow a router to be configured as a firewall. To begin this task, click the Firewall and ACL icon in the Tasks panel. The Firewall and ACL window opens, as shown in Figure 10-33. Here you can choose between the Basic Firewall Configuration Wizard and the Advanced Firewall Configuration Wizard.



**Figure 10-33** Firewall and ACL Configuration

The Basic Firewall Configuration Wizard allows you to create a simple firewall consisting of one trusted and one untrusted interface. The Advanced Firewall Configuration Wizard allows you to configure a trusted, untrusted, and DMZ (or demilitarized zone interfaces) firewall. The configuration of a DMZ is the main difference between the Basic and Advance firewall wizards; a DMZ cannot be created using the Basic Firewall Wizard. In the following examples, we will focus on creating a basic firewall.

Figure 10-34 shows the first window of the Basic Firewall Configuration Wizard. Before you begin any type of firewall configuration, you must first designate what interface will be trusted (or Inside) and what interface will be untrusted (or Outside). Normally, the trusted interface is the interface connected to your company LAN via a FastEthernet or faster connection. The untrusted interface usually connects to the ISP and can be serial or FastEthernet.



**Figure 10-34** Basic Firewall Wizard

In Figure 10-35, the FastEthernet0/0 interface has been selected as the trusted interface, and the Serial0/3/0 has been selected as the untrusted interface. A trusted interface can originate traffic and is allowed through the router by default. Any traffic from a trusted interface can go to an untrusted interface. The untrusted interface, however, cannot accept inbound traffic by default. In our example, the users on the FastEthernet can send traffic out to the ISP and receive responses because the traffic originated on a trusted interface. In contrast, traffic from the ISP is not able to be the source of originating traffic because it is an untrusted interface.

The next step in the Basic Firewall Configuration Wizard is determining the level of security you wish to impose on the router. The SDM offers three choices: High Security, Medium Security, and Low Security. Each of these settings has distinct properties. Figure 10-36 shows

## 288 Chapter 10 Access Lists

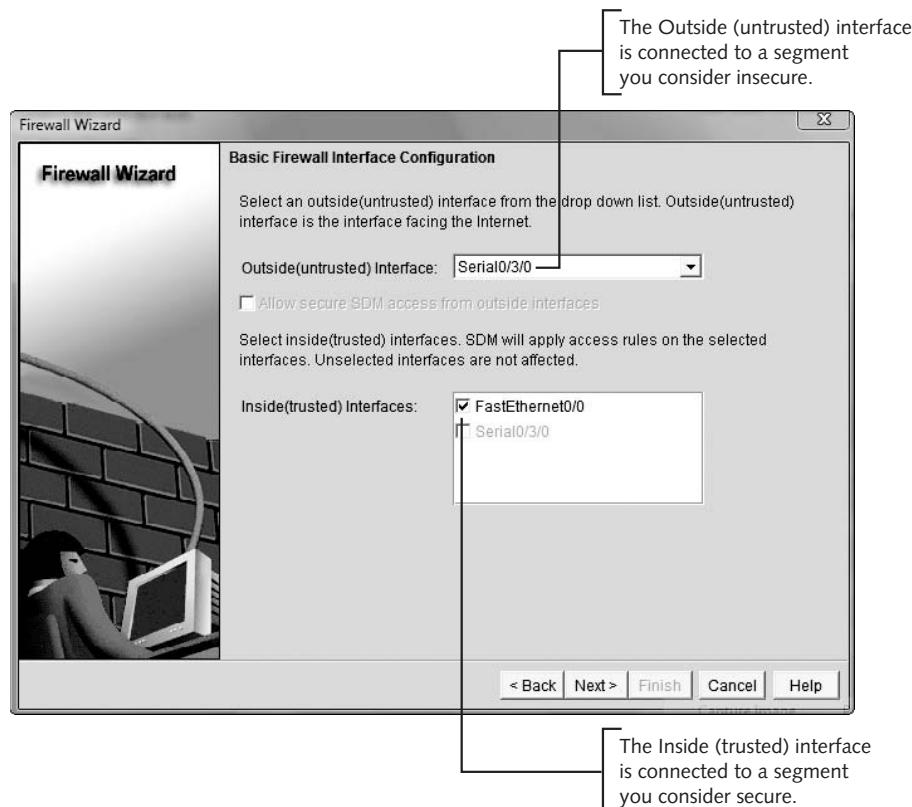


Figure 10-35 Configuring trusted and untrusted interfaces

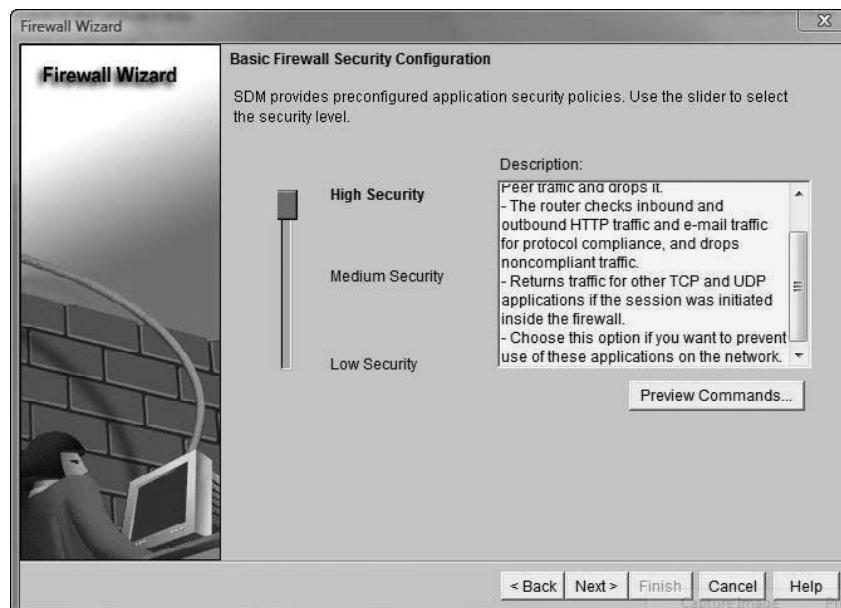


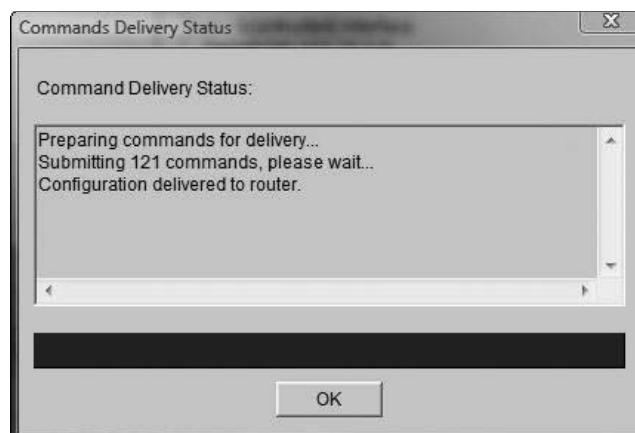
Figure 10-36 Basic Firewall Security Configuration

the slider set to High Security. Table 10-2 shows the basic firewall security settings and their effects on the router.

| Setting         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High Security   | <p>The router identifies inbound and outbound Instant Messaging and Peer-to-Peer traffic and drops it.</p> <p>The router checks inbound and outbound HTTP traffic and e-mail traffic for protocol compliance, and drops noncompliant traffic.</p> <p>The router returns traffic for other TCP and UDP applications if the session was initiated inside the firewall.</p> <p>Choose this option if you want to prevent use of these applications on the network.</p> |
| Medium Security | <p>The router identifies inbound and outbound Instant Messaging and Peer-to-Peer traffic, and checks inbound and outbound HTTP traffic and e-mail traffic for protocol compliance.</p> <p>The router returns TCP and UDP traffic on sessions initiated inside the firewall.</p> <p>Choose this option if you want to track use of these applications on the network.</p>                                                                                            |
| Low Security    | <p>The router does not identify application-specific traffic. Returns TCP and UDP traffic on sessions initiated inside the firewall.</p> <p>Choose this option if you do not need to track use of these applications on the network.</p>                                                                                                                                                                                                                            |

**Table 10-2** Basic Firewall Security Configuration Settings

Once you select a Security Configuration, click Next, add a DNS entry, and then click Finish. The SDM then configures the router as a firewall. When the configuration is finished, you see the Commands Delivery Status dialog box, shown in Figure 10-37, which reports that 121 commands were delivered to the router. As the entire configuration process takes about five minutes, this is a simple way to convert your router into a basic firewall. Figure 10-38 shows the Edit Firewall Policy/ACL tab after the router has been configured with the High Security Configuration option of the Basic Firewall Configuration Wizard.



**Figure 10-37** Command Delivery Confirmation

## 290 Chapter 10 Access Lists



Figure 10-38 Edit Firewall Policy/ACL Tab

To see the results of the Basic Firewall Wizard, you can issue the `show running-config` command at the command prompt. The following output shows the configuration delivered to the firewall router once the wizard completes:

```

RouterB#sh run
Building configuration...

Current configuration : 4666 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
```

```
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
ip name-server 192.168.12.12
ip inspect log drop-pkt
ip inspect name SDM_HIGH appfw SDM_HIGH
ip inspect name SDM_HIGH icmp
ip inspect name SDM_HIGH dns
ip inspect name SDM_HIGH esmtp
ip inspect name SDM_HIGH https
ip inspect name SDM_HIGH imap reset
ip inspect name SDM_HIGH pop3 reset
ip inspect name SDM_HIGH tcp
ip inspect name SDM_HIGH udp
!
appfw policy-name SDM_HIGH
    application im aol
        service default action reset alarm
        service text-chat action reset alarm
        server deny name login.oscar.aol.com
        server deny name toc.oscar.aol.com
        server deny name oam-d09a.blue.aol.com
        audit-trail on
    application im msn
        service default action reset alarm
        service text-chat action reset alarm
        server deny name messenger.hotmail.com
        server deny name gateway.messenger.hotmail.com
        server deny name webmessenger.msn.com
        audit-trail on
    application http
        strict-http action reset alarm
        port-misuse im action reset alarm
        port-misuse p2p action reset alarm
        port-misuse tunneling action reset alarm
    application im yahoo
        service default action reset alarm
        service text-chat action reset alarm
        server deny name scs.msg.yahoo.com
        server deny name scsa.msg.yahoo.com
        server deny name scsb.msg.yahoo.com
        server deny name scsc.msg.yahoo.com
```

**292** Chapter 10 Access Lists

```
server deny name scsd.msg.yahoo.com
server deny name cs16.msg.dcn.yahoo.com
server deny name cs19.msg.dcn.yahoo.com
server deny name cs42.msg.dcn.yahoo.com
server deny name cs53.msg.dcn.yahoo.com
server deny name cs54.msg.dcn.yahoo.com
server deny name ads1.vip.scd.yahoo.com
server deny name radio1.launch.vip.dal.yahoo.com
server deny name in1.msg.vip.re2.yahoo.com
server deny name data1.my.vip.sc5.yahoo.com
server deny name address1.pim.vip.mud.yahoo.com
server deny name edit.messenger.yahoo.com
server deny name messenger.yahoo.com
server deny name http.page.yahoo.com
server deny name privacy.yahoo.com
server deny name csa.yahoo.com
server deny name csb.yahoo.com
server deny name csc.yahoo.com
audit-trail on
!
!
voice-card 0
no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
class-map match-any sdm_p2p_kazaa
match protocol fasttrack
match protocol kazaa2
class-map match-any sdm_p2p_edonkey
match protocol edonkey
class-map match-any sdm_p2p_gnutella
match protocol gnutella
class-map match-any sdm_p2p_bittorrent
```

```
match protocol bittorrent
!
!
policy-map sdmappfw2p_SDM_HIGH
    class sdm_p2p_gnutella
        drop
    class sdm_p2p_bittorrent
        drop
    class sdm_p2p_edonkey
        drop
    class sdm_p2p_kazaa
        drop
!
!
!
!
!
!
!
interface FastEthernet0/0
    description $FW_INSIDE$
    ip address 172.22.2.1 255.255.255.0
    ip access-group 100 in
    duplex auto
    speed auto
!
interface FastEthernet0/1
    no ip address
    shutdown
    duplex auto
    speed auto
!
interface Serial0/3/0
    description $FW_OUTSIDE$
    ip address 172.22.3.2 255.255.255.0
    ip access-group 101 in
    ip verify unicast reverse-path
    ip inspect SDM_HIGH out
    no fair-queue
    clock rate 64000
    service-policy input sdmappfw2p_SDM_HIGH
    service-policy output sdmappfw2p_SDM_HIGH
!
interface Serial0/3/1
    no ip address
    shutdown
    clock rate 125000
!
```

**294 Chapter 10 Access Lists**

```
!
!
ip http server
no ip http secure-server
!
access-list 100 remark auto generated by SDM firewall configuration
access-list 100 remark SDM_ACL Category=1
access-list 100 deny    ip 172.22.3.0 0.0.0.255 any
access-list 100 deny    ip host 255.255.255.255 any
access-list 100 deny    ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
access-list 101 remark auto generated by SDM firewall configuration
access-list 101 remark SDM_ACL Category=1
access-list 101 deny    ip 172.22.2.0 0.0.0.255 any
access-list 101 permit icmp any host 172.22.3.2 echo-reply
access-list 101 permit icmp any host 172.22.3.2 time-exceeded
access-list 101 permit icmp any host 172.22.3.2 unreachable
access-list 101 deny    ip 10.0.0.0 0.255.255.255 any
access-list 101 deny    ip 172.16.0.0 0.15.255.255 any
access-list 101 deny    ip 192.168.0.0 0.0.255.255 any
access-list 101 deny    ip 127.0.0.0 0.255.255.255 any
access-list 101 deny    ip host 255.255.255.255 any
access-list 101 deny    ip host 0.0.0.0 any
access-list 101 deny    ip any any log
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
  login
!
scheduler allocate 20000 1000
!
```

```
webvpn context Default_context
  ssl authenticate verify all
  !
  no inservice
  !
  !
end

RouterB#
```

Looking at the configuration, it is easy to see how much time the SDM can save in the configuration of a router. Without the firewall wizard, an administrator would have to manually type each of the commands shown above into the CLI of the firewall router. As Cisco continues to expand the use of the SDM, it will become a vital tool for anyone who works with Cisco devices.

---

## Chapter Summary

- Access lists are one of the most important IOS tools for controlling network traffic and security.
- Access lists are created in a two-step process. First, you create the list in global configuration mode, using the specific syntax of the type of list you want to create. Then, you apply the list to an interface in interface configuration mode to make it active.
- All access lists are created sequentially and applied sequentially to all packets that enter an interface where the list is applied.
- By default, access lists always end in an `implicit deny any` statement, which will drop any packet that does not meet an access list criterion.
- Only one access list per direction (inbound or outbound) per protocol can be applied to an interface.
- Standard IP access lists allow you to filter traffic based on the source IP address of a packet. They should be applied to an interface as close to the destination as possible to avoid accidentally blocking valid traffic.
- Extended IP access lists filter traffic based on source, destination, protocol type, and application type. They allow for more specific control over network traffic. They should be placed as close to the source as possible to keep unnecessary traffic from getting onto the internetwork.
- Access lists can be used to restrict telnet by controlling VTY line access. This is usually done using a single-permit access list line. The list is applied using the `access-class` command. The list is placed on the device to which telnet is being restricted.
- Ranges of numbers represent all access lists. Table 10-3 summarizes the numbers associated with each type of list you need to be familiar with to pass the CCNA exam.

| Access List Type         | Number  |
|--------------------------|---------|
| Standard IP access lists | 1–99    |
| Extended IP access lists | 100–199 |

**Table 10-3** Access list number ranges

- The SDM can be used to configure both standard and extended ACLs via the Additional Tasks configuration tab.
- The SDM can be used to configure a router as either a Basic or Advanced firewall.
- The main difference between a Basic and Advanced firewall is the ability to configure DMZ interfaces in the Advanced firewall setup wizard.

## Key Terms

**access lists** Permit or deny statements that filter traffic based on criteria such as source address, destination address, and protocol type.

**any** A keyword used to represent all hosts or networks; replaces 0.0.0.0 255.255.255.255 in an access list.

**established** A keyword that requires traffic to have originated inside the trusted network.

**extended IP access lists** IP access lists that filter traffic by source IP address, destination IP address, protocol type, and port number.

**host** A keyword for an extended IP list that specifies that an address should have a wildcard mask of 0.0.0.0.

**implicit deny any** Blocks all packets that do not meet the requirements of the access list. Exists at the end of all lists.

**inbound** A direction parameter used when applying an access list. Direction is into the router.

**inverse mask** See **wildcard mask**.

**named access list** An access list that uses names instead of number ranges.

**outbound** A direction parameter used when applying an access list. Direction is out of the router.

**partial masking** When an octet in a wildcard mask contains a mix of binary 1s and 0s.

**standard IP access lists** Access lists that filter traffic based on source IP address.

**wildcard mask** Applied to IP addresses to determine if an access list line will act upon a packet. Zeros are placed in positions deemed significant, and 1s are placed in nonsignificant positions.

## Review Questions

1. Which wildcard mask would apply an access list line to all packets from network 175.25.0.0?
  - a. 255.255.255.0
  - b. 255.255.0.0
  - c. 255.254.0.0
  - d. 0.0.255.255

2. Standard IP access lists filter traffic based on which of the following? (Choose all that apply.)
- destination IP address
  - IP protocol
  - port number
  - source IP address
3. Wildcard masks use a \_\_\_\_\_ to signify which bits of an address are significant.
4. Which command shows only the IP access lists on a router?
- show access-lists
  - show ipx access-lists
  - show ip access-lists
  - show interface
5. Which commands allow you to view the interfaces that have IP access lists applied to them? (Choose all that apply.)
- show interfaces
  - show ip interface
  - show ip traffic
  - show ip counters
6. Which host and wildcard mask pair does the any keyword represent?
- |                    |                 |
|--------------------|-----------------|
| a. 255.255.255.255 | 0.0.0.0         |
| b. 0.0.255.255     | 0.0.0.0         |
| c. 0.0.0.0         | 0.0.0.0         |
| d. 0.0.0.0         | 255.255.255.255 |
7. Which command is used to apply an IP access list to an interface?
- ip access-group [list #] [in/out]
  - ip access-group permit 100
  - ip access-group [list #] [permit/deny]
  - show ip interface
8. Access lists are \_\_\_\_\_. (Choose all that apply.)
- used to filter traffic and control network security
  - applied as either inbound or outbound filters
  - sequential permit or deny statements
  - built into the router's firmware
9. Standard IP access lists are represented by the \_\_\_\_\_ number range.
- 100–199
  - 1–99
  - 1000–1099
  - 200–299

**298** Chapter 10 Access Lists

10. Which command could be used to remove an access list from your router?
  - a. no ip access-group in
  - b. no ip access-list 1 in
  - c. no access-list 1
  - d. no ip access-list one
11. Extended IP access lists are represented by the \_\_\_\_\_ number range.
  - a. 100–199
  - b. 200–299
  - c. 1000–1099
  - d. 1–99
12. The show access-lists command displays \_\_\_\_\_.
  - a. access lists applied to interfaces
  - b. all access lists on the router
  - c. only IP access lists on the router
  - d. only IPX access lists on the router
13. At which of the following prompts would you create an access list?
  - a. routerC#
  - b. routerC>
  - c. routerC(config-if)#
  - d. routerC(config)#
14. At which of the following prompts would you apply an access list to an interface?
  - a. routerC#
  - b. routerC>
  - c. routerC(config-if)#
  - d. routerC(config)
15. Which of the following host and corresponding wildcard mask pairs represent the same value as host 172.29.2.2?

|                    |                 |
|--------------------|-----------------|
| a. 0.0.0.0         | 255.255.255.255 |
| b. 172.29.2.2      | 0.0.0.0         |
| c. 255.255.255.255 | 0.0.0.0         |
| d. 0.0.0.0         | 172.29.2.2      |
16. A router can have one access list per protocol, per direction on each interface. True or False?
17. Which of the following is a benefit of using named lists?
  - a. The syntax is identical to using numbered lists.
  - b. Fewer lists are allowed, so it is easier to remember them.

- c. You are not constrained by the 100 lists per filter type limit.
  - d. Using named lists offers no benefits.
18. What happens if a list is applied to an interface and then the list itself is removed?
- a. The commands will be executed and all traffic will be denied.
  - b. The commands will be executed and all traffic will be permitted.
  - c. The commands will not be executed and all traffic will be permitted.
  - d. None of the above
19. What is true of the host keyword? (Choose all that apply.)
- a. It can only be used with extended IP lists.
  - b. It can be used with standard and extended IP lists.
  - c. It replaces the 0.0.0.255 wildcard mask.
  - d. It replaces the 0.0.0.0 wildcard mask.
  - e. It is placed before the IP address with which it is associated.
  - f. It is placed after the IP address with which it is associated.
20. What is the purpose of the “established” parameter?
- a. to establish a connection between the sender and receiver
  - b. to prevent any traffic into a network
  - c. to prevent any traffic into a network that did not originate from that network
  - d. to permit all TCP traffic but not IP traffic into the established network
21. All access lists presented in this chapter, except standard IP lists, should be placed where?
- a. as close to the source as possible
  - b. as close to the destination as possible
  - c. as close to the serial interface as possible
  - d. as close to the tftp server as possible
22. Which command links an access list to the VTY lines?
- a. ip access-group
  - b. ip access-class
  - c. vty access-class
  - d. access-class
23. Which SDM wizard allows you to configure a DMZ?
- a. Firewall configuration wizard
  - b. Security configuration wizard
  - c. Basic Firewall Wizard
  - d. Advanced Firewall Wizard
24. List the three Basic Firewall Wizard security settings.
25. The SDM cannot be used to create complex access control lists. True or False?

## Case Projects



1. Freytech Industries has hired you and your team at Winslow Networks to help with an important network project. They want to block HTTP traffic from network 170.55.0.0 to their Web server at 164.106.105.3. Lisa suggests the following list:

```
access-list 10 deny 170.55.0.0  
access-list 10 permit any
```

What will Lisa's list do? Modify the list so that it will work for your client.

2. You have been asked to deliver a speech on the ability of access lists to control access to VTY lines. Describe how you would limit access to the VTY lines to a single management workstation at IP address 173.13.6.1/24. Also, describe how you would limit access to the 173.13.6.0 subnet only.
3. During the last departmental meeting, your manager asked you to create a firewall router for the company's network. In particular, she wants all peer-to-peer networking and instant messaging services to be unable to connect to the internet from the company LAN. A co-worker in the meeting stated that it would take hours to accomplish this task. However, you know it will not take long using the SDM. Prepare a short paragraph describing why this task will be easy to accomplish with the SDM.



# 11

chapter

## PPP and Frame Relay

**After reading this chapter and completing the exercises, you will be able to:**

- Describe PPP encapsulation
- Configure PPP encapsulation and its options
- Describe and enable PPP multilink
- Understand Frame Relay standards and equipment
- Describe the role of virtual circuits and performance parameters in Frame Relay
- Understand the Frame Relay topologies
- Understand the difference between multipoint and point-to-point configurations
- Configure and monitor Frame Relay

## **WAN technologies typically define Physical and Data Link layer connections**

between devices. PPP and Frame Relay are both Data Link layer encapsulation types implemented on a router. In this chapter, you will learn about PPP and Frame Relay. In addition, the chapter covers the format of PPP data frames, Frame Relay terms, specifications, and service types. Finally, the chapter demonstrates how to implement and configure PPP and Frame Relay connections on Cisco routers.

## **PPP**

PPP is an Internet standard protocol defined in RFCs 2153 and 1661. The IETF defined PPP to provide point-to-point, router-to-router, host-to-router, and host-to-host connections. PPP is considered a peer technology based on its point-to-point physical configuration. It is commonly used over dial-up or leased lines to provide connections into IP networks. PPP also supports other Network layer protocols such as Novell IPX and AppleTalk. Due to its flexibility, PPP is the most widely used WAN connection method today.

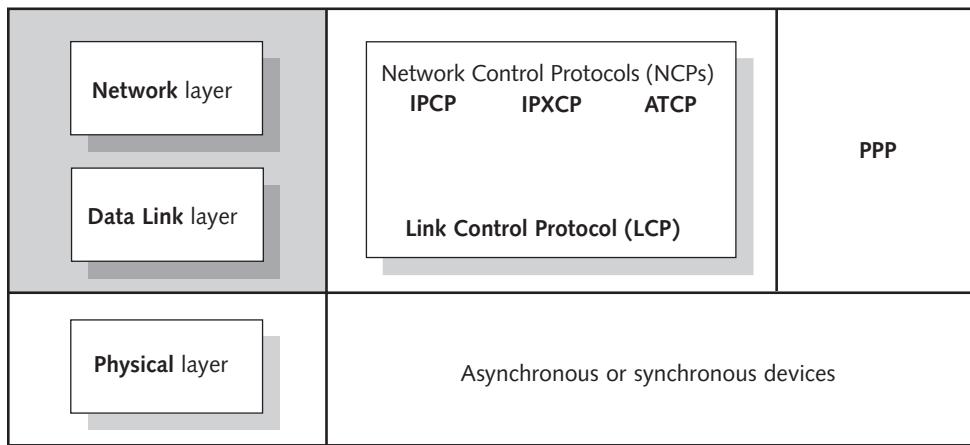
Serial Line Internet Protocol (SLIP) was the predecessor to PPP; it only supports TCP/IP connections. In addition, SLIP offers no encryption, compression, or error correction. It is an analog protocol limited to 56-Kbps transmission. PPP overcomes all of SLIP's limitations. Other advantages offered by PPP are the capability to handle asynchronous as well as synchronous communication. PPP is also more efficient and supports more protocols and interfaces. PPP can be used over several different physical interfaces, including:

- Asynchronous serial
- ISDN synchronous serial
- High-Speed Serial Interface (HSSI)

Asynchronous serial connections are typically used with analog modems, which connect directly to the existing phone lines and outlets that are wired in residential areas throughout the United States. ISDN synchronous serial connections require the use of ISDN modem equipment to interface with the Integrated Services Digital Network (ISDN) provided by many public carriers. **High-Speed Serial Interface (HSSI)** is a type of serial device that was developed by Cisco and T3Plus Networking. It defines a serial connection that operates at speeds of up to 52 Mbps over distances of up to 15 meters (50 feet).

## **PPP in the Protocol Stack**

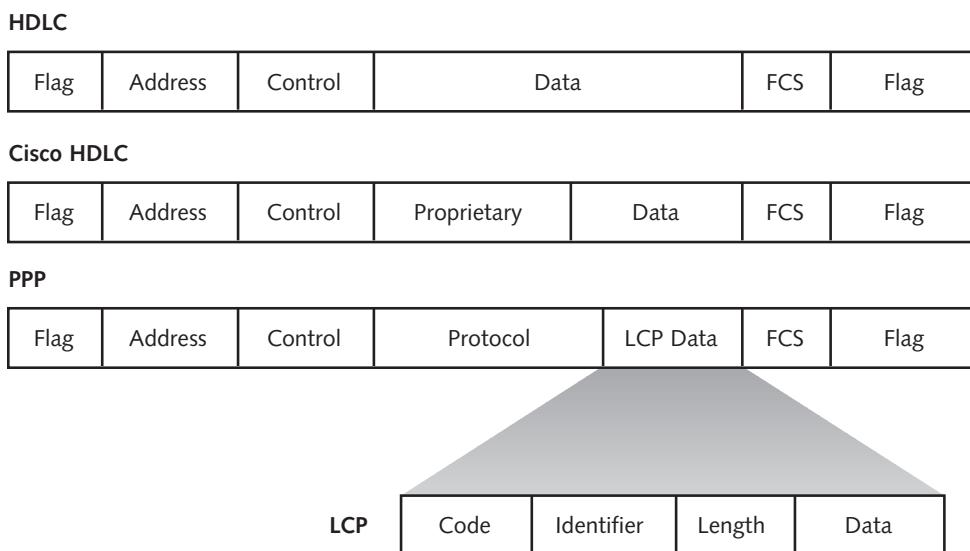
Most WAN protocols operate at the Data Link layer of the OSI model. As mentioned, you can use PPP over both asynchronous and synchronous connections at the Physical layer of the OSI reference model. The **Link Control Protocol (LCP)** is used at the Data Link layer to establish, configure, and test the connection. PPP also relies on Network layer services called **Network Control Protocols (NCPs)** at layer 3 of the OSI model. NCPs allow the simultaneous use of multiple Network layer protocols and are required for each protocol that uses PPP. Examples of NCPs include **IP Control Protocol (IPCP)**, **IPX Control Protocol (IPXCP)**, and **AppleTalk Control Protocol (ATCP)**. Figure 11-1 illustrates the location of PPP in the protocol stack; notice that the NCPs function at the Network layer.



**Figure 11-1** PPP in the protocol stack

## Frame Format

PPP, like many WAN technologies, is based on the **High-Level Data Link Control (HDLC)** protocol. The difference between PPP frames and HDLC frames is that PPP frames contain protocol and Link Control Protocol (LCP) fields, as shown in Figure 11-2. The Protocol field allows PPP to simultaneously support multiple protocols by allowing it to indicate which protocol it is encapsulating. PPP uses the LCP field to establish, configure, maintain, and terminate connections.



**Figure 11-2** HDLC and PPP packet structure

Figure 11-2 also shows the Cisco proprietary HDLC frame. Cisco HDLC has proprietary fields that support the encapsulation of multiple protocols. Cisco's HDLC is the default

encapsulation type for serial interfaces on Cisco routers. The elements of the PPP frame are as follows:

- *Flag*—Binary sequence 01111110, which indicates the beginning of the frame
- *Address*—Binary sequence 11111111; because PPP is used to create a point-to-point connection, there is no need for PPP to assign an individual address for each host.
- *Control*—Binary sequence 00000011, which indicates that the transmission of user data will not be sequenced and is to be delivered over a connectionless link
- *Protocol*—Two bytes used to identify the protocol that is encapsulated
- *LCP (or Data)*—The LCP information and the data that has been encapsulated from the higher layers. The default size of this field is 1500 bytes, but PPP implementations can negotiate a larger size for this field. LCP is explained in greater detail in the following section.
- *Frame Check Sequence (FCS)*—Two bytes by default, but can be as large as four bytes; uses a cyclical redundancy check (CRC) to verify the integrity of the frame and ensure that it was not corrupted during transmission
- *Flag*—Binary sequence 01111110 that identifies the end of the data frame

**LCP** LCP is described in RFCs 1548, 1570, 1661, 2153, and 2484. RFC 1661, which made RFC 1548 obsolete, describes PPP organization and methodology, including basic LCP extensions. RFC 1661 was later updated by RFC 2153, which explains PPP Vendor extensions. RFC 1570 and its update, RFC 2484, further expand the definition of LCP extensions. The LCP field of the PPP packet can contain many different pieces of information, including:

- *Asynchronous character map*—Allows PPP to encode its transmission properly for the recipient host
- *Maximum receive unit size*—Sets the receive buffer size for the LCP connection, typically 1500 bytes
- *Compression*—Indicates the type of compression used. Data compression that can be performed on the PPP packet at the source and then uncompressed at the destination; typically improves the speed of data transfer over slow serial connections because less data has to traverse the connection.
- *Authentication*—Specifies whether a password is required to establish the PPP connection. Two authentication protocols are available: **Password Authentication Protocol (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**. Authentication is described in greater detail in the following section.
- *Magic number*—Aids in detecting links that are in the looped-back condition. When interfaces are looped back, data that is sent out the interface is immediately received on that interface. Magic numbers are unique numbers added by the router to a packet, which allow it to detect a looped-back link. If the router receives a packet that contains its own unique magic number, it detects that the interface is looped back. Loopback is typically used for testing interfaces to ensure they are sending and receiving data. The **loopback command** can be run from the interface configuration prompt. Although good for testing, looped-back interfaces are undesirable in production environments. In a production environment, you can use the **down-when-looped** command from

interface configuration mode, which will automatically shut down that interface when looping is detected.

- *Link Quality Monitoring (LQM)*—Checks the reliability of the link by monitoring the number of errors, latency between requests, connection retries, and connection failures on the PPP link
- *Multilink*—Allows multiple transmission devices to send data over separate physical connections. The benefit of multilink is that you can combine the bandwidth of two separate devices over one logical connection. For example, two 64-Kbps ISDN channels can be combined to provide an effective throughput of 128 Kbps. PPP will fragment, sequence, and reassemble these packets to provide faster throughput over multiple slow serial connections. Multilink is defined in RFC 1717; you can enable multilink with the `ppp multilink` command from the interface configuration mode.

**LCP Link Configuration** The LCP link configuration process modifies and enhances the default characteristics of a PPP connection. This part of the link configuration process manages the link, controls the authentication, and can be used to set link quality. The LCP link configuration process includes the following actions:

- *Link establishment*—PPP must open and configure the PPP connection before any data can be transferred over the link.
- *Authentication (optional)*—CHAP or PAP can be used to verify the identity of the devices that are establishing the connection. CHAP and PAP are discussed in greater detail later in this chapter.
- *Link-quality determination (optional)*—Checks the quality of the link and monitors its reliability
- *Network layer protocol configuration negotiation*—Identifies the appropriate Network layer protocol for the connection; the devices negotiate to use a protocol that is common to both.
- *Link termination*—When the call is complete, or the specifications defining the call are no longer met, the call is terminated.

11

## Establishing PPP Communications

Three of the five link configuration actions defined in the preceding list are involved in establishing PPP communications: link establishment, optional authentication, and Network layer protocol configuration negotiation. The link establishment phase involves the configuration and testing of the data link. As mentioned earlier, PPP connections may use the information contained in the LCP portion of the PPP packet to configure the link by passing requirements for maximum transmission units and compression.

The second phase of the establishing process is optional. The authentication process can use two authentication types with PPP connections: PAP and CHAP. Most network administrators configure their devices to use CHAP because it is the stronger authentication method of the two. RFC 1994 documents the PAP and CHAP authentication protocols.

PAP uses a simple two-way handshake method to establish the link. In this link, PPP transmits a clear text username and password across the link between hosts to establish the link. The device attempting to establish the link transmits the username and password, so that the destination host will allow the PPP session. PPP only conducts PAP authentication during initial link establishment.

Compared with PAP, CHAP provides a much more sophisticated authentication process. Like PAP, CHAP provides username and password authentication service during the initial link establishment. However, CHAP employs a three-way, rather than two-way handshake. Once the link is established, the local router queries the remote host with a packet known as a **challenge**. The challenge is in the form of a unique encryption key. The remote host uses the encryption key to encode the username and password. The router compares the decrypted username and password and looks for a match with its username and password. It then either accepts or drops the connection based on whether the comparison yields a matching username and password.

After the connection is made, CHAP can continue this query process, using a different encryption key each time and using unique and unpredictable intervals. This further ensures that connections are legitimate because it prevents someone from capturing the data packets that are exchanged during the initial authentication process between two authorized systems and then playing those data packets from an unauthorized system in an attempt to gain PPP access to the server.



The router typically controls the authentication process, but a **Terminal Access Controller Access Control System (TACACS)**, **RADIUS server**, or third-party authentication server can also be used to centralize management of CHAP authentication and other security features.

PPP is an encapsulation type for serial interface communications. Therefore, to configure a PPP connection, you must access the interface configuration mode for the specific interface you want to configure. For example, if you want to configure PPP on the first serial interface of the router (S0/0), you would use the commands shown in Figure 11-3 (assuming that the router was already in enable mode).

```
router#config t
router(config)#int s0/0
router(config-if)#encap ppp
```

**Figure 11-3** Enabling PPP

The third phase of the establishing process is Network layer protocol configuration negotiation. After LCP has finished negotiating the configuration parameters, Network layer protocols can be configured individually by the appropriate NCP. At this point, packets can be sent over the link. The different protocols can be established and terminated at any time.

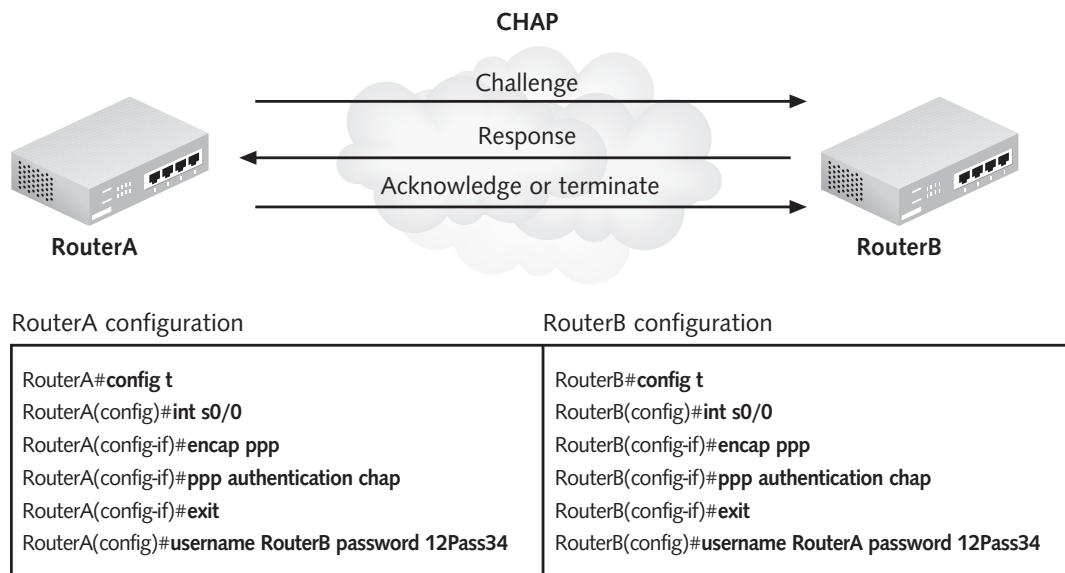
**Configuring PPP Authentication** As mentioned previously, using authentication with PPP connections is optional. Therefore, you must specifically configure PPP authentication on each PPP host in order for the host to use it. You can choose to enable CHAP, PAP, or both on your PPP connection, in either order. For example, to set the router to first use CHAP, and then to go to PAP (assuming that CHAP is not available), you would type the command shown in Figure 11-4.

```
router(config-if)#ppp authentication chap pap
```

**Figure 11-4** Enabling both CHAP and PAP authentication

If you entered that command, your local router would request CHAP authentication during the connection, but if the other device did not support CHAP or attempted PAP authentication instead, then PAP would be tried. You could also decide to use just CHAP or just PAP by omitting the undesired method from the command line.

Once you set the authentication type, you must still configure a username and password for the authentication. To do so, you must exit interface configuration mode and enter global configuration mode. Type `username` followed by the host name of the remote router, then type `password` followed by the password for that connection. Ensure that each router uses the same password, but uses the other router's host name after `username`. The link will go up and down (flapping) until both ends of the point-to-point link are configured correctly. Figure 11-5 illustrates a configuration and the commands required for that configuration to operate using CHAP authentication.



**Figure 11-5** Configuring CHAP

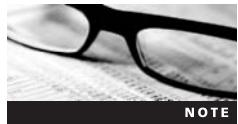
If you want to configure the same host name and password for CHAP authentication on several routers, you can do so via the interface configuration mode prompt. For example, if you wanted to configure the host name `flagstaff` and set the password to `lumberjack` for all routers, you would enter the commands in Figure 11-6 on all routers' PPP interfaces.

```
router(config-if)#ppp chap hostname flagstaff
router(config-if)#ppp chap password lumberjack
```

**Figure 11-6** Configuring PPP and CHAP

In this example, the host name `flagstaff` sets the alternate CHAP host name to `flagstaff`. The password `lumberjack` part of the command sets the default CHAP password to `lumberjack`. This type of configuration is easier to implement than the one shown in

Figure 11-5, in which you must configure each router with the same password, but with opposite host names.



If you are using PAP authentication with Cisco IOS Releases 11.1 or later, you must enable PAP on the interface of the router to receive the PAP request.

**NOTE**

**Confirming PPP Communications** Once you have completed configuring your PPP interface, you can verify the changes using the show interface command. You must be in privileged EXEC mode to view the interfaces. For example, if you want to view your configuration on the Serial 0/1 interface, type the following:

```
Router#show interface S0/1
```

## Frame Relay Standards and Equipment

Frame relay is a packet switching and encapsulation technology that functions at the Physical and Data Link layers of the OSI reference model. Frame relay is a communications technique for sending data over high-speed digital connections operating at anywhere from 56 Kbps to 44.736 Mbps or higher. A streamlined version of the older X.25 technology, Frame Relay is more efficient and faster because it does not perform the error checking that was present in X.25. Frame relay also provides cost-effective access to remote facilities because one site can connect to multiple remote sites using a single connection. The International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) and the American National Standards Institute (ANSI) define Frame Relay as a connection between the data terminal equipment (DTE) and the data communications equipment (DCE). DCE is switching equipment supplied by a telecommunications provider that serves as a connection to the public data network (PDN). DTE is also known as customer premises equipment (CPE), because it is the equipment that belongs to, and is maintained by, the PDN customer. For example, if you connect your Cisco router to a **Frame Relay switch** (which is provided by the phone company), the Cisco router is the CPE and the Frame Relay switch is the DCE, as shown in Figure 11-7.



The ITU-T was formerly known as the **Consultative Committee on International Telephony and Telegraphy (CCITT)**, which is the primary international organization for fostering cooperative standards for telecommunications equipment and systems.

Router (a.k.a. CPE or DTE)



Frame Relay connection



Frame Relay switch  
(a.k.a. DCE)

Public data network (PDN)

**Figure 11-7** CPE to DCE connection

The physical equipment that is used on a network may vary from one organization to another. For example, some networks may use a separate router and channel service unit/data service unit (CSU/DSU) to make their WAN connections. Figure 11-8 shows a CSU/DSU that is used with a Cisco 2501 router to make the connection. The CSU/DSU is at the customer location of the digital connection. The unit is used for encoding, filtering, and translating communications to and from the digital line.



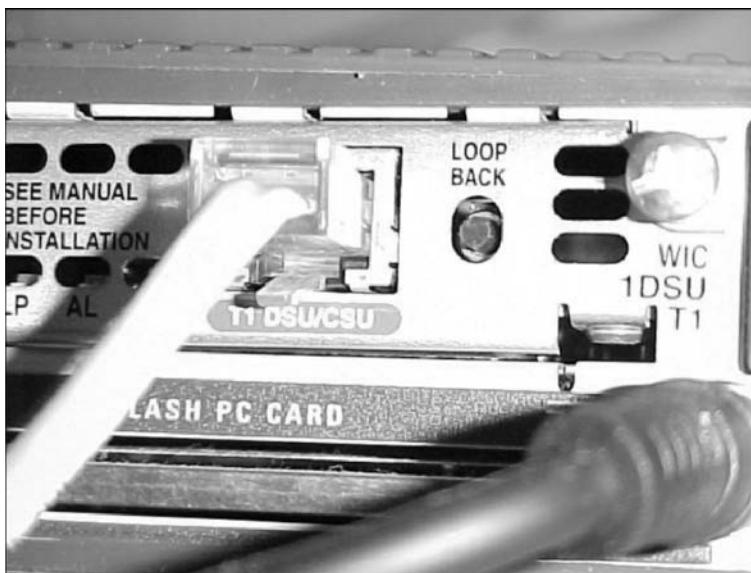
**Figure 11-8** CSU/DSU and router

Some routers have built-in cards that allow them to make WAN connections. For example, in Figure 11-9, you can see a T1 CSU/DSU card built into the router. The router in the picture is a Cisco 1600 series router. Notice that a T1 line connects directly to the CSU/DSU on the back of the router.



The order of the term—CSU/DSU or DSU/CSU—is unimportant, because both forms refer to the same device. The ordering is a matter of personal preference.

11



**Figure 11-9** CSU/DSU connection

In Frame Relay connections, the network device that connects to the Frame Relay switch is known as a **Frame Relay access device (FRAD)**; you may also see this defined as **Frame Relay assembler/disassembler**. The Frame Relay switch is also called the **Frame Relay network device (FRND)**, which is pronounced “friend.” The network administrator typically handles the local connection up to the point that it enters the PDN. Items that are part of the PDN, including the Frame Relay switch, fall under the control and responsibility of the telecommunications provider.

## Virtual Circuits

You can use Frame Relay with nearly any serial interface. It operates by multiplexing, which means that it combines multiple data streams onto one physical link. Frame relay separates each data stream into logical (software-maintained) connections called virtual circuits, which carry the data transferred on the connection. These virtual circuits are multiplexed onto the physical channel. Two types of virtual circuits, switched virtual circuits (SVC) and permanent virtual circuits (PVC), connect Frame Relay ports. SVCs, which are the less common of the two, are controlled by software and are only active while a connection to the WAN is active. The SVC software automatically dials the WAN, establishing and terminating the connection as required to transfer data over the Frame Relay service. PVCs remain permanently connected to the WAN. The network administrator manually defines the PVC; it remains until the network administrator removes it.

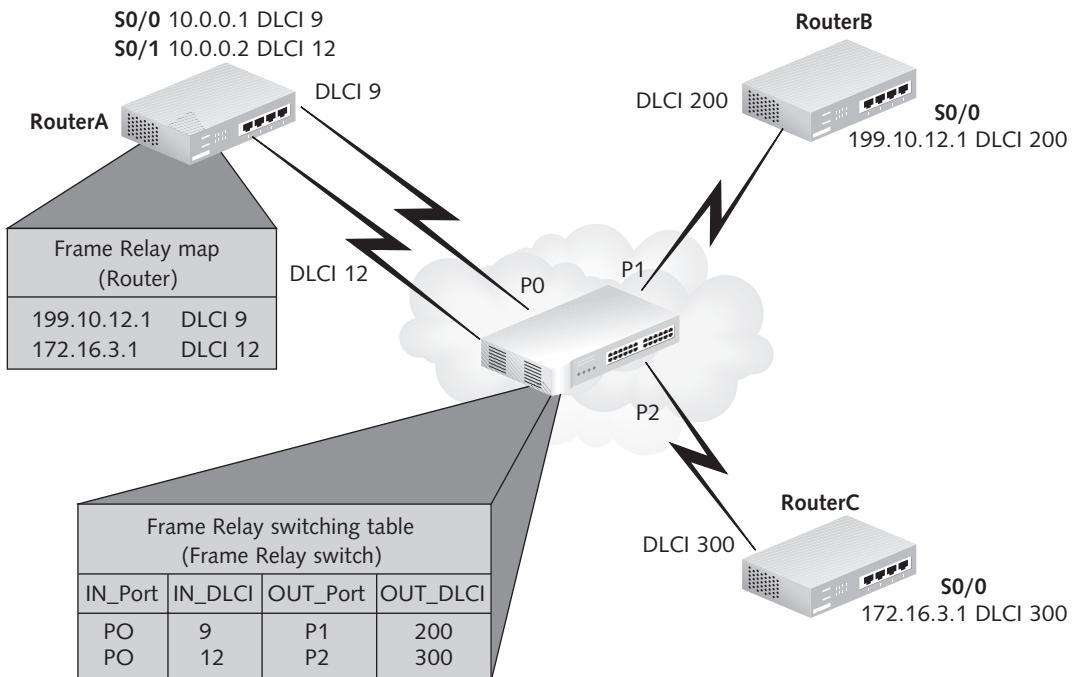
### DLCI

Frame relay connections identify virtual circuits by Data Link Connection Identifier (DLCI) numbers. The DLCI (pronounced *dell-see*) numbers map virtual circuits to layer 3 protocol addresses. For example, a DLCI number associates an IP address with a specific virtual circuit. DLCI numbers do not specify a physical port and are not unique identifiers on the network; instead, they have only local significance, which means they are important only to the local router and Frame Relay switch. DLCI numbers are usually assigned by the Frame Relay provider and are most likely not the same on either side of the Frame Relay switch. This is what is meant by “local significance.” The provider, which is usually the telco, controls how the DLCI switching occurs. Because DLCIs have only local significance, any available number can be selected for each end of a PVC at the time of subscription.

### Frame Relay Map

DLCI numbers are mapped, or assigned, to a specific interface. Each router that supports Frame Relay will have a **Frame Relay map**, which is a table in RAM that defines the remote interface to which a specific DLCI number is mapped. The definition will contain a DLCI number and an interface identifier, which is typically a remote IP address. The Frame Relay map can be built automatically or statically depending on the Frame Relay topology. Various topologies are discussed later in the chapter.

Figure 11-10 shows a sample Frame Relay configuration. RouterA has two serial interfaces configured for Frame Relay. The first serial interface (S0/0) on RouterA is configured for DLCI 9, in order to form a virtual circuit between itself and RouterB. The second serial interface (S0/1) is configured for DLCI 12. It refers to a virtual circuit between RouterA and RouterC. The Frame Relay map shows which destination IP addresses are used with which DLCI numbers.



**Figure 11-10** Sample Frame Relay configuration

Notice that the **Frame Relay switching table** is configured to map its ports (P0, P1, and P2) to the correct DLCI numbers for the virtual connection. Each switching table entry consists of four elements: the incoming port on the switch, the incoming DLCI number, the outgoing port on the switch, and the outgoing DLCI number. The switching table in this example is simplified; in reality, the switch would be more complex and involve additional Frame Relay switches.

In the example, only the mapping table for RouterA is shown. In reality, however, each router configured for Frame Relay will have its own mapping table. Remember that DLCI numbers are only locally significant, so it would be possible for RouterA and RouterB to use the same DLCI number to specify a virtual circuit.

**Subinterfaces** In Figure 11-10, RouterA has two different serial interfaces, each configured for one virtual connection. In early implementations of Frame Relay, each PVC required its own dedicated serial interface. With current technology, however, a single router serial interface can now service multiple PVCs through a single physical serial interface. To allow a single serial interface to support multiple PVCs, the IOS divides the interface into logical subinterfaces.

Subinterfaces are created by referencing the physical interface followed by a period and a decimal number. For example, if Serial 0/0 had three subinterfaces, they would be referenced as S0/0.1, S0/0.2, and S0/0.3. Subinterfaces are not real physical interfaces; they are virtual interfaces associated with a physical interface. For the purposes of routing, however, subinterfaces are treated as physical interfaces. With subinterfaces, the cost of implementing multiple Frame Relay virtual circuits is reduced because only one port is required on the router. Also,

the network administrator has to configure and maintain fewer physical connections. Sample subinterface configurations are shown later in this chapter.

## LMI

Frame relay engineers designed Local Management Interface (LMI) in 1990 to enhance standard Frame Relay. The LMI basically extended the functionality of Frame Relay by:

- Making the DLCIs globally significant rather than locally significant
- Creating a signaling mechanism between the router and the Frame Relay switch, which could report on the status of the link
- Supporting multicasting

Providing DLCI numbers that are globally significant rather than just locally significant makes automatic configuration of the Frame Relay map possible (as explained in the following section). Global significance means that each site is given a DLCI number and that number is then used as the DLCI at the far end of any PVC terminating at that site. In this manner, you can look at the DLCI numbers on the PVCs at one site and know the IP address of the destination router.

LMI uses **keepalive packets** (sent every 10 seconds by default) to verify the Frame Relay link and to ensure the flow of data. The Frame Relay switch in turn provides the status of all virtual circuits and their respective DLCI numbers to the Frame Relay connectivity device. Each virtual circuit, represented by its DLCI number, can have one of three connection states:

- *Active*—The connection is working and routers can use it to exchange data.
- *Inactive*—The connection from the local router to the switch is working, but the connection to the remote router is not available.
- *Deleted*—No LMI information is being received from the Frame Relay switch; this can indicate that the connection between the CPE and DCE is not functional.

The Frame Relay switch reports this status information to the Frame Relay map on the local router. The status information is used by the Frame Relay connectivity devices to determine whether data can be transmitted over the configured virtual circuits. Without LMI, the Frame Relay map must be built statically in the routers. However, by making the DLCIs globally significant, LMI facilitates dynamic Frame Relay map tables through the use of the Inverse ARP protocol, described in the next section.

## Inverse ARP

As previously mentioned and illustrated in Figure 11-10, a Frame Relay map includes DLCIs and their corresponding remote IP addresses. In **multipoint** configurations, routers use the protocol Inverse ARP to send a query using the DLCI number to find a remote IP address. Multipoint and **point-to-point** configurations are discussed later in this chapter. As other routers respond to the Inverse ARP queries, the local router can build its Frame Relay map automatically. To maintain the Frame Relay map, routers exchange Inverse ARP messages every 60 seconds by default. Inverse ARP is on by default. LMI is required for Inverse ARP to work.



NOTE

If the remote router does not support Inverse ARP, the Frame Relay map will have to be maintained statically (built and updated manually by the network administrator). Do not confuse Inverse ARP with Reverse Address Resolution Protocol (RARP); RARP is used primarily on LANs to provide hosts that only have MAC addresses with IP addresses.

## Encapsulation Types

In the early days of Frame Relay, vendors and standards organizations worked separately to develop and define LMI. As a result, LMI has several different protocol encapsulation types that it can use for management communications. Different Frame Relay switches, CPE, and Frame Relay connectivity equipment employ or support different types of LMI encapsulation. Cisco routers, for example, support these types of LMI encapsulation:

- *cisco*—This LMI type was originally defined by four companies: DEC, Nortel, StrataCom, and Cisco. It allows for 992 virtual circuit addresses and uses DLCI 1023 as a management circuit, which transfers link and DLCI status messages. This is the default LMI encapsulation type on Cisco routers.
- *ansi*—ANSI standard T1.617 Annex-D provides for 976 virtual circuit addresses and uses DLCI 0 as the management circuit.
- *q933a*—ITU-T Q.933 Annex A, similar to ANSI T1.617 Annex-D, uses DLCI 0 as a management circuit.

Cisco routers (using IOS Release 11.2 or later) can “autosense” the LMI type used by the Frame Relay switch. If the Frame Relay responds with more than one LMI type, the Cisco router will automatically configure itself to use the last LMI type received. The network administrator can also manually configure the LMI type. This manual configuration is explained later in the chapter.

The basic LMI type has three information elements: report type, keepalive, and PVC status. The report type indicates whether the message is just a keepalive frame or a full status message. The Frame Relay devices send keepalive frames every 5 to 30 seconds (10 by default) to ensure that the link is still active. Full status messages contain DLCI status in addition to the keepalive information.

As stated, management circuits transfer DLCI status messages. Depending on your Frame Relay provider, these messages may contain all or some of the following information concerning the status of the virtual circuit:

- *New*—Used if a new DLCI connection has been configured
- *Active*—Used to indicate whether the virtual circuit is available for data transfer
- *Receiver not ready*—Used for flow control to indicate that the virtual circuit is congested; this option is not available in the q933a LMI type
- *Minimum bandwidth*—Indicates the minimum available bandwidth
- *Global addressing*—Used to give DLCI global significance, as described earlier
- *Multicasting*—Used to configure a group of destination addresses rather than a single address; the IEEE has reserved DLCI numbers 1019 through 1022 for this purpose. Frame relay devices use multicasting to make DLCI numbers globally significant by advertising them across the Frame Relay network.

- *Provider-Initiated Status Update*—Normally, the Frame Relay switch obtains PVC status information only when the CPE sends a full status message and requests status information for the other DLCI connections; this option allows the provider to initiate a status inquiry.

Not all Frame Relay providers support every piece of link status information. All current implementations provide the New and Active information, but support for other information varies by provider.



Frame relay does not provide error checking, as do other network protocols such as Synchronous Data Link Control (SDLC). This makes Frame Relay connections more efficient, but it also means that Frame Relay must rely on the upper-layer protocols, such as TCP, to provide error correction.

**Split Horizon** Split horizon is a routing technique that reduces the chance of routing loops on a network. A split horizon implementation prevents routing update information received on one physical interface from being rebroadcast to other devices through that same physical interface. People also refer to this rule as **nonbroadcast multiaccess (NBMA)**.

Although split horizon is useful for reducing routing loops, it can cause problems for Frame Relay routing updates. For example, consider a router (RouterA) that is connected to two other routers (RouterB and RouterC) through a single physical interface configured for different virtual circuits, as shown in Figure 11-11. This is a multipoint configuration, which is the default when configuring Frame Relay. Because of split horizon, RouterA would not be able to send router updates received from RouterB to RouterC, and vice versa.

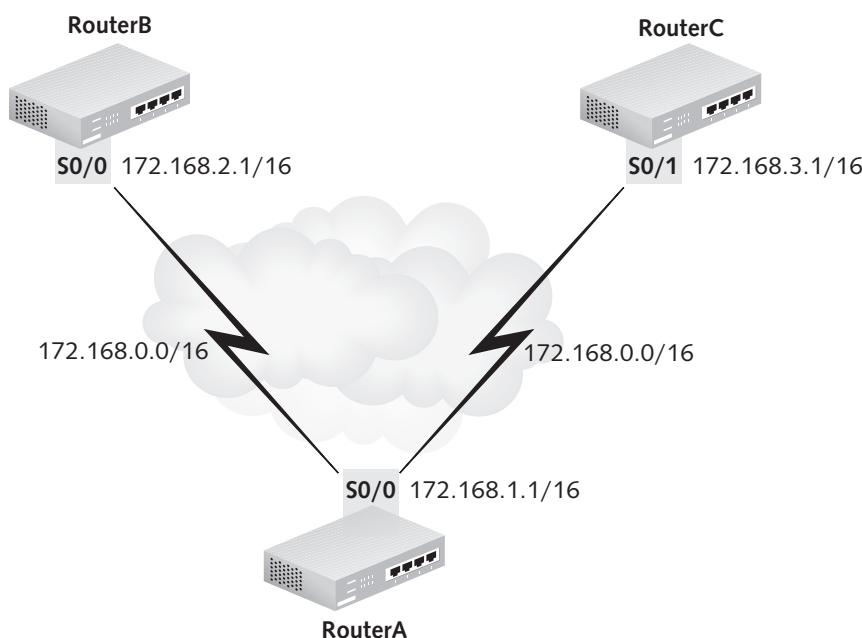
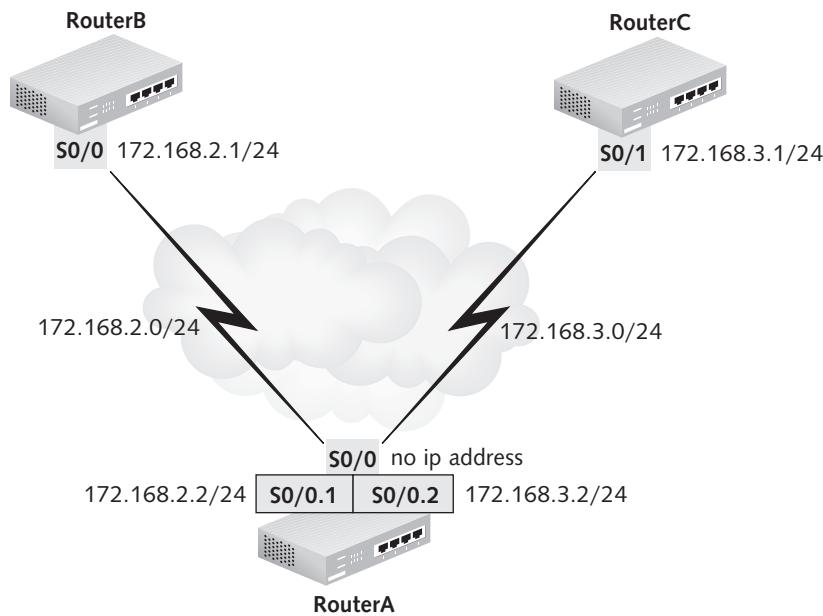


Figure 11-11 Split horizon problem

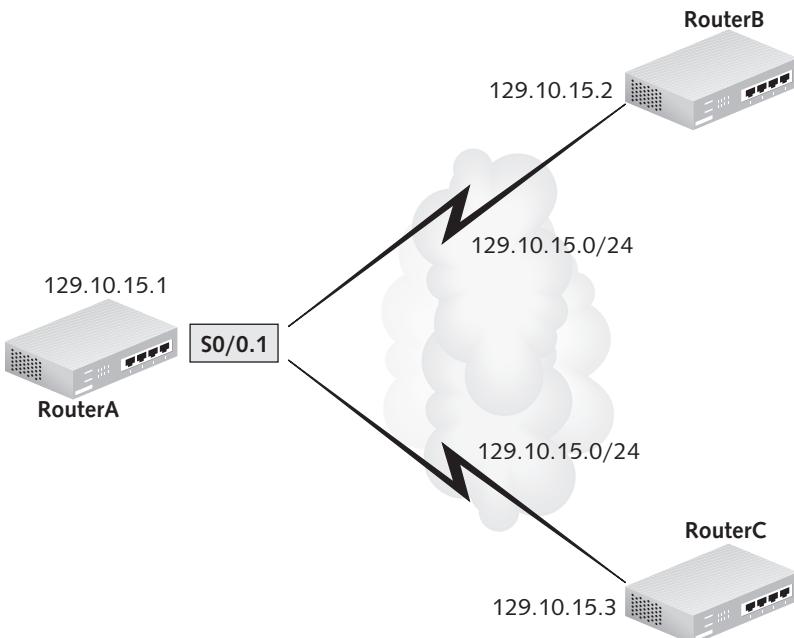
If the network is using IP, split horizon could be disabled on RouterA, which would solve the problem. However, disabling split horizon is not an option for IPX/SPX or AppleTalk. Furthermore, if the network administrator disables split horizon, the chance of getting routing loops on the network will be increased. The best solution is to configure separate point-to-point subinterfaces for each virtual connection, because the individual virtual circuits can be maintained and split horizon can remain on. Routing update information that is received through one subinterface can be propagated to other subinterfaces because they have different logical addresses.

As an example of this use of subinterfaces, examine Figure 11-12. It is the same as Figure 11-11, except that now the division of serial zero (S0/0) into subinterfaces S0/0.1 and S0/0.2 allows a different subnet identifier to be assigned to each virtual circuit. This allows router updates from RouterB to be transmitted to RouterC, and vice versa, because RouterA treats the subinterfaces as physically separate even though they are really only logically separate.



**Figure 11-12** Subinterfaces in use in a point-to-point configuration

The network administrator can configure each subinterface as a point-to-point connection or a multipoint connection. Point-to-point connections allow you to divide a single serial interface into multiple subinterfaces, each supporting a separate virtual connection. The network administrator must configure each subinterface with its own subnet identifier in a point-to-point configuration, as shown in Figure 11-12. In a multipoint configuration, the network administrator can configure a single interface or subinterface to support multiple connections to physical or logical interfaces on other routers. A multipoint configuration is still subject to the split horizon rule, because multiple Frame Relay connections on the same network are connected to a single logical interface. The only benefit to the multipoint configuration is that it allows you to use a single network for all of your routers, as shown in Figure 11-13.



**Figure 11-13** Single subinterface configured for multipoint connection

Notice that in Figure 11-13, the network uses the same subnet identifier for both virtual circuit connections. Note also that the routers all share the same subnet, identified by their first three octets.

## Performance Parameters

When organizations contract Frame Relay services from a telecommunications provider such as MCI, Sprint, AT&T, or one of the Regional Bell Operating Companies (RBOCs), the contract specifies parameters by which the connection is expected to function. Terms that appear in the contract may include:

- *Access rate*—The speed of the line, which indicates transfer rate. Common U.S. access rates are 56 Kps, 64 Kbps, and 128 Kbps, which are provided by Integrated Services Digital Network (ISDN) connections; and 1.544 Mbps, which is provided by T1 connections. Access rate is also known as the local access rate.
- *Committed Information Rate (CIR)*—The minimum transfer rate that the Frame Relay customer negotiates with the Frame Relay service provider. The service provider agrees to always allow the customer to transfer information at no less than the transfer rate specified by the CIR. This is usually lower than the access rate because the transfer rate may exceed the CIR during short bursts.
- *Committed Burst Size (CBS)*—The maximum amount of data bits that the service provider agrees to transfer in a set time period under normal conditions.
- *Excess Burst Size (EBS)*—The amount of excess traffic (over the CBS) that the network will attempt to transfer during a set time period. The network can discard EBS data, if necessary.

- **Oversubscription**—When the sum of the data arriving over all virtual circuits exceeds the access rate, the situation is called **oversubscription**. This can occur when the CIR is exceeded by burst traffic from the virtual circuits. oversubscription results in dropped packets. In such a case, the dropped packets must be retransmitted.

## Congestion

Frame relay switches attempt to control congestion on the network. When the Frame Relay switch recognizes congestion, it sends a forward explicit congestion notification (FECN) message to the destination router. This message tells the router that congestion occurred on the virtual circuit. In addition, the switch sends a backward explicit congestion notification (BECN) message to the transmitting, or source, router. The router's reaction to the BECN should be to reduce the amount of traffic it is sending.

A network administrator can configure certain types of traffic at the router as discard eligible (DE). Thus, during times of congestion, the router can discard DE frames to provide a more reliable service to frames that are not discard eligible. DE lists can be configured on a Cisco router to identify the characteristics of frames eligible for discard. These lists are created based on the protocol or the interface, as well as on other characteristics.

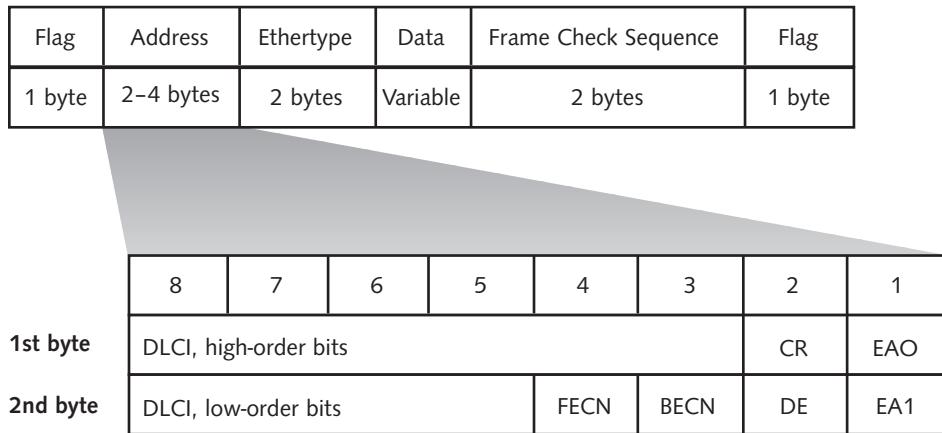
---

## Frame Format

Frame relay devices can use different Frame Relay frame formats. Because this course is focused on Cisco devices, this section will focus on the Cisco proprietary Frame Relay frame format, its Frame Relay frame structure, and the Address field of the frame.

Figure 11-14 shows the Frame Relay frame format, the basic frame structure, and an expanded look at the Address field of that structure.

11



**Figure 11-14** Frame Relay frame format

The Frame Relay frame format has the following specific parts:

- **Flag**—An eight-bit binary sequence (01111110) that indicates the start of the data frame
- **Address**—Two to four bytes that contain several pieces of Frame Relay information

**318** Chapter 11 PPP and Frame Relay

- *Ethertype*—Identifies the type of higher-layer protocol being encapsulated (IP, IPX, or AppleTalk); this data field is specific to the Cisco proprietary frame format
- *Data*—A variable-length field that contains the information from the higher layers encapsulated in the Frame Relay frame
- *FCS*—frame check sequence (FCS) or cyclical redundancy check (CRC), a mathematical computation placed at the end of the frame and used to ensure that the frame was not corrupted during transmission
- *Flag*—An eight-bit binary sequence (01111110) that indicates the end of the data frame

Although the Address portion of the Frame Relay frame can contain up to four bytes, Figure 11-14 displays only two bytes because that is the most common format. Three- and four-byte addressing varies only slightly from the structure of two-byte addressing. Refer back to Figure 11-14 as you read the descriptions for the bits of the Address field.

- *CR*—A command or response bit that is used for sending connection management and frame acknowledgment information between stations
- *FECN*—Setting used to alert receiving devices if the frame experiences congestion
- *BECN*—Setting used on frames traveling away from the congested area to warn source devices that congestion has occurred on that path
- *DE*—Discard eligible bit that is used to identify frames that are first to be dropped when the CIR is exceeded; Cisco routers allow you to set the DE bit for a particular virtual connection by DLCI number
- *EA*—Extension address bits that are used to extend the Address field from two bytes to either three or four bytes; they allow you to create additional DLCI numbers. For each EA bit that is turned on, one byte is added to the Address field.

Although the frame formats in Frame Relay vary slightly, the preceding information provides a thorough description. In addition to variety in Frame Relay formats, there is some variation in the topology that Frame Relay can use. In the next section you will explore different Frame Relay topologies.

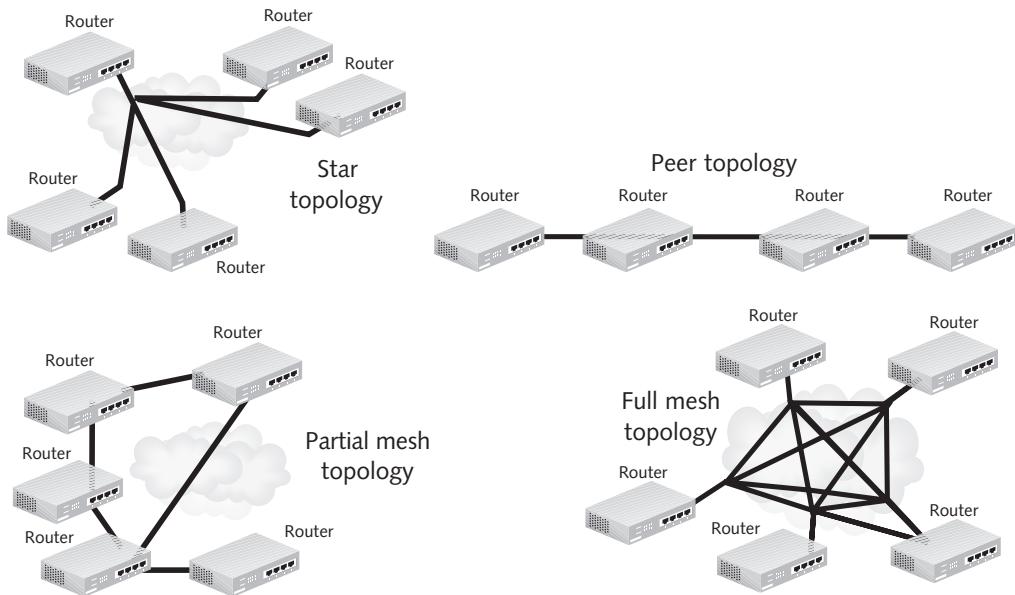
---

## Frame Relay Topologies

Frame relay can use many different WAN topologies: peer (point-to-point), star (hub and spoke), partial mesh, or full mesh physical topology. Figure 11-15 depicts the four common topologies used in Frame Relay.

The peer topology is like the bus LAN topology; nodes are simply strung along in a daisy-chained fashion. Very often, only two routers will be connected. This is the simplest WAN topology, and is the least expensive and easiest to configure. The disadvantage to the peer WAN topology is that a failure between nodes will affect the WAN; there is no redundancy.

The star is the most popular Frame Relay topology. One router functions as a central point, or hub, in a simple hierarchical configuration. All other devices are connected to the central router as spokes would connect to a hub. Typically the network administrator will configure the central router with a single interface that makes a multipoint connection to all other routers.



**Figure 11-15** WAN topologies

The full mesh is the most expensive topology to implement because each router has a direct connection to every other router. While this offers the most redundancy, it is extremely expensive to implement.

The partial mesh allows redundancy for critical connections while being less expensive than the full mesh. Essentially, any Frame Relay topology that is not a star or a full mesh is a partial mesh.

11

## Frame Relay Configuration

In this section, you will learn how to configure Frame Relay over serial interfaces using IP as the Network layer protocol. We will look at several examples, beginning with the simplest configuration and moving to successively more complex scenarios.

### Basic Multipoint Configuration with Two Routers

We begin with the easiest Frame Relay configuration: a multipoint connection between two routers in which the local and remote routers support LMI and Inverse ARP. In this case, LMI will notify the router about the available DLCI numbers and Inverse ARP will build the Frame Relay map dynamically.

Working from Figure 11-16, assume that you are responsible for configuring RouterA. RouterA is a Cisco router running IOS version 12.4, so it has the ability to autosense the LMI type. In addition, it automatically receives the DLCI information by querying the network. You only have to configure the serial interface for the correct IP address (129.10.15.1) and the subnet mask (255.255.255.0), and then configure it to support Frame Relay. Assume that the negotiated bandwidth of this connection is 56 Kbps and that you want to use the Routing Information Protocol (RIP) to pass the routing table updates between the routers.

## 320 Chapter 11 PPP and Frame Relay

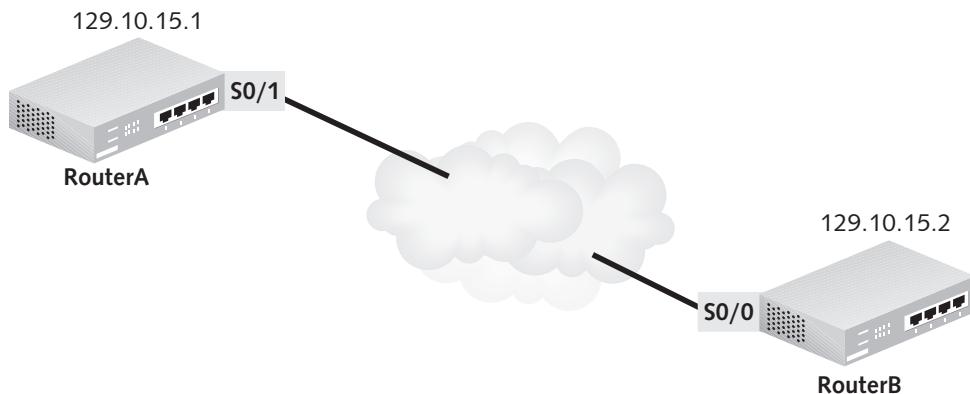
**Figure 11-16** Simple Frame Relay configuration

Table 11-1 lists the Cisco router prompts and commands that you will need to complete this configuration.

| Router prompts this:     | You type this:                             | Description                                                                                                                               |
|--------------------------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| RouterA>                 | enable                                     | Allows you to enter privileged EXEC (also called enable) mode. You will be prompted to enter the appropriate password after this command. |
| RouterA#                 | config terminal                            | Allows you to configure the router from the terminal line                                                                                 |
| RouterA(config)#         | int s0/1                                   | Tells the router to access interface serial 0/1 for configuration                                                                         |
| RouterA(config-if)#      | ip address<br>129.10.15.1<br>255.255.255.0 | Maps the interface serial 0/1 to the IP address and subnet mask shown                                                                     |
| RouterA(config-if)#      | encapsulation<br>frame-relay               | Sets the encapsulation for this port to Frame Relay using Cisco (the default). The other option is ietf.                                  |
| RouterA(config-if)#      | bandwidth<br>56                            | Sets the bandwidth for this port to 56 Kbps                                                                                               |
| RouterA(config-if)#      | exit                                       | Exits interface configuration mode                                                                                                        |
| RouterA(config)#         | router rip                                 | Enables the RIP for routing table updates                                                                                                 |
| RouterA(config-router) # | network 129.10.15.0                        | Enables RIP on the specified network address                                                                                              |

**Table 11-1** Basic router prompts and commands for configuring the multipoint example shown in Figure 11-16

The commands in Table 11-1 successfully configure RouterA for the connection shown in Figure 11-16.

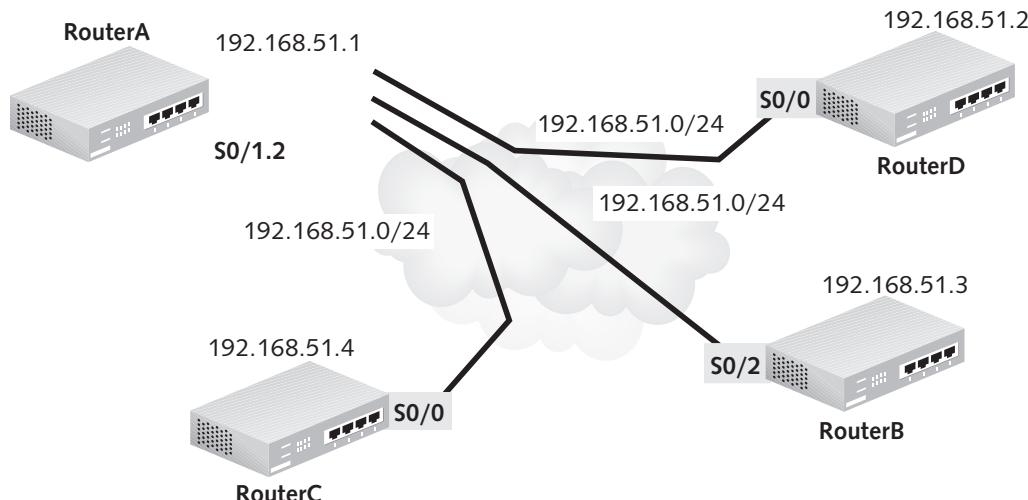
Now assume that you are the network administrator for RouterB and all the same information applies, except that your router is using IOS release version 11.0, which does not support automatic LMI sensing. To accommodate this new fact, you would have to enter the LMI type and, of course, different IP addresses. Also assume that the LMI type is ansi. With these conditions, the configuration commands for RouterB are shown in Figure 11-17.

```
RouterB#config t
RouterB(config)#int s0/0
RouterB(config-if)#ip address 129.10.15.2 255.255.255.0
RouterB(config-if)#encap fr
RouterB(config-if)#ban 56
RouterB(config-if)#frame-relay lmi-type ansi
RouterB(config-if)#ex
RouterB(config)# router rip
RouterB(config-router)# net 129.10.0.0
```

**Figure 11-17** RouterB configuration

## Multipoint Configuration Using a Subinterface

This example configuration requires more work than the previous example because it has multiple routers and RouterA is using a subinterface rather than a physical interface. In this case the Frame Relay map will have to be built statically on RouterA. To configure a multipoint subinterface, you map it to multiple remote routers using the same subnet mask, but different DLCI numbers. For example, assume that you are the administrator for RouterA in Figure 11-18 and you want to configure subinterface S0/1.2, which has IP address 192.168.51.1 and subnet mask 255.255.255.0, to connect over three different virtual connections to the remote Routers B, C, and D.



**Figure 11-18** Multipoint subinterface configuration on S1.2

Table 11-2 outlines the steps to configure RouterA.

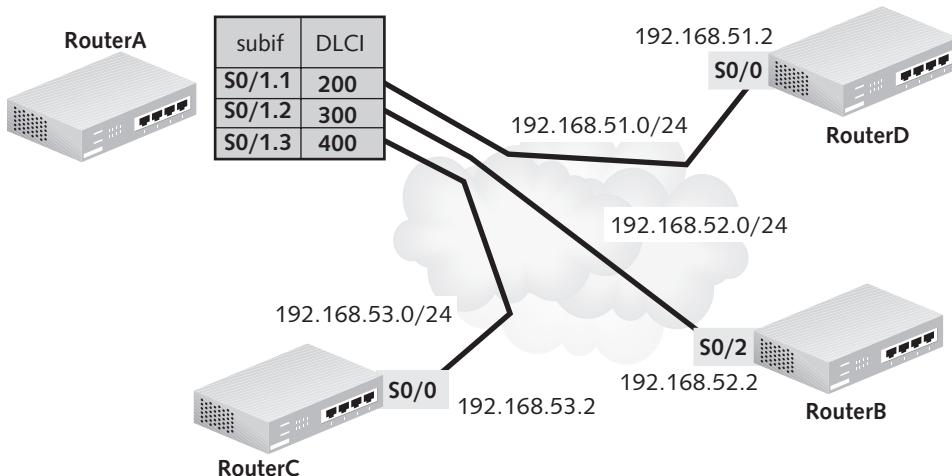
| Router prompts this:     | You type this:                      | Description                                                                                                                                                               |
|--------------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RouterA#                 | config t                            | Allows you to configure the router from the terminal line                                                                                                                 |
| RouterA(config)#         | int s0/1                            | Tells the router to access interface serial 0/1 for configuration                                                                                                         |
| RouterA(config-if)#      | no ip address                       | When you are configuring a subinterface, you do not want the main interface to have an IP address; this command removes any configured IP address for the S0/1 interface. |
| RouterA(config-if)#      | encap fr                            | Sets the encapsulation for this port to Frame Relay using Cisco (the default). The other option is ietf.                                                                  |
| RouterA(config-if)#      | exit                                | Exits interface configuration mode                                                                                                                                        |
| RouterA(config)#         | int s0/1.2 multipoint               | Configures subinterface S0/1.2 for a multipoint connection                                                                                                                |
| RouterA(config-subif)#   | ip ad 192.168.51.1<br>255.255.255.0 | Sets S0/1.2 for the IP address shown                                                                                                                                      |
| RouterA(config-subif)#   | bandwidth 64                        | Sets the bandwidth for this port to 64 Kbps                                                                                                                               |
| RouterA(config-subif)#   | frame map ip 192.168.51.2<br>200 b  | Maps subinterface to DLCI 200 and enables broadcast routing updates                                                                                                       |
| RouterA(config-subif)#   | frame map ip 192.168.51.3<br>300 b  | Maps subinterface to DLCI 300 and enables broadcast routing updates                                                                                                       |
| RouterA(config-subif)#   | frame map ip 192.168.51.4<br>400 b  | Maps subinterface to DLCI 400 and enables broadcast routing updates                                                                                                       |
| RouterA(config-subif)#   | exit                                | Leaves subinterface configuration mode                                                                                                                                    |
| RouterA(config)#         | router rip                          | Enables RIP                                                                                                                                                               |
| RouterA(config-router) # | network 192.168.51.0                | Sets RIP to be used on the network                                                                                                                                        |

Table 11-2 Subinterface configuration prompts and commands for RouterA in Figure 11-18

## Point-to-Point Configuration Using Subinterfaces

The example shown in Figure 11-19 has the same physical star, but the “hub” router will be configured for three point-to-point connections to remote routers B, C, and D. Notice there is a different subinterface on RouterA for each remote router connection, and the remote routers are all on different subnets. This is the definition of point-to-point. Point-to-point Frame Relay configurations do not support Inverse ARP. In this situation, you will have to configure each subnet separately and use the `frame-relay interface-dlci` command

to associate the DLCI numbers with a specific subinterface. The configuration on the remote routers will be much simpler than the one on the hub router. These remote router configurations will resemble the earlier basic multipoint configuration example with two routers. If LMI and Inverse ARP are supported, the remote routers will build their Frame Relay map tables dynamically. The commands to configure RouterA for the point-to-point example shown in Figure 11-19 are shown in Figure 11-20



**Figure 11-19** Point-to-point configuration sample using subinterfaces

```

RouterA(config)#int s0/1
RouterA(config-if)#no ip address
RouterA(config-if)#en fr
RouterA(config-if)#exit
RouterA(config)#int s0/1.1 point-to-point
RouterA(config-subif)#ip ad 192.168.51.1 255.255.255.0
RouterA(config-subif)#ban 64
RouterA(config-subif)#frame-relay interface-dlci 200 b
RouterA(config-if)#exit
RouterA(config)#int s0/1.2 point-to-point
RouterA(config-subif)#ip ad 192.168.52.1 255.255.255.0
RouterA(config-subif)#ban 64
RouterA(config-subif)#frame-relay interface-dlci 300 b
RouterA(config-if)#exit
RouterA(config)#int s0/1.3 point-to-point
RouterA(config-subif)#ip ad 192.168.53.1 255.255.255.0
RouterA(config-subif)#ban 64
RouterA(config-subif)#frame-relay interface-dlci 400 b
RouterA(config-subif)#exit
RouterA(config)#router rip
RouterA(config-router)#network 192.168.51.0
RouterA(config-router)#network 192.168.52.0
RouterA(config-router)#network 192.168.53.0

```

11

**Figure 11-20** Point-to-point configuration commands

## Frame Relay Static Mapping

As shown in Table 11-2 and Figure 11-20, you sometimes have to define the DLCI numbers manually. This is called making a **static address to DLCI Frame Relay map**. You statically configure your DLCI entries in the following situations:

- The remote router does not support Inverse ARP.
- You need to assign specific subinterfaces to specific DLCI connections.
- You want to reduce broadcast traffic.
- You are configuring Open Shortest Path First (OSPF) over Frame Relay.

## Non-Cisco Routers

You have seen in the previous examples that the encapsulation frame-relay command is used to enable Frame Relay on a Cisco router. Non-Cisco routers use a different Frame Relay encapsulation than Cisco routers. If you are configuring Cisco routers to connect to other Cisco routers, they will automatically use the Cisco Frame Relay encapsulation. If, however, you are connecting a Cisco router to a non-Cisco router, you must specify `ietf` Frame Relay encapsulation using the following command:

```
RouterA(config-if)#encapsulation frame-relay ietf
```

## Keepalive Configuration

By default, keepalive packets are sent out every 10 seconds to the Frame Relay switch. Keepalive packets, as previously described, are used to maintain the connection and inform the router of the connection status. You can change the keepalive period by typing `keepalive` followed by the time in seconds of the keepalive period at the `router(config-if) #` interface configuration prompt. The keepalive period can be set from as low as zero to as high as 30 seconds. For example, if you want to set the keepalive period to 15 seconds, type `keepalive 15` at the interface configuration prompt:

```
RouterA(config-if)#keepalive 15
```

---

## Monitoring Frame Relay

You can check your Frame Relay configuration by using `show` commands. These commands allow you to verify that the commands you previously entered produced the desired effect on your router. The most common `show` commands for monitoring Frame Relay operation are `show interface`, `show frame-relay pvc`, `show frame-relay map`, and `show frame-relay lmi`. Figures 11-21, 11-22, 11-23, and 11-24 show these commands with their output.

The serial configuration for each serial interface is available by its interface number.

The router gives a status report for the interface, the IP address and subnet mask, and DLCI and LMI statistics.

```

router# show interface Serial 0/0
Serial0/0 is up, line protocol is down
Hardware is HD64570
Internet address is 199.6.13.1/24
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
LMI enq sent 19, LMI stat recv 0, LMI upd recv 0, DTE LMI down
LMI enq recv 11, LMI stat sent 0, LMI upd sent 0
LMI DLCI 1023 LMI type is CISCO frame relay DTE
Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0
Last input 00:00:07, output 00:00:04, 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
  354 packets input, 24860 bytes, 0 no buffer
  Received 290 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  303 packets output, 18589 bytes, 0 underruns
  0 output errors, 0 collisions, 26 interface resets
  0 output buffer failures, 0 output buffers swapped out
  19 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up

```

**Figure 11-21** The `show interface` command and output

11

This command shows the PVC statistics for each serial interface.

The router tells you the DLCI number and whether the link is active. Other information includes total packet counts for the link and statistics for each FECN, BECN, and DE packet.

```

router# show frame-relay pvc
PVC Statistics for interface Serial0/0 (Frame Relay DTE)

DLCI = 200, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Serial0/0.1

  input pkts 0      output pkts 0      in bytes 0
  out bytes 0      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

pvc create time 00:06:41, last time pvc status changed 00:06:41

```

**Figure 11-22** The `show frame relay permanent virtual circuit` command and output

## 326 Chapter 11 PPP and Frame Relay

This command shows the DLCI-to-Network-layer address mapping for each remote router to which the local device is connected.

```
router# show frame-relay map
Serial0/0.1 (down): ip 199.6.13.2 dlci 200(0xC8,0x3080), static,
broadcast,
CISCO, status defined, inactive
```

**Figure 11-23** The `show frame-relay map` command and output

This command displays the amount and type of management information that is being transferred over the LMI DLCI connection. It also displays the LMI type used on the interface.

```
router# 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 39          Num Status msgs Rcvd 0
  Num Update Status Rcvd 0         Num Status Timeouts 38
```

**Figure 11-24** The `show frame relay local management interface` command

## Chapter Summary

- Many WAN connectivity options are available for modern networks, including digital lines, Frame Relay, and analog modems.
- WAN technologies typically define Data Link and Physical layer standards.
- The Point-to-Point Protocol (PPP) is the most widely used WAN protocol today.
- On Cisco routers, PPP is used mainly as a Data Link layer encapsulation method; however, it does provide an interface to the Network layer via specific Network Control Protocols (NCPs).
- PPP provides link establishment, quality determination, Network layer protocol encapsulation, and link termination services.
- Frame relay is a flexible WAN technology that can be used to connect two geographically separate LANs.
- Frame relay is both a service and type of encapsulation.
- The service parameters must be discussed with the Frame Relay provider (telecommunications company).
- Service parameters for Frame Relay include the access rate, Committed Information Rate (CIR), Committed Burst Size (CBS), and Excess Burst Size (EBS).

- Frame relay connections employ virtual circuits that can be either permanent or switched.
- Virtual circuit connections across Frame Relay connections are defined by Data Link Connection Identifier (DLCI) numbers.
- The DLCI numbers can be associated with remote Network layer addresses; however, they are only locally significant unless the Local Management Interface (LMI) is available.
- Most Frame Relay providers support LMI, which allows Frame Relay maps to be dynamically created via Inverse ARP.
- Static mappings of DLCI numbers to remote IP addresses can be configured when routers do not support Inverse ARP.
- Inverse ARP is on by default for multipoint configurations.
- Inverse ARP is not enabled on point-to-point links because only one path is available.
- Frame relay circuits can be established over serial interfaces or subinterfaces on Cisco routers.
- relay

## Key Terms

**address** The element of the PPP frame represented by the binary sequence 11111111; because PPP is used to create a point-to-point connection, there is no need for PPP to assign an individual address for each host.

**AppleTalk Control Protocol (ATCP)** PPP interface protocol for AppleTalk; *see Network Control Protocol.*

**asynchronous character map** The piece of information in the LCP field of the PPP packet that allows PPP to encode its transmission properly for the recipient host.

**authentication** The process of verifying the right to complete a connection.

**challenge** The query packet, or the action of sending the query packet over a CHAP connection, that is used to verify the participants of the PPP connection.

**Challenge Handshake Authentication Protocol (CHAP)** PPP authentication protocol that provides better security than PAP in authenticating devices on PPP connections.

**compression** Data compression that can be performed on the PPP packet at the source and then uncompressed at the destination.

**Consultative Committee on International Telephony and Telegraphy (CCITT)** The former name of International Telecommunication Union-Telecommunication Standardization Sector (ITU-T).

**control** The element of the PPP frame represented by the binary sequence 00000011, which indicates that the transmission of user data will not be sequenced and is to be delivered over a connectionless link.

**data** The LCP field is also known as the Data field. This location contains the LCP information and the data that has been encapsulated from the higher layers. The default size of this field is 1500 bytes, but PPP implementations can negotiate a larger size for this field.

**down-when-looped** A Cisco router command that shuts down an interface when looping is detected; used to prevent testing scenarios from causing troubleshooting problems in a production environment.

**flag** Identifies the beginning and end of the PPP frame.

**Frame Check Sequence (FCS)** A mathematical computation placed at the end of the frame, used to ensure that the frame was not corrupted during transmission.

**Frame Relay access device (FRAD)** The device that the Frame Relay customer uses to connect to a Frame Relay network; also known as the Frame Relay assembler/disassembler.

**Frame Relay assembler/disassembler** *See* Frame Relay access device (FRAD).

**Frame Relay map** A table that defines the interface to which a specific DLCI number is mapped.

**Frame Relay network device (FRND)** The device that the Frame Relay provider supplies as the connection to the Frame Relay network; the acronym FRND is pronounced *friend*.

**Frame Relay switch** A telecommunications company device that is used to support Frame Relay connections from customer locations; used to route Frame Relay traffic inside the public data network.

**Frame Relay switching table** A table that is maintained on a Frame Relay switch; used to route Frame Relay traffic via virtual circuit DLCI numbers.

**High-Level Data Link Control (HDLC)** A common layer 2 WAN protocol that many other WAN protocols are based upon.

**High-Speed Serial Interface (HSSI)** Defines a serial connection that operates at speeds of up to 52 Mbps over distances of up to 15 meters (50 feet)

**International Telecommunication Union-Telecommunication Standardization Sector (ITU-T)** A standards organization based in Europe, but with membership worldwide; involved in telecommunications standardization.

**IP Control Protocol (IPCP)** PPP interface protocol for IP; *see* Network Control Protocol.

**IPX Control Protocol (IPXCP)** PPP interface protocol for IPX; *see* Network Control Protocol.

**keepalive packets** Data packets sent between devices to confirm that a connection should be maintained between them.

**LCP link configuration** A process that modifies and enhances the default characteristics of a PPP connection; includes the following actions: link establishment, authentication, link-quality determination, Network layer protocol configuration negotiation, and link termination.

**Link Control Protocol (LCP)** Used to establish, configure, maintain, and terminate PPP connections.

**link establishment** The process of opening and configuring a PPP connection before any data can be transferred over the link.

**link-quality determination** The process of checking the quality of a PPP link and monitoring its reliability.

**Link Quality Monitoring (LQM)** PPP feature that checks the reliability of the link by monitoring the number of errors, latency between requests, connection retries, and connection failures on the PPP link.

**link termination** The process of disconnecting a PPP connection when the call is complete, which is determined by the PPP hosts that made the connection.

**loopback command** A Cisco router command that places an interface in a looped-back state, which means that all outgoing data will be redirected as incoming data without going out on the network; used for testing purposes.

**magic number** Unique numbers added by the router to a packet, which allows it to detect a looped-back link.

**maximum receive unit size** The piece of information in the LCP field of the PPP packet that sets the receive buffer size for the LCP connection, typically 1500 bytes.

**multilink** Allows multiple transmission devices (such as two modems) to send data over separate physical connections; defined in RFC 1717.

**multipoint** The configuration of a single interface or subinterface to use multiple virtual circuits.

**Network Control Protocol (NCP)** Allows PPP to encapsulate multiple protocols including IP, IPX, and AppleTalk. NCPs are functional fields containing codes that indicate the type of protocol that is encapsulated.

**Network layer protocol configuration negotiation** The process of determining a Network layer protocol to use over a PPP connection that is common to both PPP hosts.

**nonbroadcast multiaccess (NBMA)** A rule used in Frame Relay that does not allow broadcasts to be sent to multiple locations from a single interface.

**oversubscription** When the sum of the data arriving over all virtual circuits exceeds the access rate.

**Password Authentication Protocol (PAP)** PPP authentication protocol that provides some security in verifying the identity of devices using PPP connections.

**point-to-point** The configuration of one or more interfaces or subinterfaces to connect to multiple virtual circuits. Each circuit will be on its own subnet. Acts like a leased line.

**protocol** The element of the PPP frame represented by two bytes used to identify the protocol that is encapsulated.

**public data network (PDN)** A telecommunications network that connects telephones around the country. These services can be provided by AT&T, Sprint, MCI, and RBOCs.

**RADIUS server** RADIUS is an authentication and accounting server.

**static address to DLCI Frame Relay map** A Frame Relay map that has been manually created by a network administrator.

**subinterface** A logical division of an interface; for example, a single serial interface can be divided into multiple logical subinterfaces.

**Terminal Access Controller Access Control System (TACACS)** An authentication protocol that allows Cisco routers to offload user administration to a central server. TACACS and Extended TACACS (XTACACS) are defined in RFC 1492.

11

## Review Questions

1. If you want to use CHAP authentication, which protocol would you employ?
  - a. Multilink
  - b. PAP
  - c. Frame relay
  - d. PPP relay

**330** Chapter 11 PPP and Frame Relay

2. What is the default encapsulation type on serial interfaces of Cisco routers?
  - a. PPP
  - b. HDLC
  - c. SDLC
  - d. Frame Relay
3. Which of the following is an NCP? (Choose all that apply.)
  - a. IPXCP
  - b. HDLC
  - c. SDLC
  - d. ATCP
  - e. IPCP
4. PPP was derived from \_\_\_\_\_.
  - a. Frame Relay
  - b. HDLC
  - c. RBOC
  - d. ISDN
5. What is a common reason for looping an interface?
  - a. to achieve greater bandwidth
  - b. to drop nonessential frames
  - c. to increase packet size
  - d. testing
6. Which of the following is a unique number that helps devices discover looped interfaces?
  - a. MAC
  - b. LCP
  - c. magic number
  - d. bandwidth
7. Which of the following employs the strongest encryption technique?
  - a. plain text
  - b. PAP
  - c. CHAP
  - d. clear text
8. If you want your router to use CHAP and then PAP authentication, which of the following commands would be correct?
  - a. router>ppp au chap pap
  - b. router#ppp authentication chap pap
  - c. router(config-if)#ppp au pap chap

- d. router(config-if)#ppp au chap pap
  - e. router(config)#ppp authentication chap pap
9. Which WAN protocol did PPP replace?
- a. HDLC
  - b. SDLC
  - c. SLIP
  - d. LAPD
10. Which protocol is used to automatically build the Frame Relay map along with LMI?
- a. ARP
  - b. RARP
  - c. Inverse ARP
  - d. DLCI
11. To make DLCI numbers globally significant, LMI causes routers to issue \_\_\_\_\_ that advertise the DLCI numbers.
- a. unicasts
  - b. keepalives
  - c. broadcasts
  - d. multicasts
12. When negotiating a data transfer rate for Frame Relay with a telecommunications provider, the rate agreed upon is the \_\_\_\_\_. 11
- a. keepalive rate
  - b. CIR
  - c. EBS
  - d. DDR
13. The Address portion of the Frame Relay frame contains which of the following pieces of information? (Choose all that apply.)
- a. DLCI
  - b. FECN
  - c. Flag
  - d. BECN
  - e. FCS
14. The line speed of a Frame Relay connection is known as the \_\_\_\_\_.  
a. access rate  
b. CBS  
c. EBS  
d. CIR

**332** Chapter 11 PPP and Frame Relay

15. \_\_\_\_\_ numbers are locally significant in Frame Relay connections and are used to identify specific virtual circuits.
  - a. DLCI
  - b. PDN
  - c. ARP
  - d. LMI
16. To prevent routing loops, Frame Relay uses \_\_\_\_\_.
  - a. loopback attack
  - b. split horizon
  - c. event horizon
  - d. DLCI numbers
17. Frame relay is more efficient than older WAN encapsulation methods because error correction is handled by \_\_\_\_\_ Frame Relay communications.
  - a. lower layers
  - b. DLCI
  - c. LMI
  - d. upper layers
18. Frame relay uses \_\_\_\_\_ to combine multiple data streams on one connection.
  - a. duplexing
  - b. simplex
  - c. multiplexing
  - d. encoding
19. What is the purpose of keepalive packets?
  - a. to reduce data transfer rates
  - b. to keep PVCs active
  - c. to increase data transfer rates
  - d. to negotiate connection speed
20. Which of the following layers do WAN specifications typically define? (Choose all that apply.)
  - a. Physical
  - b. Data Link
  - c. Network
  - d. Transport
  - e. Presentation
21. In Frame Relay, what would be considered the DCE?
  - a. customer's router
  - b. terminal adapter

- c. PPP
  - d. frame relay switch
22. Which of the following was formerly CCITT?
- a. ASCII
  - b. ANSI
  - c. ITU-T
  - d. EBCDIC
23. What is another term used to describe a Frame Relay switch?
- a. FRND
  - b. FRAD
  - c. PDN
  - d. PSTN
24. Which of the following would be a subinterface for Serial 0/1?
- a. S0/0.1
  - b. S0/0.2
  - c. S0/1.2
  - d. S0/2.1
25. What does LMI stand for?
- a. Logical Management Interface
  - b. Local Management Interface
  - c. Logical Maintenance Interconnect
  - d. Logical Maintenance Interface
26. What are the three possible connection states for a DLCI? (Choose all that apply.)
- a. Interactive
  - b. Active
  - c. Inactive
  - d. Disconnected
  - e. Deleted
27. Which of the following does not allow broadcasts to be sent to multiple destinations through a single interface?
- a. LMI
  - b. subinterfaces
  - c. LCP
  - d. MBA
  - e. NBMA

**334** Chapter 11 PPP and Frame Relay

28. Which of the following is a type of virtual circuit? (Choose all that apply.)
- a. MVC
  - b. PVC
  - c. SVC
  - d. QVC
29. Which of the following are LMI encapsulation types supported by Cisco routers? (Choose all that apply.)
- a. LMI 2
  - b. cisco
  - c. ansi
  - d. v923i
  - e. q933a
30. Which of the following is the default LMI encapsulation type for a Cisco router?
- a. LMI 2
  - b. cisco
  - c. ansi
  - d. v923i
  - e. q933a
31. What does the `router(config-if)#encap fr` command do?
- a. sets the enable mode prompt to FR
  - b. enables Frame Relay on the first serial interface
  - c. sets the encapsulation to Frame Relay
  - d. sets the language to French
32. Which of the following commands would show statistics for a virtual circuit?
- a. `router>sh frame map`
  - b. `router#sh frame map`
  - c. `router#sh frame pvc`
  - d. `router(config-if)#sh frame pvc`
33. What Frame Relay encapsulation must be configured on Cisco routers that are attached to non-Cisco routers?
- a. ietf
  - b. cisco
  - c. ansi
  - d. q933a

34. How often are Frame Relay keepalive packets sent by default?

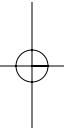
- a. every 30 seconds
- b. every 10 seconds
- c. once every hour on the half-hour
- d. once every hour on the hour
- e. once every 30 minutes

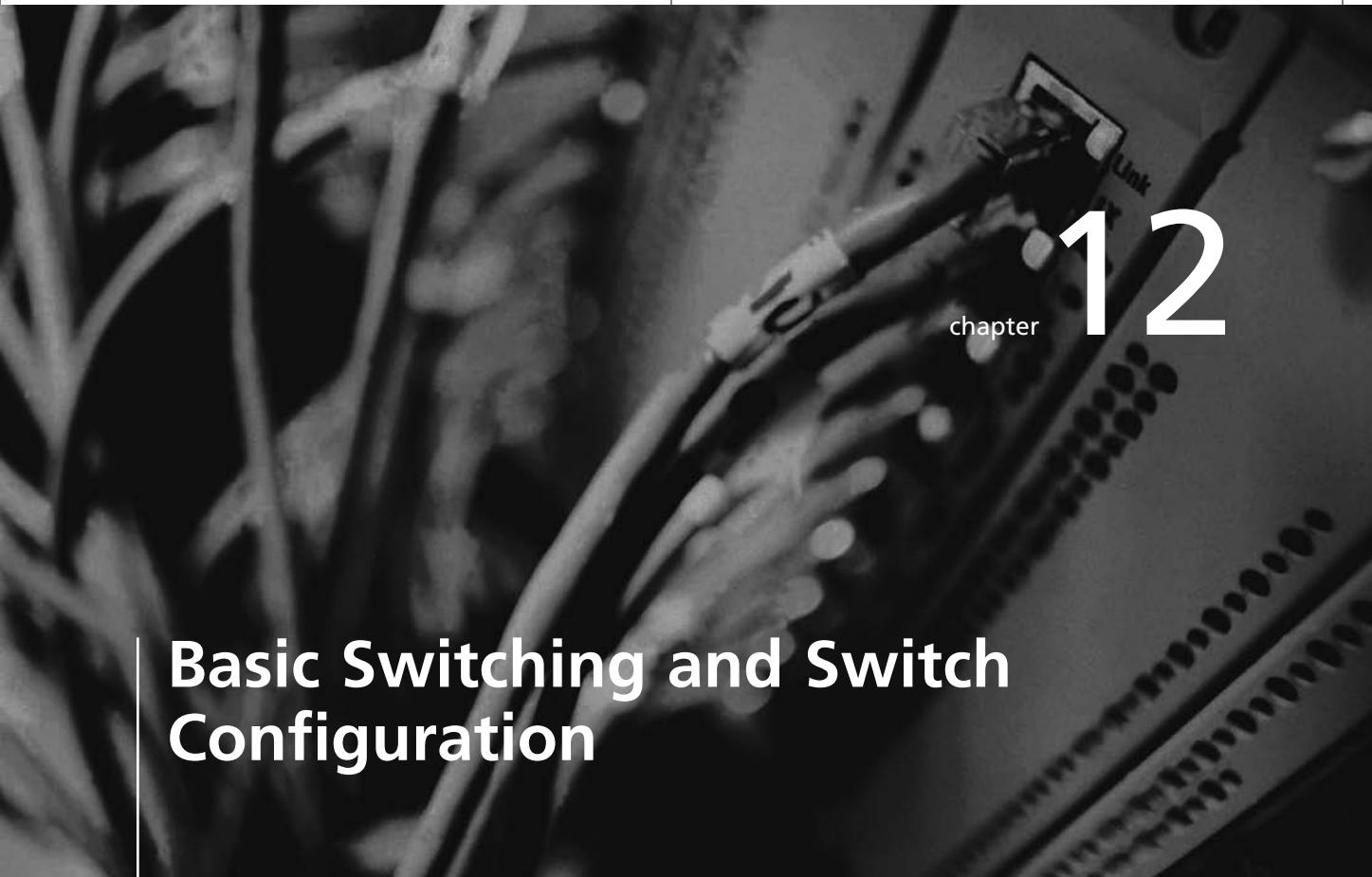
---

## Case Projects



1. Big Byte Consulting has hired your company to help it set up Frame Relay to connect several locations. Big Byte's headquarters are in Austin, Texas; it will be connecting PVCs to Dallas, San Antonio, and Houston. You and Jennifer are expected to have a conference call with the network administrators at the other locations to discuss the Frame Relay configuration. What type of information will have to be coordinated among the various locations? What type of information would you require to configure your Cisco 2500 series router to support your Frame Relay connection?
2. During the conference call with Big Byte, the subject of multipoint and point-to-point is raised. The Big Byte network team does not understand the differences between multipoint and point-to-point connections. How do you explain the differences to Big Byte using its own network as an example?
3. Big Byte has configured its Frame Relay network but is experiencing problems. You have been informed that the Frame Relay connection between Austin and Houston is down. Someone has already contacted the phone company and determined that the Frame Relay switches are operating properly. You decide to verify the Frame Relay configuration between the two locations. What commands would you use to check the configuration? What type of configuration problems might you expect to find?
4. Big Byte has a Cisco router they want to connect to a non-Cisco router via a serial connection. Explore the data link layer encapsulation methods available on each type of router and write a short paragraph describing which protocol should be used.





# 12

chapter

## Basic Switching and Switch Configuration

**After reading this chapter and completing the exercises, you will be able to:**

- Explain the technology and media access control method for Ethernet networks
- Explain network segmentation and basic traffic management concepts
- Explain basic switching concepts and the operation of Cisco switches
- Perform and verify switch configuration tasks
- Implement basic switch security

**Up to this point, the focus of this book has been on routing with Cisco routers.** In this chapter and the next, the focus moves to a different piece of equipment: the Cisco layer 2 switch. The discussion covers Ethernet operations, performance and improvement methods, Fast Ethernet, Gigabit Ethernet, and half- and full-duplex communication modes. You will also learn about Cisco layer 2 switching technologies, terminology, and basic configurations.

## Ethernet Operations

As you have learned, Ethernet is a **network access method** (or **media access method**) originated by the University of Hawaii, later adopted by Xerox Corporation, and standardized as IEEE 802.3 in the early 1980s. Today, Ethernet is the most pervasive network access method in use and is the most commonly implemented media access method in new LANs. Many companies and individuals are continually working to improve the performance and increase the capabilities of Ethernet technology.

In the following sections, you will revisit the Ethernet access method, discuss Ethernet errors, investigate latency problems, and learn ways in which Ethernet performance can be improved. Becoming comfortable with these concepts will help you troubleshoot and improve the performance of your LAN.

### CSMA/CD

Ethernet uses **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** as its **contention method**. This means that any station connected to a network can transmit anytime a transmission is not present on the wire. After each transmitted signal, each station must wait a minimum of 9.6 microseconds before transmitting another packet. This is called the **interframe gap**, or **interpacket gap (IPG)**, which provides sufficient spacing between frames so that network interfaces have time to process a packet before receiving another.

**Collisions** Even though stations must listen to the wire before sending a transmission, two stations could listen to the wire simultaneously and not sense a **carrier signal**. In such a case, both stations might begin to transmit their data simultaneously. Shortly after the simultaneous transmissions, a collision would occur on the network wire. The stations would detect the collision as their transmitted signals collided with one another.

Once a collision is detected, the first station to detect the collision transmits a 32-bit **jam signal** that tells all other stations not to transmit for a brief period (9.6 microseconds or slightly more). The jam signal is used to ensure that all stations are aware that a collision has occurred. After the the jam signal is transmitted, the two stations that caused the collision use an algorithm to enter a **backoff period**, which causes them not to transmit for a random interval. The backoff period is an attempt to ensure that the two stations do not immediately cause another collision.

**Collision Domain** A **collision domain** is the physical area in which a packet collision might occur. You need to understand this concept in order to understand network segmentation, which is essentially the division of collision domains. Repeaters and hubs do not segment the network and therefore do not divide collision domains. Routers, switches, bridges, and gateways do segment networks and thus create separate collision domains.

If a station transmits at the same time as another station in the same collision domain, a collision will occur. The 32-bit jam signal that is transmitted when the collision is discovered

prevents all stations on that collision domain from transmitting. If the network is segmented, the collision domain is also divided, and the jam signal will only affect those stations that operate within that collision domain. Stations that operate within remote segments (other collision domains) are not subject to the collisions or frame errors that occur on the local segment.

**Broadcasts** Stations on a network broadcast packets to other stations to make their presence known on the network and to carry out normal network tasks such as IP address-to-MAC address resolution. However, when a segment has too much broadcast traffic, utilization increases and network performance in general suffers. People may experience slower file transfers, e-mail access delays, and slower Web access when broadcast traffic is above 10% of the available network bandwidth.

One simple way to reduce broadcast traffic is to reduce the number of services that servers provide on your network and to limit the number of protocols in use on your network. Limiting the number of services will help because each computer that provides a service, such as file sharing, broadcasts its service at a periodic interval over each protocol it has configured. Many operating systems allow you to bind the service selectively to only a specific protocol, which will reduce broadcast traffic on the network. You can also eliminate unnecessary protocols to eliminate broadcast traffic on the network. An example of an unnecessary protocol is the IPX protocol on a server in an IP-only network. In this case, services would be advertised on both IP and IPX, when other stations would only be communicating via IP. IPX advertisements and the use of the IPX protocol is unnecessary in this case because no other stations on the network would be using IPX.



NOTE

Network users who share files may be sharing them over multiple protocols. Broadcast messages typically advertise these file-sharing services on each network protocol configured. Therefore, limiting the number of protocols in use on stations that share files can reduce the amount of broadcast traffic on the network.

12

If a broadcast from one computer causes multiple stations to respond with additional broadcast traffic, a broadcast storm could occur. A **broadcast storm**, as the name implies, is a sudden rush of network transmissions that causes all other network communications to slow down due to the volume of data competing for access to the same bandwidth on the communications medium. One of the most common causes of broadcast storms is a network loop, which in turn is the result of redundant links between switches and bridges. A broadcast storm occurs on an Ethernet collision domain when 126 or more broadcast packets are being transmitted per second.



NOTE

As you will learn in Chapter 13, the Spanning Tree Protocol is used to combat the problems caused by these physical loops.

Software faults with network card drivers or computer operating systems can also cause broadcast storms. You can use a **protocol analyzer** to locate the device causing the broadcast storm. Once the device is identified, you can correct the configuration error or apply an appropriate software driver update to correct the problem.

## Latency

The time that a signal takes to travel from point to point on a network affects the performance of the network. **Latency**, or **propagation delay**, is the length of time that is required to forward, send, or otherwise propagate a data frame. Latency differs depending on the resistance offered by the transmission medium, the number of nodes, and in the case of a connectivity device, the amount of processing that must be done on the packet. For instance, sending a packet across a copper wire does not introduce as much latency as sending a packet across an Ethernet switch.

The amount of time it takes for a packet to be sent from one device to another is called the **transmission time**. The latency of the devices and media between the two hosts affects the transmission time; the more processing a device must perform on a data packet, the higher the latency. The maximum latency for a repeater can be as high as 140 bit times. The maximum propagation delay for an electronic signal to traverse a 100-meter section of Category 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable is 111.2 bit times.



**Bit time** refers to the amount of time required to transmit one data bit on a network. On a 10-Mbps Ethernet network, bit time is 100 nanoseconds. On a 100-Mbps Ethernet network, bit time is 10 nanoseconds.

Table 12-1 illustrates the maximum propagation delays for various media and devices on an Ethernet network. The propagation delays shown illustrate the maximum allowable round-trip delays for cabling and devices on a 100-Mbps Ethernet network.

| Media or Device                                               | Maximum Propagation Delay (Bit Times) |
|---------------------------------------------------------------|---------------------------------------|
| Two Ethernet stations using two-pair UTP or fiber-optic cable | 100                                   |
| Two Ethernet stations using 100Base-T4                        | 135                                   |
| 1-meter segment of Category 3 or 4 UTP cable                  | 1.14                                  |
| 1-meter segment of Category 5 UTP or STP cable                | 1.112                                 |

**Table 12-1** Propagation delay for Ethernet media and devices

Repeaters can take anywhere from less than 8 bit times up to 140 bit times to propagate a signal.

**Slot time** (512 bit times) is an important specification that limits the physical size of each Ethernet collision domain. Slot time specifies that all collisions should be detected from anywhere in a network in less time than is required to place a 64-byte frame on the network. To maintain the same slot time on expanded Ethernet networks the IEEE instituted the **5-4-3 rule**, which limits collision domains to five segments of wire, four repeaters and/or hubs, and three populated hubs between any two stations on a 10-Mbps network. Violating those design parameters could cause network errors. For example, if a station at one end of an Ethernet network did not receive the jam signal before transmitting a frame on the network, another collision could occur as soon as the jam signal and newly transmitted frame crossed paths. Theoretically, this situation could occur repeatedly and prevent any useful data from being transmitted on the wire.

## Ethernet Errors

Most errors on an Ethernet network are caused by defective or incorrectly configured equipment. Errors impede the performance of a network and the transmission of useful data. In this section, you will learn about several Ethernet packet errors and their potential causes.

**Frame Size Errors** An Ethernet packet sent between two stations should be between 64 bytes and 1518 bytes. According to Ethernet specifications, shorter or longer frames are errors. Frame size errors that occur on Ethernet networks include:

- *Short frame* or *runt*—A frame that is shorter than 64 bytes. A collision, a faulty network adapter, corrupt NIC software drivers, or a repeater fault can cause this error.
- *Long frame* or *giant*—A frame that is larger than 1518 bytes. Because 1518 is the largest legal frame size, a long frame is too large to be valid. A collision, faulty network adapter, illegal hardware configuration, transceiver or cable fault, termination problem, corrupt NIC software drivers, repeater fault, or noise can cause this error.
- *Jabber*—This is another classification for giant or long frames. This frame is longer than Ethernet standards allow (1518 bytes) and has an incorrect **frame check sequence** (FCS).

In addition to frame size errors, other packet errors might be seen on an Ethernet network. For example, a **frame check sequence (FCS) error**, which indicates that bits of a frame were corrupted during transmission, can be caused by any of the previously listed errors. An FCS error is detected when the calculation at the end of a packet does not conform correctly to the number and sequence of bits in the frame, which means some type of bit loss or corruption occurred. An FCS error can be present even if the packet is within the accepted size parameters for Ethernet transmission. If a frame with an FCS error also has an octet missing, it is called an **alignment error**.

12

**Collision Errors** Collisions are a fact of life on an Ethernet network. Because the likelihood of collisions increases with the number of devices, reducing the number of devices per collision domain will usually solve the problem. You can do this by segmenting your network with a router, a bridge, or a switch.



A transmitting station will attempt to send its packet 16 times before discarding it as an **NIC error**. Thus, a network with a high rate of collisions, which prompts multiple retransmissions, may also have a high rate of NIC errors, and vice versa.

Another Ethernet error related to collisions is called a **late collision**. A late collision occurs when two stations transmit more than 64 bytes of data frames before detecting a collision. In other words, a late collision occurs when the slot time of 512 bits has been exceeded. The only way a station can distinguish between a late and normal collision is by determining that the collision occurred after the first 64 bytes of the frame were transmitted.

Typical causes of this type of collision include too many repeaters on a network or network cabling that is too long. Occasionally, a network device malfunction may also cause late collisions.

**Fast Ethernet** When a 10BaseT network is experiencing congestion, upgrading to Fast Ethernet can reduce congestion considerably. Fast Ethernet uses the same network access method (CSMA/CD) as common 10BaseT Ethernet, but provides ten times the data transmission rate—100 Mbps. That means that frames can be transmitted in 90% less time with Fast Ethernet than with standard Ethernet.

When you upgrade from 10BaseT to Fast Ethernet, all the network cards, hubs, and other connectivity devices that are now expected to operate at 100 Mbps must be upgraded. If the 10BaseT network is using Category 5 or higher cable, that cable can still be used for Fast Ethernet operations. Also, a 10-Mbps Ethernet NIC can function on a Fast Ethernet network because the Fast Ethernet hub or switch to which the device attaches will automatically negotiate a 10-Mbps connection. The Fast Ethernet hub will continue to operate at 100 Mbps with the other Fast Ethernet devices. Most modern NICs can operate at either 10 or 100 Mbps. Finally, Fast Ethernet devices are also capable of full-duplex operation, which allows them to obtain a transmission rate of 100 Mbps in each direction.

Fast Ethernet, which is defined under the IEEE 802.3u standard, has three defined implementations:

- **100Base-TX**—Uses two pairs of either Category 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP); one pair is used for transmit (TX), and the other is used for receive (RX). The maximum segment length is 100 meters; two Class II repeaters and a five-meter patch cable can be used to create a maximum distance of 205 meters between stations for each collision domain.
- **100Base-T4**—Uses four pairs of either Category 3, 4, or 5 UTP cable; one pair is used for TX, one pair for RX, and two pairs are used as bidirectional data pairs. The maximum segment length is 100 meters; as with 100Base-TX, two Class II repeaters and a five-meter patch cable can be used to create a maximum distance of 205 meters between stations for each collision domain. Because all four pairs are used, the T4 specification does not support full-duplexing, which is discussed in the next section.
- **100Base-FX**—Uses **multimode fiber-optic (MMF)** cable with one TX and one RX strand per link. The maximum segment length is 412 meters.

IEEE 802.3u specifies two types of repeaters: Class I and Class II. Class I repeaters have higher latency than Class II repeaters, as shown previously in Table 12-1. When two Class II repeaters are deployed on a twisted-pair network (100Base-TX or 100Base-T4), the specification allows for an additional five-meter patch cord to connect the repeaters. This patch cord is in addition to the normal 200-meter segment length. This means that the maximum distance between two stations can be up to 205 meters. When repeaters are used on networks with fiber-optic cable (e.g., 100Base-FX), the maximum segment lengths are actually reduced because the repeaters introduce latency. Latency increases the propagation delay, which means that the maximum distance possible between stations must be reduced to ensure that the slot time is maintained.

## Gigabit Ethernet

Recent advances in technology have allowed us to reach even higher speeds than those of Fast Ethernet. It is not uncommon to be working in a switched environment that consists of all Gigabit Ethernet switches. Gigabit switches work at 1000 Mbps, which is equal to one billion bits per second. Some standards operate at 10 Gbps, but they are outside of the scope of this text.

The Gigabit Ethernet specifications and the governing IEEE standards are:

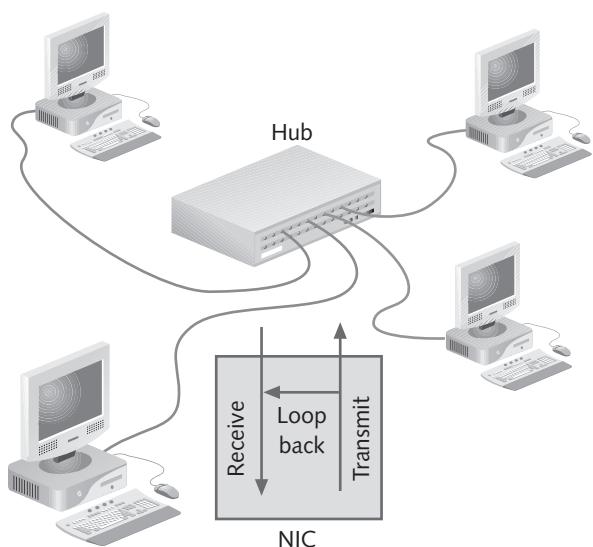
- *1000Base-TX (802.3ab)*—Uses four pairs of Category 5 unshielded twisted-pair cable. The maximum segment length is 100 meters.
- *1000Base-SX (802.3z)*—Uses multimode fiber. The maximum segment length varies based on what type of fiber is being used. For example, using a 62.5 micron core, the maximum length is 220 meters. When using a 50 micron core, the maximum length is 550 meters.
- *1000Base-LX (802.3z)*—Uses single-mode fiber. The maximum distance for this standard is 10 kilometers.
- *1000Base-CX (802.3z)*—Uses shielded twisted-pair copper cabling. The maximum segment length is 25 meters.

## Half- and Full-Duplex Communications

In **half-duplex** communications, devices can send and receive signals, but not at the same time. In **full-duplex** (or **duplex**) communications, devices can send and receive signals simultaneously. As an analogy of these communication types, consider the walkie-talkie and the telephone. When two people use walkie-talkies, one person must finish speaking before the other can transmit. This is half-duplex communication. When two people communicate over the telephone, both people can speak simultaneously, and both transmissions will be heard at the opposite ends. This is full-duplex communication.

Ethernet networks can use equipment that supports half- and full-duplex communications. In half-duplex Ethernet communications, when a twisted-pair NIC sends a transmission, the card loops that transmission back from its transmit wire pair onto its receive pair (see Figure 12-1). The card stores the looped-back frame. The transmission is also sent out of the card. The card then compares the looped-back frame with the original frame. If the frame is the same, then there is no collision. If the looped-back frame is different from the original frame, then a collision is recorded.

12



**Figure 12-1** Half-duplex Ethernet communications

**344** Chapter 12 Basic Switching and Switch Configuration

The transmitted frame travels along the network through the hub to all other stations on the collision domain. Half-duplex NICs cannot transmit and receive simultaneously, so all stations on the collision domain (including the transmitting station) listen to the transmission before sending another.

In full-duplex Ethernet components, one set of wires is used to send a signal; a separate set is used to receive a signal. Because full-duplex network devices conduct the transmit and receive functions on different wire pairs and do not loop back transmissions as they are sent, collisions cannot occur. Furthermore, full-duplex Ethernet increases the throughput capability between devices because there are two separate communication paths. This means that 10BaseT full-duplex network cards are capable of transferring data at a rate of 10 Mbps in each direction, as compared with half-duplex 10BaseT cards. The benefits of using full-duplex are:

- Time is not wasted retransmitting frames because collisions do not occur.
- The full bandwidth is available in both directions because the send and receive functions are separate.
- Stations do not have to wait until other stations complete their transmissions because only one transmitter is used for each twisted pair.

On a Cisco Catalyst 2950 switch, you can set the duplex capabilities port-by-port. To change the duplex of a switch port, you must enter the interface configuration mode for the specific port you want to configure. The four different duplex options are:

- *Auto*—The default setting for 100-Mbps Ethernet ports. The switch port is set to determine whether the connected device is full- or half-duplex and configures itself to match.
- *Full*—This setting forces full-duplex mode on a 10- or 100-Mbps port. Use this if you know that the duplex should be full, but auto-negotiate (auto) does not seem to be working.
- *Full-flow control*—This setting is used for 100Base-TX ports only. As its name implies, it uses flow control to ensure that switch buffers do not overflow.
- *Half*—The default setting for 10-Mbps Ethernet ports, which forces the port to communicate half-duplex.

Networking tools, like the Fluke One Touch, can determine whether your switch ports are set for full or half duplex. Some operating system tools, such as mii-diag in Linux, allow you to verify full- or half-duplex operations. Client network cards can be configured through the system BIOS, operating system, or manufacturer-provided software or hardware.

---

## A Review of LAN Segmentation

You can improve the performance of your Ethernet network by reducing the number of stations per collision domain. Typically, network administrators implement bridges, switches, or routers to segment the network and divide the collision domains. This will improve performance because the more collision domains you have, the fewer collisions occur.

### Segmenting with Bridges

A **bridge** segments a network by filtering traffic at the Data Link layer. It divides a network into two or more segments, and only forwards a frame from one segment to another if the frame is a broadcast or has the MAC address of a station on a different segment. Bridges

learn MAC addresses by reading the source MAC addresses from frames as the frames are passed across the bridge. As you have already learned, MAC addresses are contained in the header information inside each packet. If the bridge does not recognize a MAC address, it will forward the frame to all segments except the one over which it travelled.

The bridge maintains a **bridging table** that maps the MAC addresses on each segment to the corresponding port on the bridge to which each segment is connected. Bridges increase latency, but because they effectively divide the collision domain, this does not affect slot time.

When you segment a LAN with one or more bridges, remember these points:

- Bridges reduce collisions on the LAN and filter traffic based on MAC addresses.
- A bridge does not reduce broadcast or **multicast** traffic. A multicast packet is similar to a broadcast, but rather than going from one node to all nodes it is from one node to a group of nodes that are listening on a predefined IP address.
- A bridge can extend the useful distance of the Ethernet LAN because distance limitations apply to collision domains, and a bridge separates collision domains.
- The bandwidth for the new individual segments is increased because they can operate separately at 10 Mbps or 100 Mbps, depending on the technology.
- Bridges can be used to limit traffic for security purposes by keeping traffic segregated; traffic between two hosts on one side of the bridge will not be propagated to the other side of the bridge.

## Segmenting with Routers

A **router** operates at layer 3 of the OSI reference model. It interprets the Network layer protocol and makes forwarding decisions based on the layer 3 address. Routers typically do not propagate broadcast traffic; thus, they reduce network traffic even more than bridges do. Routers maintain routing tables that include the Network layer addresses of different segments. The router forwards packets to the correct router on another segment, based on those Network layer addresses. Because the router has to read the layer 3 address and determine the best path to the destination station, latency is higher than with a bridge or repeater/hub.

Keep in mind that when you segment a LAN with routers, they will:

- Decrease collisions by filtering traffic
- Reduce broadcast and multicast traffic by blocking or selectively filtering packets
- Support multiple paths and routes between them
- Provide increased bandwidth for the newly created segments
- Increase security by preventing packets between hosts on one side of the router from propagating to the other side of the router
- Increase the effective distance of the network by creating new collision domains
- Provide layer 3 routing, packet fragmentation and reassembly, and traffic flow control
- Provide communications between different technologies, such as Ethernet and Token Ring or Ethernet and Frame Relay
- Have a higher latency than bridges, because routers have more to process; faster processors in the router can reduce some of this latency

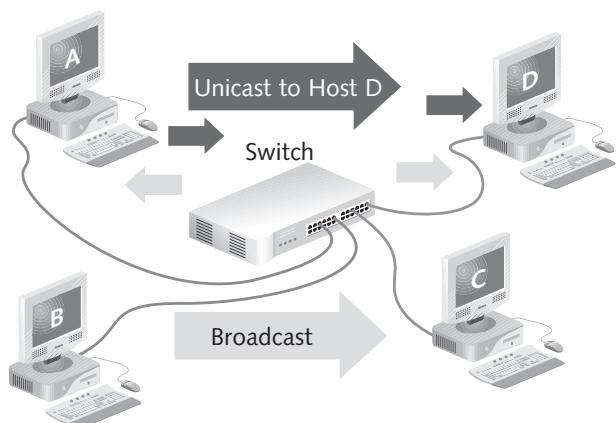
## LAN Switching

Although switches are similar to bridges in several ways, using a switch on a LAN has a different effect on the way network traffic is propagated. This difference happens because switches do quite a bit more than merely segment the LAN; they truly change the way in which communication is carried out on the LAN.

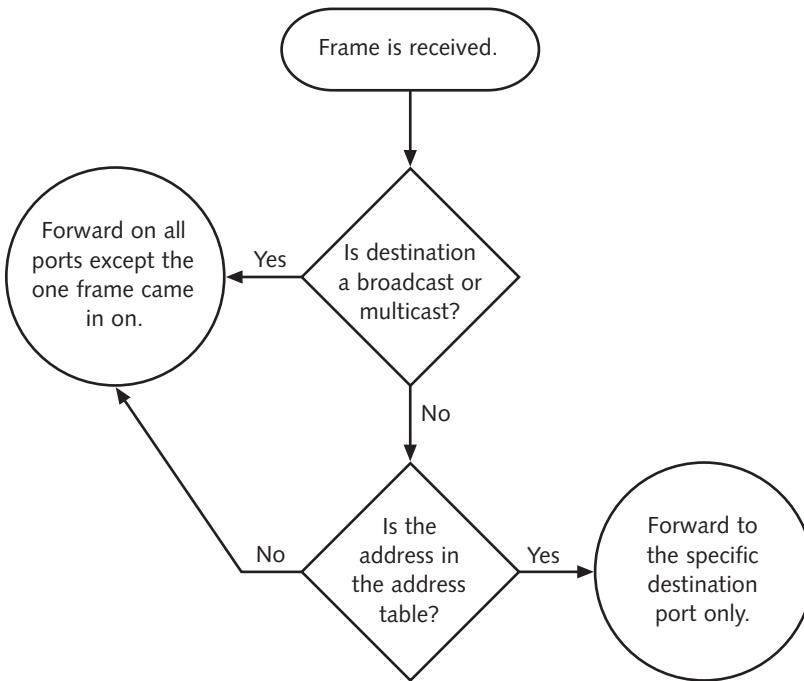
### Segmentation with Switches

Bridges and switches are similar—so much so that switches are often called **multiport bridges**. The main difference between a switch and a bridge is that the switch typically connects multiple stations individually, thereby segmenting a LAN into multiple collision domains. A bridge only separates two or more segments and is usually limited to 16 ports. In addition, switches are hardware-controlled, whereas bridges are controlled by software. Typically, hubs are connected to the bridge ports, so the workstations connected to the hubs are sharing the bandwidth on that segment. By connecting each port to an individual workstation, switches **microsegment** the network. The bandwidth is not shared as long as each workstation connects to its own switch port. This is called **switched bandwidth**, and it operates differently than the shared bandwidth through hubs.

Consider the illustration shown in Figure 12-2. When Host A sends a **unicast** to Host D, the switch (which operates at the Data Link layer of the OSI reference model) receives the unicast frame on the port to which Host A is attached, opens the data frame, reads the destination MAC address, and then passes the frame directly to the port to which Host D is attached. Unlike hub operations, the other hosts on the switch will not see the frame. However, when Host B sends a broadcast frame, the switch forwards the frame to all devices attached to the switch. This is similar to how a bridge handles broadcasts. Bridges and switches generally do not create broadcast domains. Figure 12-3 shows the inherent logic structure of this process.



**Figure 12-2** Switch packet forwarding actions



**Figure 12-3** Packet forwarding decisions made by a switch

Given the number of steps that a switch must perform on each frame, its latency is typically higher than that of a repeater or hub. Although switches do slightly more work than bridges, faster processors and a variety of switching techniques make switches typically faster than bridges. In general, however, you can count on a switch adding approximately 21 microseconds of latency to network communications.

As previously mentioned, because switches microsegment most traffic, they utilize available bandwidth more efficiently. When one host is communicating directly with another host, the connection's full bandwidth is available to them. For example, with a 10-Mbps switch on a 10BaseT LAN, the switch can often provide 10-Mbps connections for each host that is attached. If a hub were used instead of a switch, all devices on the collision domain would share the 10-Mbps connection.

Switches provide the following benefits:

- Reduction in network traffic and collisions
- Increase in available bandwidth per station, because stations can communicate in parallel
- Increase in the effective distance of a LAN by dividing it into multiple collision domains
- Increased security, because unicast traffic is sent directly to its destination and not to all other stations on the collision domain

## Switch Operations

A switch learns the hardware address of devices to which it is attached by reading the source address of frames as they are transmitted across the switch. The switch then matches the source MAC address with the port from which the frame was sent. The MAC-to-switch-port mapping is stored in the switch's **content-addressable memory (CAM)**. The switch refers to the CAM when it is forwarding frames, and it updates the CAM continuously. Each mapping receives a time stamp every time it is referenced. Old entries that are not referenced frequently enough are removed from the CAM.

The switch uses a memory buffer to store frames as it determines to which port(s) a frame will be forwarded. The two different types of memory buffering that a switch can use are **port-based memory buffering** and **shared memory buffering**. In port-based memory buffering, each port has a certain amount of memory that it can use to store frames. If a port is inactive, then its memory buffer is idle. However, if a port is receiving a high volume of traffic (near network capacity), the traffic may overload its buffer, and other frames may be delayed or require retransmission.

Shared memory buffering offers an advantage over port-based memory buffering in that any port can store frames in the shared memory buffer. The amount of memory that each port uses in the shared memory buffer is dynamically allocated according to the port's activity level and the size of frames transmitted. Shared memory buffering works best when a few ports receive a majority of the traffic. This situation occurs in client/server environments, because the ports to which servers are attached will typically see more activity than the ports to which clients are attached.

Some switches can interconnect network interfaces of different speeds. For example, a switch might have a mix of 10-Mbps, 100-Mbps, and 1000-Mbps devices attached. These switches use **asymmetric switching** and, typically, a shared memory buffer. The shared memory buffer allows switches to store packets from the ports operating at higher speeds (100/1000 Mbps) when it is necessary to send that information to ports operating at lower speeds (10 Mbps). Asymmetric switching is also better for client/server environments when the server is configured with a network card that is faster than the network cards of the clients. The switch allows the server's NIC to operate at 100 Mbps or greater and all the clients' NICs to operate at 10/100 Mbps, if necessary. This allows the server to handle the clients' requests more quickly than if it was limited to 10 Mbps.

Switches that require all attached network interface devices to use the same transmit/receive speed are using **symmetric switching**. For example, a symmetric switch could require all ports to operate at 100 Mbps or maybe at 10 Mbps, but not at a mix of the two speeds.

## Switching Methods

All switches base frame-forwarding decisions on a frame's destination MAC address. However, all switches do not forward frames in the same way. The three main methods for processing and forwarding frames are cut-through, store-and-forward, and fragment-free. One additional forwarding method, adaptive cut-through forwarding, is a combination of the cut-through and store-and-forward methods. Although menus are not covered on the CCNA exam, you should be aware that it is possible to configure some Cisco switches through a menu-driven prompt. Figure 12-14 show how configuring a switch through a menu is possible, using the example of a legacy Cisco Catalyst 2820 switch.

```
Catalyst 2820 - System Configuration
System Revision: 0 Address Capacity: 2048
System UpTime: 2day(s) 21hour(s) 15 minute(s) 4second(s)
-----Settings-----
[N] Name of system
[C] Contact name
[L] Location
[S] Switching mode FragmentFree
[U] Use of store-and-forward for multicast Disabled
[A] Action upon address violation Suspend
[G] Generate alert on address violation Enabled
[I] Address aging time 300 seconds
[P] Network Port None
[H] Half duplex back pressure (10-mbps ports) Disabled
[E] Enhanced Congestion Control (10 Mbps Ports) Disabled
-----Actions-----
[R] Reset system [F] Reset to factory defaults
-----Related Menus-----
[B] Broadcast storm control [X] Exit to Main Menu
Enter Selection:
```

**Figure 12-4** Catalyst 2820 switching menu

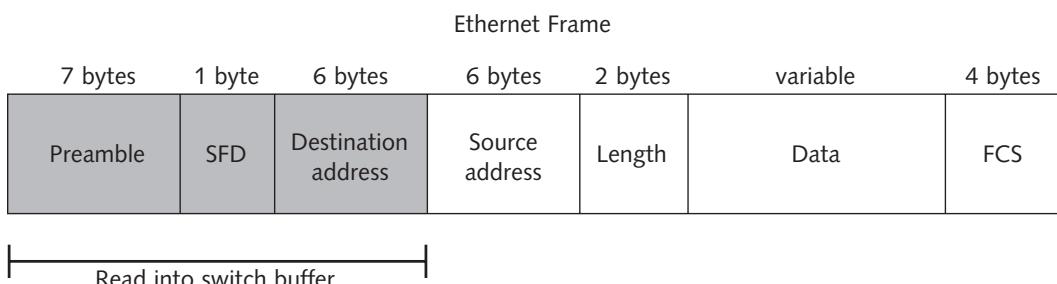
Notice in Figure 12-4 that the menu option [S] allows you to toggle switching modes and that the switch is currently set for fragment-free. Note that the mode on some models of switches cannot be changed. For example, the Cisco 2950 switch is programmed to use only the store-and-forward mode.

The four switching modes are based on varying levels of latency (delay) and error reduction in forwarding frames. For example, cut-through offers the least latency and least reduction in error propagation, whereas store-and-forward switching offers the best error-reduction services, but also the highest latency. Each of these switching methods is described in greater detail in the following sections.

12

## Cut-Through Forwarding

Switches that use **cut-through** forwarding start sending a frame immediately after reading the destination MAC address into their buffers. The main benefit of cut-through forwarding is a reduction in latency, because the forwarding decision is made almost immediately after the frame is received. For example, the switching decision is made after receiving 14 bytes of a standard Ethernet frame, as shown in Figure 12-5.



**Figure 12-5** Portion of packet read into buffer by a cut-through switch

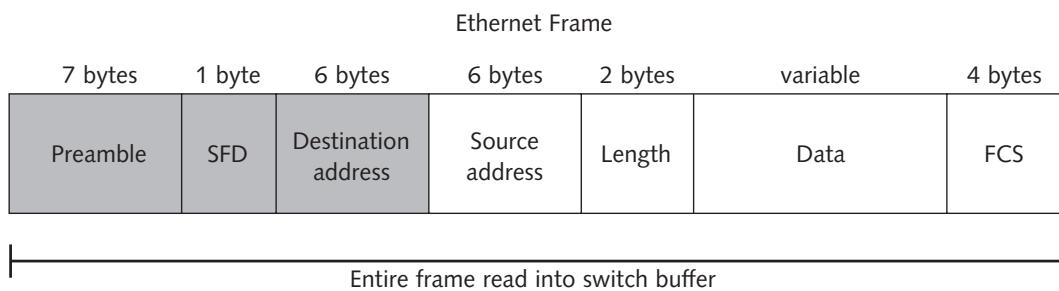
## 350 Chapter 12 Basic Switching and Switch Configuration



Cisco routers use the term **fast forward** to indicate that a switch is in cut-through mode.

The drawback to forwarding the frame immediately is the potential for errors in the frame that the switch would be unable to detect because the switch only reads a small portion of the frame into its buffer. Of course, any errors that occur in the preamble, start frame delimiter (SFD), or destination address fields will not be propagated by the switch, unless they are corrupted in such a way as to appear valid, which is highly unlikely.

**Store-and-Forward Forwarding** Store-and-forward switches read the entire frame, no matter how large, into their buffers before forwarding, as shown in Figure 12-6. Because the switch reads the entire frame, it will not forward frames with errors.



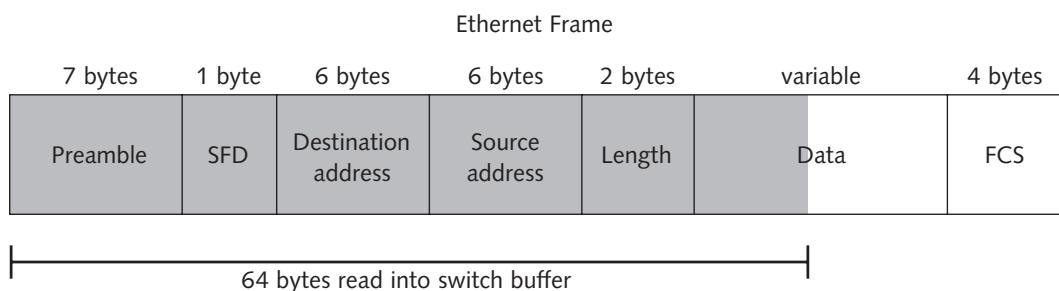
**Figure 12-6** Entire packet read into buffer by a store-and-forward switch

However, because it entails reading the entire frame into the buffer and checking for errors, the store-and-forward method has the highest latency.



Standard bridges typically use the store-and-forward technique.

**Fragment-Free Forwarding** Fragment-free forwarding represents an effort to provide more error-reducing benefits than cut-through switching, while keeping latency lower than does store-and-forward switching. A fragment-free switch reads the first 64 bytes of an Ethernet frame and then begins forwarding it to the appropriate port(s), as shown in Figure 12-7.



**Figure 12-7** Amount of packet read into buffer by a fragment-free switch

By reading the first 64 bytes, the switch will catch the vast majority of Ethernet errors and still provide lower latency than a store-and-forward switch. (Of course, for Ethernet frames that are 64 bytes long, the fragment-free switch is essentially a store-and-forward switch.)



Fragment-free switches are also known as **modified cut-through** switches.

**NOTE**

**Adaptive Cut-Through** Another variation of the switching techniques described earlier is the **adaptive cut-through** forwarding (also known as **error sensing**). For the most part, the adaptive cut-through switch will act as a cut-through switch to provide the lowest latency. However, if a certain level of errors is detected, the switch will change forwarding techniques and act more as a store-and-forward switch. Switches that have this capability are usually the most expensive, but provide the best compromise between error reduction and frame-forwarding speed.

## Switch User Interface

Two types of operating systems are in use on Cisco switches: IOS-based and set-based. Switches that use IOS-based commands are Cisco Catalyst 1900, 2820, and 2900 switches. A set-based system is older and uses “set” commands at the command-line interface. Cisco 1984G, 2926, 4000, 5000, and 6000 series switches employ the set-based configuration commands. In this book, the focus is on commands specific to the Catalyst IOS-based operating system because that is the switch type that appears on the CCNA exam. Basic IOS-based configuration is covered in this section.

You can connect to a Cisco switch in the same way you connect to a Cisco router, as described in Chapter 5. The Cisco switch has a console port to which you can connect your laptop or PC. Once you power on the switch you will be in the command-line interface; you can configure anything from the command line, and the CCNA exam focuses on it.

**12**

### Modes and Passwords

You have already learned that you cannot actually configure a router until you get to enable mode. The same is true for a Cisco switch with an IOS-based operating system. To enter enable mode, type `enable` at the command-line prompt and then press Enter. The prompt then changes to the pound (#) symbol, indicating that you are in enable mode unless a password is set on the switch. If a password is set, you will be required to enter the password at the password prompt and you will be placed into enable mode. The first step in configuring a switch is to set up a password. To start configuration mode, first type `configure terminal` or `config t` at the command prompt (just as you would when configuring a router). Once you see the `(config)#` prompt, you can configure the password as follows:

```
Switch>enable
Switch#config t
Switch(config)#enable password viewonly
```

To use a secret password, the command is slightly different:

```
Switch(config)#enable secret ccnasafe
```

**352 Chapter 12 Basic Switching and Switch Configuration**

Remember the secret password is encrypted and cannot be retrieved from the configuration file. Be sure to write your secret password down and store it in a safe place.

To enable passwords on your VTY or console line, use the following command sequence. Be sure to copy your configuration to the startup config before you power off your switch to prevent the loss of your configuration changes.

```
Switch(config)#line vty 0 15
Switch(config-line)#password vtysafe
Switch(config-line)#exit
Switch(config)#line con 0
Switch(config-line)#password consolesafe
Switch(config-line)#exit
Switch(config)#copy run start
```

## **Setting the Host Name**

The actual task of setting the host name on the Cisco Catalyst switch is identical to setting the host name on a Cisco router. As with the router, the host name is only locally significant—that is, the function of the name is to identify the switch, not to provide any sort of Internet name resolution. It is best to select a name that clearly identifies the location of the switch. For example, if you worked for a company named HudLogic, Inc. and its switch was on the fourth floor of Room 410, you might name the switch Rm410HL. To configure this name, you would type:

```
Switch(config)#hostname Rm410HL
```

Once the host name is set, the prompt will change to reflect the name of the switch. Continuing our example, the prompt would change to:

```
Rm410HL(config) #
```

## **IP on the Switch**

By default, Cisco switches are not configured with IP addresses. Generally speaking, a switch does not require an IP address, because switches operate mainly on Layer 2 (MAC addresses). However, you may want to configure an IP address for your switch so that you can manage it over the network via telnet or some other management software. Also, you may need to configure an IP address for your switch if you want to implement VLANs on your network. A VLAN is a virtual local area network that allows you to logically segment a network. This is discussed extensively in Chapter 13.

In the following example, VLAN 1 is given an IP address. The switch is then configured with a default gateway on the same subnet. The switch is also given an IP domain name which is appended to the switch's host name for IP lookups. In order to set an IP address on VLAN 1, you must enter the interface configuration mode. To configure the default gateway for the switch, you then exit the interface configuration mode and make the changes in the global configuration mode:

```
Rm410HL(config)#interface vlan 1
Rm410HL(config-if)#ip address 192.168.1.204 255.255.255.0
Rm410HL(config-if)#exit
Rm410HL(config)#ip default-gateway 192.168.1.1
Rm410HL(config)#ip domain-name classroomA
```

## Configuring Switch Ports

On a Cisco Catalyst 2950 switch, you can configure the Fast Ethernet ports via interface configuration mode. The configuration commands follow a similar syntax: `interface fastethernet slot#/port#`. On a 2950 series switch, all ports are at least 10/100 Mbps and therefore can run as either standard Ethernet or Fast Ethernet ports. To enter interface configuration mode for the first port of a switch named Rm410HL, you would use the following commands:

```
Rm410HL#configure terminal
Rm410HL(config)#interface f0/1
Rm410HL(config-if)#End
```

To view the configuration of a port, use the `show` command. The following commands will display the configuration settings for port 1 and port 24:

```
Rm410HL#show interface f0/1
Rm410HL#show interface f0/24
```

**Configuring the Duplex Mode** Remember, we have the option to change the duplex mode on the Cisco switch. In some situations, leaving the switch to detect the duplex mode automatically works fine (this is called “auto detect”). However, sometimes you will need to hard code the duplex mode. This is usually a good idea when troubleshooting possible network connectivity problems or matching the requirement of a vendor-specific setting. You would use the following command to set the duplex mode:

```
Rm410HL#configure terminal
Rm410HL(config)#interface f0/24
Rm410HL(config-if)#duplex full
```

## Securing Switch Ports

12

You can choose from several degrees of security on a switch. First, you can configure a permanent MAC address for a specific port on your switch. This means that the specified MAC address will not “age out” or be removed from the CAM table after a predetermined amount of time. Second, you could define a static MAC address entry into your switching table, which maps a restricted communication path between two ports. For example, port 7 might be configured to send frames only through port 2 via a specific hardware address. Finally, you can configure port security. This stops people from plugging hubs into network connections on your LAN by setting a limit on the number of MAC addresses that can use a specific port.

To configure port security you first must enter the interface configuration mode. From there, you can display several options by typing the following command:

```
Rm410HL(config-if)#switchport port-security ?
```

The options include `aging`, `mac-address`, `maximum`, and `violation`. The following discussion covers several of these options.

The `mac-address` option allows you to tie a specific MAC address to a specific port, thereby allowing only one NIC to communicate with the port you are configuring. This command is shown here:

```
Rm410HL(config-if)#switchport port-security mac-address
0000.aaaa.bbbb
```

**354** Chapter 12 Basic Switching and Switch Configuration

The next command, `maximum`, identifies the number of MAC addresses that may be assigned to an interface. The default setting for this command is 1. However, you are allowed to enter anywhere from 1 to 132 per interface, not to exceed to 1024 on any given switch. The correct form for this command is:

```
Rm410HL(config-if)#switchport port-security maximum 10
```

This command restricts the port to learning 10 connected MAC addresses. You can either let the switch learn the MAC addresses of those 10 hosts on its own (as they communicate) or you can configure the five MAC addresses statically, as shown earlier. When learning addresses on its own, a switch will learn as many addresses as its maximum limit allows and then configure them automatically as permanent. Cisco uses the term **sticky learn** to refer to the process by which a switch learns addresses on its own.



If you take a hub with multiple nodes connected to it and place it in a switch port, users are forced to share bandwidth; they cannot take advantage of the switched bandwidth capacity.

**NOTE**

The third command for configuring port security, `violation`, dictates what happens when a switch encounters a violation of the configured switchport security. The default is to shut down the interface. You can also define the action with one of the following three options: `protect`, `restrict`, and `shutdown`. The `protect` option stops forwarding of traffic from any host that connects after the maximum number of MAC addresses has been learned. In our example, the maximum number of MAC addresses is 10. If the `protect` option was selected, the 11th address and any subsequent new MAC addresses on the port would be prevented from communicating. The `restrict` option also stops all traffic above the number of defined MAC addresses. In addition, it sends an alert that a security violation has occurred. The final option, `shutdown`, shuts the port down if a security violation occurs.

To turn switchport security off, use the following command:

```
Rm410HL(config-if)#no switchport port-security
```

To clear the settings to include erasing the static MAC addresses, use the `clear` command:

```
Rm410HL(config-if)#clear port-security
```

---

## Chapter Summary

- Ethernet (CSMA/CD) is a media access method that was developed in the 1960s.
- Stations on an Ethernet LAN must listen to the network media before transmitting to ensure that no other station is currently transmitting.
- If two stations transmit simultaneously on the same collision domain, a collision will occur.
- The transmitting stations must be able to recognize the collision and ensure that other stations know about it by transmitting a jam signal. Once the jam signal has cleared the network, other stations can begin transmitting, but the stations that caused the collision must wait for a random backoff period before attempting to transmit again.

- The delays caused by collisions on a network can seriously affect performance when collisions exceed 5% of the traffic on the collision domain.
- One way to reduce the number of collisions on a network is to segment the network with a bridge, switch, or router.
- Switches do the most to divide the collision domain and reduce traffic without dividing the broadcast domain. This means that the LAN segment still appears to be a segment when it comes to broadcast and multicast traffic.
- A switch microsegments unicast traffic by routing frames directly from the incoming port to the destination port. This means that packets sent between two hosts on a LAN segment do not interrupt communication of other hosts on the segment. Switches are therefore able to increase the speed at which communications occur between multiple hosts on the segment.
- Another way to increase the speed at which a LAN operates is to upgrade from Ethernet to Fast Ethernet. This allows you to increase the speed at which frames are transferred on the wire, thereby improving the performance of the network.
- To fully implement Fast Ethernet, all existing hubs, NICs, and any other network interfaces must be replaced with interfaces that support Fast Ethernet. Several Fast Ethernet devices allow for compatibility between Fast Ethernet and standard Ethernet, but to take full advantage of Fast Ethernet, all components must be upgraded.
- Full duplex can also improve Ethernet performance over half-duplex operations because no collisions can occur on a full-duplex LAN.
- Full duplex allows frames to be sent and received simultaneously, which makes a 10-Mbps full-duplex connection seem like two 10-Mbps half-duplex connections.
- As with Fast Ethernet, full-duplex operations are only supported by devices designed for this type of communication. This means that the half-duplex devices on a network will have to be completely replaced to take advantage of the speed offered by full-duplex operations.
- The two types of operating systems on Cisco switches are IOS-based and set-based.
- Configuring a switch is similar to configuring a router through the CLI and has similar configuration values such as password configuration, IP configuration, and host name configuration.
- Switches can provide some level of security through the use of port security commands such as limiting the number of MAC addresses learned and specifying the action to take if the number of MAC addresses is exceeded.

12

## Key Terms

**100Base-FX** A Fast Ethernet implementation over multimode fiber-optic (MMF) cabling. The maximum segment length is 412 meters.

**100Base-T4** A 100-Mbps Fast Ethernet implementation that uses four pairs of either Category 3, 4, or 5 UTP cable. The maximum segment length is 100 meters.

**100Base-TX** A Fast Ethernet implementation that uses two pairs of either Category 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP). 100Base-TX operates at 100 Mbps with a maximum segment distance of 100 meters.

**5-4-3 rule** The networking rule that stipulates that between stations on a 10-Mbps half-duplex LAN, there can be no more than five wire segments connected, four repeaters or hubs between the segments, and three populated hubs.

**adaptive cut-through** A method of switching whereby the switch uses the cut-through technique unless network errors reach a certain threshold; then, it automatically switches to store-and-forward switching until the error rate returns to an acceptable level. Also known as **error sensing**.

**alignment error** A frame that has both an FCS error and an entire octet missing from the frame.

**asymmetric switching** A type of LAN switching that allows for multiple speeds of network communication; a switch that supports both 10-Mbps and 100-Mbps communications is an example of asymmetric switching.

**backoff period** A random interval used by devices that have caused a collision on an Ethernet network, during which the devices cannot send, to prevent them from immediately causing another collision.

**bit time** The duration of time to transmit one data bit on a network, which is 100 nanoseconds on a 10-Mbps Ethernet network or 10 nanoseconds on a 100-Mbps Ethernet network.

**bridge** A device that segments a network at the Data Link layer by filtering traffic based on the MAC address.

**bridge protocol data unit (BPDU)** Data packets sent between switches that support the spanning tree protocol.

**bridging table** A table maintained on a bridge that maps MAC addresses to the bridge port through which they can be accessed.

**broadcast** A frame that is addressed to all stations on the broadcast domain. The destination MAC address is set to FFFFFFFFFF so that all local stations will process the packet.

**broadcast storm** An error condition in which broadcast traffic is above 126 packets per second and network communications are impeded. This is typically the result of a software configuration error or programming error.

**Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** An Ethernet networking method defined by IEEE standard 802.3, which states that an Ethernet station must first listen before transmitting on a network. Any station can transmit as long as there are no transmissions active on the network. If two stations transmit simultaneously, a collision will occur, and the stations must detect the collision and reset themselves.

**carrier signal** A transmitted electromagnetic pulse or wave on the network wire that indicates a transmission is in progress.

**collision domain** The area on a network in which collisions can occur; a section of the network that is not separated by routers, switches, or bridges.

**configuration bridge protocol data unit (CBPDU)** See **bridge protocol data unit (BPDU)**.

**content-addressable memory (CAM)** A memory location on a switch that contains the MAC address-to-switch port mapping information, which the switch uses to forward frames to the appropriate destination.

**contention method** The method by which computers on a network must share the available capacity of the network wire with other computers.

**cut-through** A switching technique in which an Ethernet frame is forwarded immediately after the destination address is deciphered. This method offers the lowest latency, but does not reduce packet errors.

**error sensing** *See adaptive cut-through.*

**Ethernet** *See Carrier Sense Multiple Access with Collision Detection (CSMA/CD).*

**Fast Ethernet** Defined in IEEE 802.3u, and includes any of the following 100-Mbps Ethernet LAN technologies: 100Base-T4, 100Base-TX, 100Base-FX.

**fast forward** Indicates that a switch is in cut-through mode.

**fragment-free** A method of switching whereby the switch reads the first 64 bytes of the incoming frame before forwarding it to the destination port(s).

**frame check sequence (FCS)** A calculation based on the size of a transmitted data frame that verifies whether it was received intact.

**frame check sequence (FCS) error** An error that occurs when the calculation in the FCS field indicates that a frame was not received intact.

**full-duplex** A connection that allows communication in two directions at once; common telephone connections are typically full-duplex because people can talk and listen at the same time.

**gateway** A combination of software and hardware that translates between different protocol suites.

**giant** *See long frame.*

**half-duplex** A connection that allows communication in two directions, but not simultaneously; the circuit can be used for sending or receiving bits in only one direction at a time.

**IEEE 802.3u** The IEEE standard that defines Fast Ethernet implementations, including 100Base-T4, 100Base-TX, and 100Base-FX.

**interframe gap** The time required between the transmission of data frames on the network: 9.6 microseconds.

**interpacket gap (IPG)** *See interframe gap.*

**jabber** A frame that is longer than the 1518 bytes acceptable for transmission between stations and that also has an FCS error.

**jam signal** A 32-bit signal that is sent by the first station to detect a collision on an Ethernet network; ensures that all other stations are aware of the collision.

**late collision** A situation that occurs when two stations transmit more than 64 bytes of their frames before detecting a collision.

**latency** The lag or delay that a device or part of the network media causes; for example, fiber-optic cable delays a transmitted signal 1 bit time every 10 meters.

**long frame** An Ethernet frame that is over the 1518 bytes acceptable for transmission between stations.

**media access method** *See network access method.*

**microsegmentation** Increasing the number of collision domains without increasing the number of subnets, for example, when nodes are connected directly to a switch.

**modified cut-through** *See fragment-free.*

**358** Chapter 12 Basic Switching and Switch Configuration

**multicast** A frame that is addressed to a group of systems; typically used in radio- or television-style broadcasting on the network.

**multimode fiber-optic (MMF) cable** Fiber-optic cabling that allows for multiple simultaneous light transmissions.

**multiport bridge** Another name for a switch.

**network access method** The process by which network interface cards and devices communicate data on a network; an example is CSMA/CD. Also known as media access method.

**NIC error** An error that indicates a NIC is unable to transmit or receive a packet.

**port-based memory buffering** A memory buffer on a switch assigned by port, equally; does not allow for dynamic allocation of buffer space according to the activity level of a port.

**preamble** Binary timing information that precedes an Ethernet frame; used by the receiving station to synchronize its clock circuits so the frame can be received correctly.

**propagation delay** *See* latency.

**protocol analyzer** A hardware or software device that can capture and analyze network packets, help you analyze traffic flow and packet errors, and track network problems.

**router** A device that segments a network at the Network layer by filtering on logical addresses. Creates networks or subnetworks.

**runt** *See* short frame.

**shared memory buffering** Dynamic memory buffer that is shared by all switch ports and allocated according to the needs of the ports; ports that have more activity and larger frames to process are allowed to use more memory buffer space.

**short frame** frame that is smaller than the 64-byte minimum frame transmission size required by Ethernet.

**slot time** 512 bit times, which should be slightly longer than the time it takes to transmit a 64-byte frame on an Ethernet wire.

**start frame delimiter (SFD)** The one-octet binary pattern (10101011) that indicates the preamble is over and that the following information should be considered the actual data frame.

**sticky-learn** The process by which a switch automatically learns MAC addresses during communications and configures them as permanent.

**store-and-forward** A switching method in which the entire transmitted frame is read into a switch's buffer before being forwarded by the switch. This method offers the greatest error reduction, but the highest latency. *See* cut-through and adaptive cut-through.

**switch** A device that connects devices on a LAN and segments collision domains by port.

**switched bandwidth** A switching technique whereby the total network bandwidth is dedicated to each unicast transmission, even if multiple unicast transmissions are going through the switch at the same time. Unicast traffic between devices on a switch do not share the total bandwidth of the network.

**symmetric switching** A type of LAN switching that requires all devices to be operating at the same speed; it does not allow for a mix of 10-Mbps and 100-Mbps communications.

**transmission time** The time it takes for a transmission to go from the source host to the destination host.

**unicast** A frame that is sent or addressed to a single destination host; compare with multicast and broadcast.

---

## Review Questions

1. What address does a switch build into its table to successfully send data to that device?
  - a. routing address
  - b. IP address
  - c. bridge address
  - d. MAC address
2. Which of the following types of switching methods reads the first 64 bytes of a frame before forwarding it?
  - a. store-and-forward
  - b. cut-through
  - c. fragment-free
  - d. adaptive
3. The \_\_\_\_\_ provides sufficient spacing between frames so that network interfaces have time to process a packet before receiving another.
  - a. interframe gap
  - b. jam signal
  - c. backoff period
  - d. latency
4. Which devices look at a MAC address when making their forwarding decision? (Choose all that apply.)
  - a. switch
  - b. repeater
  - c. bridge
  - d. router
5. Which of the following network media provides the lowest latency?
  - a. STP
  - b. Category 3 UTP
  - c. Category 4 UTP
  - d. Category 5 UTP
  - e. fiber-optic cable

**360** Chapter 12 Basic Switching and Switch Configuration

6. Which of the following correctly describes microsegmentation?
  - a. creating additional segments with passive hubs
  - b. creating additional segments with routers
  - c. creating additional segments with fewer users per segment via layer 2
  - d. limiting network segments to no more than 10 users
7. Which of the following Ethernet errors describes a packet that has a bad FCS and is over 1518 bytes?
  - a. runt
  - b. short
  - c. jabber
  - d. bad FCS frame
8. When two Ethernet stations can send more than 64 bytes of their data frames before detecting a collision, this is called a \_\_\_\_\_.
  - a. jabber
  - b. jam signal
  - c. slot time
  - d. late collision
9. The minimum size of an Ethernet frame should be \_\_\_\_\_ bytes.
  - a. 32
  - b. 64
  - c. 512
  - d. 1518
10. Collisions and Ethernet errors typically occur within the first \_\_\_\_\_ bytes of an Ethernet frame, which is why fragment-free switching catches most Ethernet errors.
  - a. 64
  - b. 512
  - c. 1024
  - d. 1518
11. Which of the following describes a method of Ethernet networking that does not have collisions?
  - a. Fast Ethernet
  - b. 100-Mbps Ethernet
  - c. full-duplex Ethernet
  - d. half-duplex Ethernet
12. Which of the following switching types has the highest latency?
  - a. store-and-forward
  - b. cut-through

- c. adaptive
  - d. fragment-free
13. If a broadcast from one computer causes multiple stations to respond with additional broadcast traffic, and the level of broadcast traffic goes above 126 broadcasts per second, the situation is deemed a(n) \_\_\_\_\_.
- a. broadcast storm
  - b. transmission overload
  - c. excessive burst
  - d. jabber
14. Which of the following fall under the heading of Fast Ethernet? (Choose all that apply.)
- a. 10BaseT
  - b. 100Base-T4
  - c. 10BaseF
  - d. 100Base-TX
  - e. 100Base-FX
15. Which IEEE standard governs Fast Ethernet?
- a. 802.3a
  - b. 802.3u
  - c. 802.3g
  - d. 802.3b
16. Which of the following can divide a collision domain? (Choose all that apply.)
- a. switch
  - b. bridge
  - c. router
  - d. hub
17. What command allows you to limit the number of MAC addresses learned by a switch port?
- a. max switchport port-security 10
  - b. switchport port-security maximum 10
  - c. switch port-security maximum 10
  - d. switchport security maximum 10
18. What benefits would your network have by replacing all 10Mbps hubs with 10Mbps Catalyst switches? (Choose all that apply.)
- a. increase the number of broadcast domains
  - b. decrease the number of broadcast domains
  - c. increase the number of collision domains
  - d. decrease the number of collisions domains
  - e. Increase the bandwidth between stations that are directly connected to the switch.
  - f. Allow for full-duplex operations between nodes directly connected to the switch.

**362** Chapter 12 Basic Switching and Switch Configuration

19. Which statements are true about half-duplex Ethernet?
- In half-duplex mode, CSMA/CD is turned on.
  - In half-duplex mode, CSMA/CD is turned off.
  - On a 10Mbps link, communicating nodes would have 10Mbps of bandwidth available to them.
  - Half-duplex transmission is mandatory if nodes are directly connected to a hub that is connected to a switch.
  - Half-duplex transmission is mandatory if nodes are directly connected to a switch.
  - Because separate circuits are used by communicating end nodes in half-duplex, collisions will not occur.
20. Which statement is true about store-and-forward switching? (Choose all that apply.)
- Only the header of a frame is read before the switch forwards the frame.
  - The switch stores the frame and calculates the CRC before forwarding the frame.
  - Both latency and the error rate are decreased.
  - Both latency and the error rate are increased.
  - Latency is increased while the error rate is decreased.
21. When collisions are above 5%, you should consider \_\_\_\_\_.
- segmenting the LAN
  - increasing traffic on the LAN
  - monitoring traffic on the LAN
  - adding hubs to the LAN
22. Which of the following advantages can Cisco switches provide over hubs? (Choose all that apply.)
- increase the number of collision domains
  - increased bandwidth for individual users
  - reduced latency
  - concurrent frame forwarding
23. Which of the following are true of half-duplex operation on a CSMA/CD network? (Choose all that apply.)
- The transmitting NIC loops back its transmission.
  - The NIC listens to the media before transmitting.
  - The transmitting NIC compares the original frame with the looped-back frame to determine whether a collision occurred.
  - Collisions are not possible in a half-duplex Ethernet.
24. The \_\_\_\_\_ switching method begins forwarding the incoming frame immediately after reading the destination address.
- cut-through
  - store-and-forward

- c. adaptive
  - d. fragment-free
25. What command is used to set a port on a switch to full-duplex mode?
- a. mode full-duplex
  - b. duplex full
  - c. switch full
  - d. port full

---

## Case Projects



1. Your network administration consulting team at Winslow Networks has been assigned to a new project. Your client has requested that you optimize their LAN. Before you can begin making recommendations, what type of performance statistics should your team collect, at a minimum? What other information would be useful?
2. Your technology consulting firm has just secured a large network upgrade project. When interviewing the customer, you learn that most of the 200 users complain about the speed of the network. They explain that when the company had only 50 employees, speed was not a problem. You also learn that the entire backbone is built with hubs. The owner of the company asks you why the network has “slowed down” and how it can be fixed. What answer can you give him?
3. You are the network administrator for an organization that has to be mindful of securing its data. You learn from one of your associates that an employee has an unauthorized network in his office. What measures can you implement to ensure that only authorized network devices can communicate on the network? What unique address makes the solution possible?



# 13

chapter

## Advanced Switching Concepts

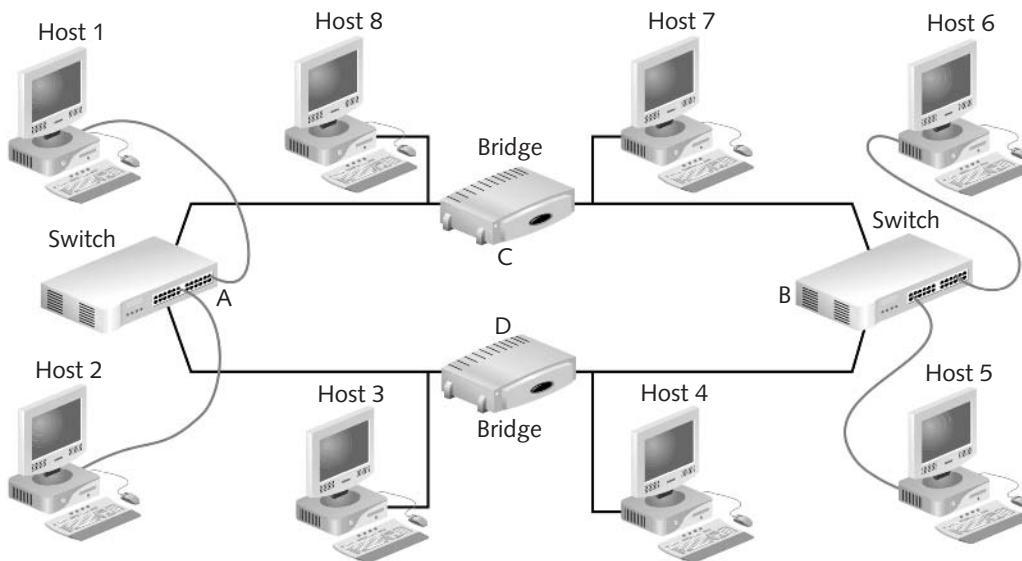
**After reading this chapter and completing  
the exercises you will be able to:**

- Explain how the Spanning Tree Protocol works and describe its benefits
- Describe the benefits of virtual LANs
- Configure a VLAN
- Understand the Purpose of the VLAN trunking protocol (VTP)
- Configure VTP

**This chapter builds on the topics introduced in Chapter 12, in which you** learned about switching concepts and basic switch configuration. In Chapter 13, you expand on that knowledge by learning some advanced switch configuration commands. In particular, you focus on the Spanning Tree Protocol, VLANs, and the VLAN Trunking Protocol (VTP).

## Spanning Tree Protocol

Networks containing several switches and bridges might include **physical path loops**. A physical path loop is a physical connection created when network devices are connected to one another by two or more physical media links. Physical path loops help improve a network's fault tolerance; if one path fails, another is available. Consider the network shown in Figure 13-1, which includes four devices (two switches and two bridges) configured in a physical loop.



**Figure 13-1** Physical loop created on LAN by switches and bridges

Assume that Host 1, which is attached to Switch A, sends out a frame with the MAC address of Host 5 as its destination. In this case, the frame could travel on two possible routes. The frame can be sent from Switch A to Bridge C or Bridge D. From there, it can be sent to Switch B, from which it can be forwarded to Host 5. The benefit of this configuration is that if either Bridge C or Bridge D fails, another path between Switch A and Switch B still exists.



This sample network could have been configured with all switches, all bridges, or any combination thereof. The number of switches and bridges is not important; the important point is that when switches and bridges are interconnected, they might create a physical loop. In this discussion the terms *bridge* and *switch* are interchangeable (e.g., root bridge could be and most likely is a switch).

The drawback to the configuration shown in Figure 13-1 is that it can result in endless packet looping, due to the existence of the physical loop. In other words, a frame can be sent continuously from one device to another, and the final destination might never be found. For example, assume that the MAC address for a station is not in any of the switching or bridging tables on the network. The frame could be forwarded endlessly around the network from bridge to switch to bridge.

The **Spanning Tree Protocol (STP)** is the solution to this problem. Invented by Radia Perlman while she was with Digital Equipment Corporation (now Compaq) in the 1980s, STP is a layer 2 link management protocol designed to prevent looping on bridges and switches. The specification for STP is IEEE 802.1d. STP uses the **Spanning Tree Algorithm (STA)** to interrupt the logical loop created by a physical loop in a bridged/switched environment. STP does this by ensuring that certain ports on some of the bridges and switches do not forward frames. Thus, although a physical loop exists, a logical loop does not. If a device fails, STP can be used to activate a new logical path over the physical network.

**Building a Logical Path** With STP enabled, the switches and bridges on a network use an election process to configure a single logical path. First, a **root bridge** (root device) is selected. Then, the other switches and bridges configure their ports, using the root bridge as a point of reference. STP-enabled devices determine the root bridge via an administratively set priority number; the device with the lowest priority becomes the root bridge. If the priorities of two or more devices are the same, then the devices will make the decision based on the lowest MAC address.



When STP-enabled devices are first enabled on a LAN, they assume that they are the root device, which begins the election process.

**NOTE**

Bridges use STP to transfer the information about each bridge's MAC address and priority number. The messages the devices send to one another are called **bridge protocol data units (BPDU)** or **configuration bridge protocol data units (CBPDU)**. Once the STP devices on the network select a root bridge, each bridge or switch determines which of its own ports offers the best path to the root bridge. The BPDU messages are sent between the root bridge and the best ports on the other devices, which are called **root ports**. The BPUDUs transfer messages about the status of the network. If BPUDUs are not received for a certain period of time, the non-root-bridge devices will assume that the root bridge has failed, and a new root bridge will be elected. The devices will then reconfigure their ports on the basis of the paths available to the new root bridge. During this period of reconfiguration, no data traffic is sent or received; only BPUDUs are received on the ports.

**13**

Once the root bridge is determined and the switches and bridges have calculated their paths to the root bridge, the logical loop is removed by one of the switches or bridges. The switch or bridge will do this by blocking the port that creates the logical loop. This blocking is done by calculating costs for each port in relation to the root bridge and then disabling the port with the highest cost. For example, refer back to Figure 13-1 and assume that Switch A has been elected the root bridge. Switch B would have to block one of its ports to remove the logical loop from the network.

**Port States** STP will cause the ports on a switch or bridge to settle into a stable state. Stable states are the normal operating states of ports when the root bridge is available and all paths are functioning as expected. STP devices use transitory states when

**368** Chapter 13 Advanced Switching Concepts

the network configuration is undergoing some type of change, such as a root bridge failure. The **transitory states** prevent logical loops during a period of transition from one root bridge to another.

The stable states are as follows:

- **Blocking**—The port is sending and receiving the STP messages (BPDUs), but it is not receiving or forwarding data frames, in order to prevent logical loops in the network.
- **Forwarding**—The port is receiving and forwarding data frames, learning new MAC addresses, and sending and receiving BPDUs. All of the ports on a root bridge are configured for forwarding.
- **Disabled**—The port is disabled and is neither sending or receiving BPDUs nor forwarding or receiving frames.

The transitory states are as follows:

- **Listening**—The port is listening to frames so that a new root can be selected; it is not receiving or forwarding data frames, and it is not learning new MAC addresses.
- **Learning**—The port is learning new MAC addresses based on incoming frames, but it is not yet receiving or forwarding data frames.

STP devices use the transitory states on ports while a new root bridge is being elected. During the listening state, STP devices are configured to receive only the BPDUs that inform them of network status. STP devices use the learning state as a transition once the new root has been selected, but all the bridging or switching tables are still being updated. Because the routes may have changed, the old entries must either be timed out or replaced with new entries. Ports on STP-enabled devices move through the different states as indicated in the following list:

- From bridge/switch bootup to blocking
- From blocking to listening (or to disabled)
- From listening to learning (or to disabled)
- From learning to forwarding (or to disabled)
- From forwarding to disabled

In a completely configured and stable STP topology, all ports will be in either the forwarding or blocking state. There will only be one root device (bridge or switch) and all other devices will have one designated root port. All of the root ports on each device and all of the ports on the root bridge will be in the forwarding state.

**Topology Changes** When the topology is changed, STP-enabled devices react automatically. If a device in an STP-enabled network stops receiving CBPDUs, then that device will claim to be the root bridge and will begin sending CBPDUs describing itself as such. This begins the rebuilding process, which is the same as the initial building of the STP topology. This event occurs when the root bridge fails or becomes separated from the other devices. Each device claims to be the root bridge for a short period until a new root bridge is elected.

**Per-VLAN STP (PVSTP)** Per-VLAN STP (PVSTP) operates on VLANs and treats all VLANs connected as separate physical networks. It provides the ability to load balance traffic between the VLANs. The load balancing takes place at Layer 2, as compared to a router

load balancing at Layer 3. PVSTP uses Cisco's proprietary ISL trunking protocol, which is covered later in this chapter. It allows a VLAN trunk to block for some VLANs and forward for others. The technology is advanced enough to prevent bridge loops on the VLANs.

**Spanning Tree PortFast** STP does have some additional features. For example, the spanning tree portfast feature allows you to configure a switch to bypass some of the latency (delay) associated with the switch ports transitioning through all of the STP transitory states before they reach the forwarding state. You should only use this command if you are certain that the devices connected to your switch will not cause a bridge loop. Suppose, for example, that you have a 2950 switch with 24 ports; that 22 of those ports are used to connect PCs, servers, and printers; and that the last two ports are used for uplinks. You can configure ports 1 to 22 with the portfast option. When the switch is recycled, the ports will come up in forwarding mode, reducing the downtime of your other components.

**Configuring STP** Although STP's default settings work without additional configuration, you do have the option of modifying its settings. For example, you can change the priority of the switch that allows you to choose which switch becomes the root bridge. The default priority for a switch on the network is 32768. As discussed earlier, Cisco's switches use PerVlan STP; this essentially means that you can have a different priority for each VLAN on the switch. The STP priority will increment for each VLAN you have configured on the switch (e.g., VLAN 1 = 32769, VLAN 2 = 32770, etc.). The range of numbers available to you are 0–61440, and the settings must be in increments of 4096. If you set a switch to a priority of 0, then the switch becomes the root bridge for all VLANs on the network. If you want a different value between VLANs, then you would configure each VLAN with a different priority. Your core switch (or the switch closest to the center of your network) should be the root bridge. Table 13-1 lists some important STP commands. Note that the last command in Table 13-1, the range option, is used to enable the portfast option on ports 1–22 without having to enter each individual interface. This option is very useful and can be used in other command sequences as well.

**13**

| Command                                                                                            | Purpose                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rm410HL(config)#spanning-tree priority 0                                                           | To set the priority of the root bridge.                                                                                                                                       |
| Rm410HL(config)#spanning-tree VLAN 1 priority 4096                                                 | To configure a switch with multiple VLANs and different priorities for each VLAN.                                                                                             |
| Rm410HL#show spanning-tree                                                                         | To view the STP configuration for the entire switch.                                                                                                                          |
| Rm410HL#show spanning-tree vlan 1                                                                  | To see the STP settings for a specific VLAN.                                                                                                                                  |
| Rm410HL(config)#int f0/1<br>Rm410HL(config-if)#spanning-tree portfast                              | To configure a switch interface to use the portfast option.                                                                                                                   |
| Rm410HL(config)#int range fastethernet 0/1 - 22<br>Rm410HL(config-if-range)#spanning-tree portfast | To enable the portfast option on ports 1–22 without having to enter each individual interface. This option is very useful and can be used in other command sequences as well. |

**Table 13-1** Important STP Commands

**Rapid STP (RSTP) 802.1w** Rapid spanning tree protocol (RSTP) is an IEEE standard governed as 802.1w. It takes the basis of 802.1d (STP) and incorporates some additional features (such as portfast) that overcome some of the flaws of STP. Cisco had enhanced its version of STP to include the portfast, uplink fast, and backbone fast features; however, this made Cisco's version of STP proprietary. The IEEE then developed RSTP as a standard and incorporated these additional features.

UplinkFast improves the convergence time of STP. This ensures that the secondary link on a switch comes up quickly, rather than waiting for a 50-second convergence time. BackboneFast is used to speed up convergence when a link that is not directly connected to the local switch goes down. As stated earlier, these two commands are proprietary to Cisco switches using 802.1d and available in the 802.1w RSTP standard. To turn RSTP on in the switch, use the following command:

```
Rm410HL(config)#spanning-tree mode rapid-pvst
```

RSTP is backward-compatible to 802.1d, but you cannot take advantage of its additional features unless it is running throughout your network.

## Virtual LANs

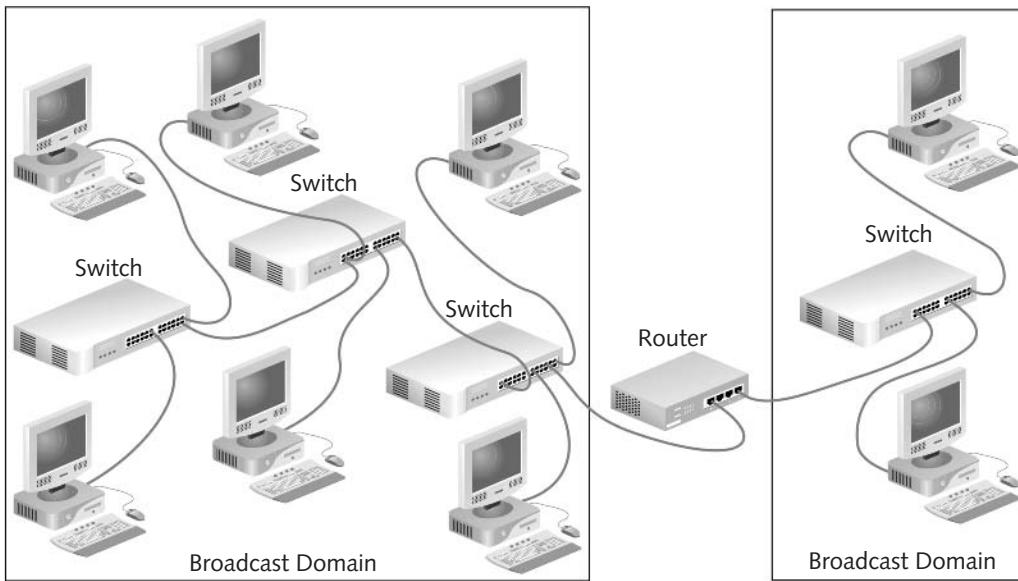
A **virtual LAN (VLAN)** is a grouping of network devices that is not restricted to a physical segment or switch. VLANs can be configured on most switches to restructure broadcast domains similarly to the way that bridges, switches, and routers divide collision domains. A **broadcast domain** is a group of network devices that will receive LAN broadcast traffic from each other.



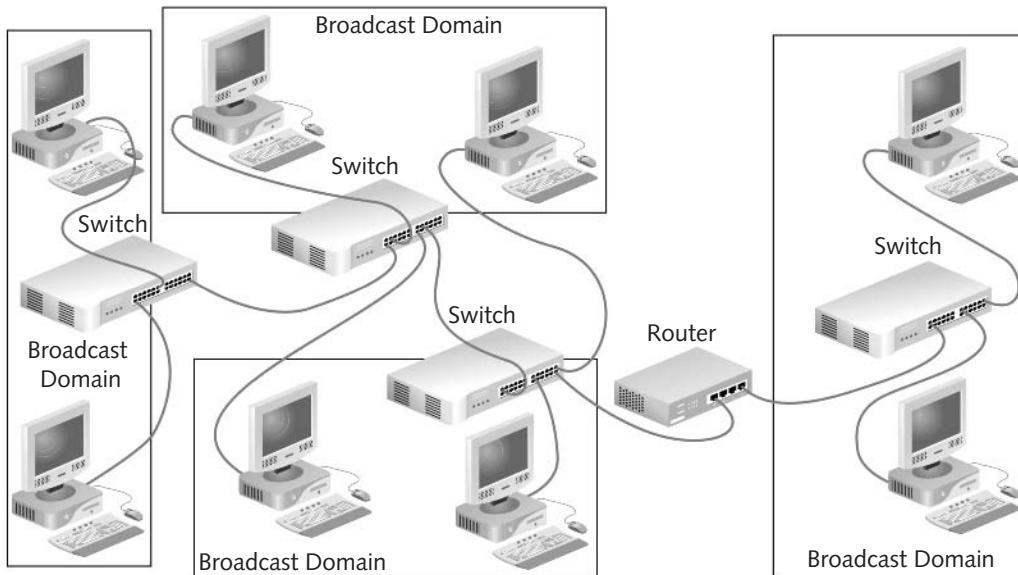
**NOTE** Because switches and bridges forward broadcast traffic to all ports, by default, they do not separate broadcast domains. Routers are the only devices previously mentioned that both segment the network and divide broadcast domains, because routers do not forward broadcasts by default.

By default, every port on a switch is in VLAN 1. This is the **management VLAN** (also known as the **default VLAN**), and it cannot be deleted. You can create multiple VLANs on a single switch or even create one VLAN across multiple switches; however, the most common configuration is to create multiple VLANs across multiple switches. With the latter configuration, routers must be used to move the traffic between the VLANs. Consider the network configuration shown in Figure 13-2, which does not employ VLANs. Notice that two broadcast domains are created, one on each side of the router.

Now consider the same network with VLANs implemented, as shown in Figure 13-3. The broadcast domains can now be further subdivided because of the VLAN configuration. This, of course, is only one way in which VLANs can be used to divide a broadcast domain.



**Figure 13-2** Broadcast domains on a LAN



**Figure 13-3** Broadcast domains using VLANs

Although VLANs can separate broadcast domains, as can routers, this does not mean that they segment at layer 3. A VLAN is a layer 2 implementation, and does not affect layer 3 logical addressing.

## Benefits of VLANs

The benefits of using VLANs center on the idea that the administrator can divide a LAN logically without changing the actual physical configuration. This ability provides the administrator with several benefits:

- Ease of adding and moving stations on the LAN
- Ease of reconfiguring the LAN
- Better traffic control
- Increased security

VLANs help to reduce the cost of moving employees from one location to another because many changes can be made at the switch. In addition, physical moves do not necessitate the changing of IP addresses and subnets because the VLAN can be made to span multiple switches. Therefore, if a small group is moved to another office, a reconfiguration of the switch to include those ports in the previous VLAN may be all that is required.

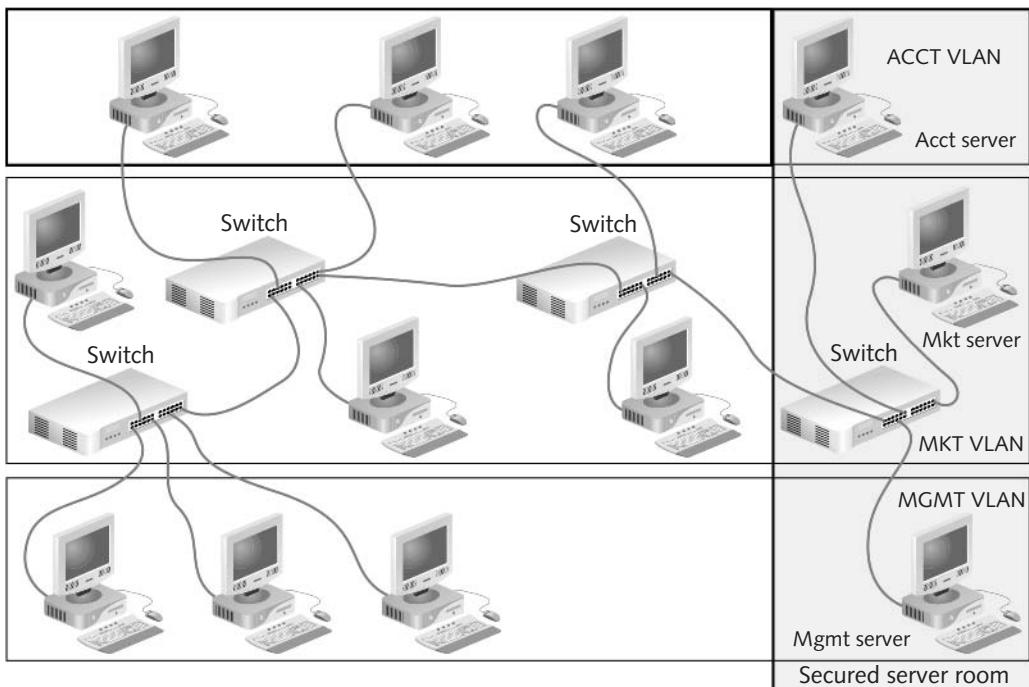
In the same way that the VLAN can be used to accommodate a physical change, it can also be used to implement one. For example, assume that a department needs to be divided into two sections, each requiring a separate LAN. Without VLANs, the change may necessitate the physical rewiring of several stations. However, with VLANs available, the change can be made easily by dividing the ports on the switch that connect to the separate sections. Network reconfigurations of this nature are much easier to implement when VLANs are an option.

Because the administrator can set the size of the broadcast domain, the VLAN gives the administrator added control over network traffic. Implementing switching already reduces collision traffic immensely; dividing the broadcast domains further reduces traffic on the wire. In addition, the administrator can decide which stations should be sending broadcast traffic to each other.

Dividing the broadcast domains into logical groups increases security because it requires a hacker to perform the difficult feat of tapping a network port and then figuring out the configuration of the LAN. Thus, the actual physical layout of the LAN is hidden from would-be network spies. Furthermore, the VLAN allows the administrator to make servers behave as if they were distributed throughout the LAN, when in fact they can all be locked up physically in a single, central location.

As an example of this flexibility, consider Figure 13-4. All the servers are locked in the secured server room, yet they are servicing their individual clients. Notice that even the clients of the different VLANs are not located on the same switches. The figure illustrates the true flexibility of using VLANs, because the logical configuration of the network is quite different from the physical configuration.

In addition to allowing for the physical security of mission-critical servers, VLANs can be configured by network administrators to allow membership only for certain devices. Network administrators can do this with the management software included with the switch. The restrictions that can be used are similar to those of a firewall; unwanted users can be flagged or disabled, and administrative alerts can be sent if someone attempts to infiltrate a given VLAN. This type of security is typically implemented by grouping switch ports together according to the type of applications and access privileges required.



**Figure 13-4** Securing servers with VLANs

## Dynamic vs. Static VLANs

Depending on the switch and switch management software, VLANs can be configured statically or dynamically. Static VLANs are configured port-by-port, with each port being associated with a particular VLAN. In a static VLAN, the network administrator manually types in the mapping for each port and VLAN.

Dynamic VLAN ports can automatically determine their VLAN configuration. Although they may seem easier to configure than static VLANs, given the description thus far, that is not quite the case. The dynamic VLAN uses a software database of MAC address-to-VLAN mappings that is created manually. This means that the MAC addresses and corresponding VLANs must be entered and maintained by the network administration team. Instead of saving administrative time, the dynamic VLAN could prove to be more time-consuming than the static VLAN. To its credit, however, the dynamic VLAN does allow the network administration team to keep the entire administrative database in one location. Furthermore, on a dynamic VLAN, moving a cable from one switch port to another is not a problem, because the VLAN will automatically reconfigure its ports on the basis of the attached workstation's MAC address. This is the real advantage of using dynamic VLAN systems.

## VLAN Standardization

Before VLAN was an IEEE standard, early implementations depended on the switch vendor and on a method known as **frame filtering**. Frame filtering was a complex process that involved one table for each VLAN and a master table that was shared by all VLANs. This process allowed for a more sophisticated VLAN separation because frames could be separated into

**374** Chapter 13 Advanced Switching Concepts

VLANs via MAC address, network-layer protocol type, or application type. The switches would then look up the information and make a forwarding decision based on the table entries.

When creating its VLAN standard, the IEEE did not choose the frame-filtering method. Instead, the **IEEE 802.1q** specification that defines VLANs recommends **frame tagging** (also known as **frame identification**). Frame tagging involves adding a four-byte field to the actual Ethernet frame to identify the VLAN and other pertinent information. The members of the IEEE considered this solution to be more scalable (able to accommodate larger networks) than frame filtering.

Frame tagging makes it easier and more efficient to ship VLAN frames across network backbones because switches on the other side of the backbone can simply read the frame instead of being required to refer back to a frame-filtering table. In this way, the frame-tagging method implemented at layer 2 is similar to routing layer 3 addressing because the identification for each frame is contained within the frame. A tagged frame can be as large as 1522 bytes, whereas a normal Ethernet frame is limited to 1518 bytes. Devices that are not VLAN-aware would see a 1522-byte frame as a long frame (a frame larger than normal size) or jabber.

The two most common types of frame tagging (encapsulation) are 802.1q and **Inter-Switch Link (ISL) protocol**. ISL is a Cisco-proprietary frame-tagging method that uses a 26-byte header. It only works between Cisco devices. If you need a frame-tagging method that works between Cisco and another vendor, you will have to use 802.1q frame tagging. The Cisco 2950 supports 802.1q. The lowest-level Cisco router that supports ISL is the 2600 series. Some Cisco switches support additional types of frame tagging, such as **LAN emulation (LANE)** and **IEEE 802.10 (FDDI)**.



**NOTE**

The additional header with the VLAN addressing information is stripped off the frame before it reaches the connected host stations. Otherwise, non-VLAN-aware host stations would see the additional information as a long frame or jabber.

## Creating VLANs

When creating VLANs on the Cisco Catalyst 2950 switch using the command-line interface, you need to consider two options. You can create VLANs by entering the **(config-vlan) #** mode and using the **VLAN** command, or you can enter the VLAN database and use the **VLAN configuration mode**. To use the config-vlan mode, you type the following:

```
Rm410HL(config)#VLAN 2
Rm410HL(config-vlan)name production
```

To use the VLAN configuration mode, you start by entering the VLAN database. Note that you must name the VLANs individually via global configuration mode. The following example assumes that you want to create three VLANs on your switch (host name Rm410HL). The three VLANs are production—remember we already configured VLAN 2 [production] above—accounting, and marketing. There will actually be four VLANs when you are finished, because the default VLAN, VLAN 1, is assumed. Look at the following command sequence, which shows how to create and list these VLANs on a Cisco Catalyst 2950:

```
Rm410HL>enable
Rm410HL#vlan database
Rm410HL(vlan)#vlan 2 name production
```

```
Rm410HL(vlan)#vlan 3 name accounting
Rm410HL(vlan)#vlan 4 name marketing
Rm410HL(vlan)#exit
```

At this point, ports are still assigned to the default VLAN, which is VLAN 1. The next step is to assign switch ports to the new VLANs. Ports can be assigned as static or dynamic. Assigning dynamic VLANs is more complicated and is not a requirement for CCNA candidates. The commands to assign static ports to VLANs are shown next. The commands are entered port-by-port. Assume that you want to assign port 5 to VLAN 2, port 7 to VLAN 3, and port 9 to VLAN 4.

```
Rm410HL(config)#interface f0/5
Rm410HL(config-if)#switchport access vlan 2
Rm410HL(config-if)#exit
Rm410HL(config)#interface f0/7
Rm410HL(config-if)#switchport access vlan 3
Rm410HL(config-if)#exit
Rm410HL(config)#interface f0/9
Rm410HL(config-if)#switchport access vlan 4
Rm410HL(config-if)#exit
Rm410HL(config)#exit
Rm410HL#show vlan
```

| <i>VLAN Name</i>    | <i>Status</i>  | <i>Ports</i>     |
|---------------------|----------------|------------------|
| 1 <i>default</i>    | <i>Enabled</i> | 1-4, 6, 8, 10-12 |
| 2 <i>production</i> | <i>Enabled</i> | 5                |
| 3 <i>accounting</i> | <i>Enabled</i> | 7                |
| 4 <i>marketing</i>  | <i>Enabled</i> | 9                |

*[remaining output cut]*



You can use the `show vlan [#]` command to gather information about a specific VLAN (instead of listing all VLANs). The `show vlan-membership` command gives a variation of the same output as the `show vlan` command. You also have the option of using the `range` command to assign multiple interfaces to a VLAN so you don't have to configure each interface individually.

13

To remove a VLAN, use the `no` parameter:

```
Rm410HL(config)#no vlan 2
```

## Link Types and Configuration

Two types of links are on Cisco switches: trunk links and access links. Trunk links are switch-to-switch or switch-to-router links that can carry traffic from multiple VLANs. Frame tagging is used to keep track of different VLANs between VLAN-aware connectivity devices.

**376** Chapter 13 Advanced Switching Concepts

Access links are links to non-VLAN-aware devices such as hubs and individual workstations. These devices have no need to understand VLANs and they operate as if they were on a single broadcast domain.

You choose from five different states for a trunk link, as follows:

- *Auto*—Configure this interface for trunking only if the connected device is set to on or desirable.
- *Desirable*—The interface will become a trunk port if the connected device is on, desirable, or auto.
- *Negotiate*—The interface is a trunk interface and will not negotiate that status with any other device.
- *Off*—The interface is not a trunk interface and will attempt to disable trunking on attached devices.
- *On*—The interface is a trunk interface and will try to enable trunking on attached devices.

To configure a trunk link on a Catalyst 2950, you must be in the appropriate interface configuration mode. The commands to complete this operation are:

```
Rm410HL#config term
Rm410HL(config)#int fastethernet 0/24
Rm410HL(config-if)#switchport mode trunk
```

After implementing the above commands, all VLANs are now enabled to be routed over this newly configured trunk link. No command exists to selectively enable VLANs for trunking. However, you can selectively prevent ports from being able to send data through specific VLANs by removing the ports. The following commands show how to prevent several ports from sending or receiving data on a VLAN:

```
Rm410HL#config t
Rm410HL(config)#int fastethernet 0/24
Rm410HL(config-if)#switchport trunk allowed vlan remove 4
```

Although it is unnecessary in this current configuration, you could add VLANs to the trunk, as follows:

```
Rm410HL(config-if)#switchport trunk allowed vlan add 1,3,5
```

**Switch Interface Descriptions** You can configure a name for each port on a switch. This is useful when you begin to define roles for a switch port on a more global basis, such as when you configure VLANs. For example, perhaps you have dedicated port 1 on your switch to serve the production department's VLAN and port 24 on your switch to be a trunk to the next building (#777). You may decide to configure your switch interface descriptions as follows:

```
Rm410HL#configure terminal
Rm410HL(config)#int f0/1
Rm410HL(config-if)#description productionVlan
Rm410HL(config-if)#int f0/24
Rm410HL(config-if)#description trunkBldg777
```

## VLAN Trunking Protocol

Cisco created the VLAN trunking protocol (VTP) to manage all of the configured VLANs that traverse trunks between switches. VTP is a layer 2 messaging protocol that manages all the changes to the VLANs across networks. Any changes made to a VLAN by an administrator (e.g., add, rename, or delete) are automatically propagated by VTP to all VTP-enabled devices.

**VTP Domains** VTP devices are organized into domains. Each switch can only be in one VTP domain at a time, and all devices that need to share information must be in the same VTP domain. To configure a VTP domain named hudlogic, you would enter the following command on the switch:

```
Rm410HL#vlan database
Rm410HL(vlan)#VTP domain hudlogic
```

You would have to perform the same command on all the switches that you expect to share VLAN information. When you make changes to the VTP configuration on your switches, you should verify them with the `show vtp` command from enable mode.

```
Rm410HL(vlan)#exit
Rm410HL#show VTP status
```



If all of your switches are in the same VLAN, configuring a VTP domain is not necessary.

**NOTE**

13

**VTP Device Modes** VTP-enabled devices have three modes: server, client, and transparent. Switches default to server mode, which means that they can add, rename, and delete VLANs and propagate those changes to the rest of the VTP devices. VTP servers save the VLAN configuration information in NVRAM. You must have at least one VTP server in your VTP domain. When a device is placed in VTP client mode, it is not allowed to make changes to the VLAN structure, but it can receive, interpret, and propagate changes made by a server. Clients do not save the VTP configuration in NVRAM. VTP transparent mode means that a device is not participating in VTP communications, other than to forward that information through its configured trunk links.

To configure a 2950 switch as a server, client, or transparent mode device, you can enter the appropriate `vtp` command, as follows:

```
Rm410HL#vlan database
Rm410HL(vlan)#vtp client
```

To set the switch back to server mode or to transparent mode, you would type “server” or “transparent” (respectively) instead of “client.”



You can configure VTP from either the VLAN configuration mode or the global configuration mode (`config #`). This book focuses on the VLAN configuration mode by entering the `vlan database` command before entering the VTP commands.

**VTP Pruning** The VTP pruning option reduces the number of VTP updates that traverse a link. It is off by default on all switches. If you turn VTP pruning on, VTP message broadcasts are only sent through trunk links that must have the information. For example, if a switch with two trunks receives an update concerning VLAN 7 on Trunk A, it will typically forward that update through Trunk B, assuming both ports are enabled for trunking.

However, assume that you have removed VLAN 7 from Trunk B. The update would still be forwarded out of Trunk B unless you enabled VTP pruning. VTP pruning can be enabled on a VTP device configured as a server, which enables it on every device in the entire domain. The command to enable and disable VTP pruning is `vtp pruning` or `vtp pruning disable` from global configuration mode. The following commands enables VTP pruning:

```
Rm410HL(vlan)#vtp pruning
```

Once enabled, VTP pruning will occur for VLANs 2 through 1005. VLAN 1 is not eligible to be pruned because it is an administrative (and default) VLAN. Therefore, all updates for VLAN 1 will always traverse the switch.

When you add a new switch to a LAN, you should clear all VTP information so as not to propagate it to the rest of the network. Use the following command on a 2950 series switch:

```
Rm410HL#show flash  
Rm410HL#delete flash:vlan.dat
```

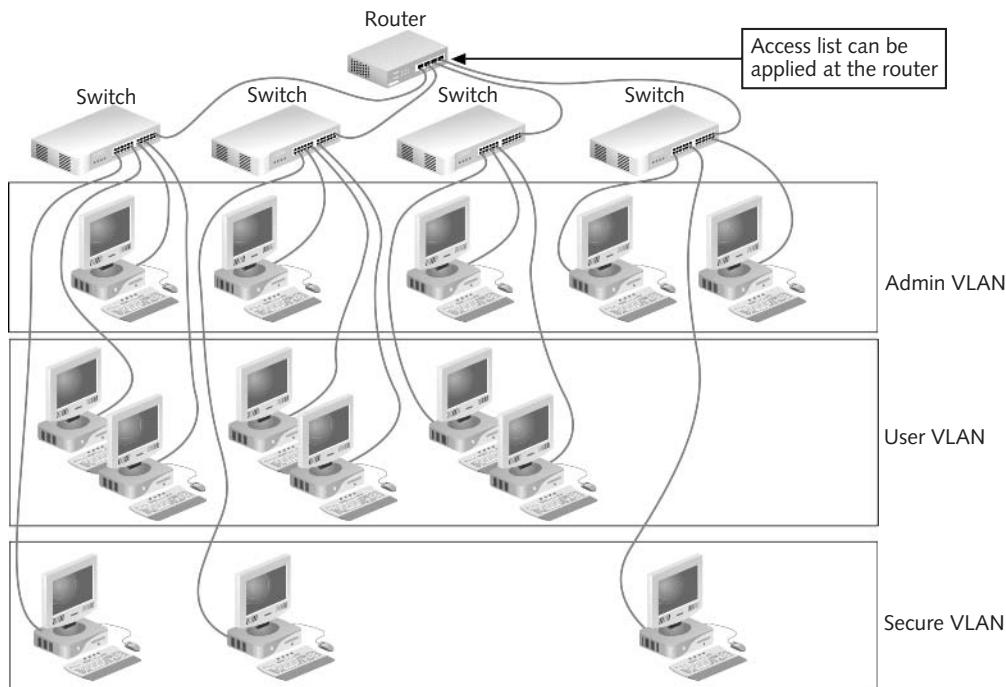
## Nonswitching Hubs and VLANs

When implementing hubs on a network that employs VLANs, you should keep a few important considerations in mind:

- If you insert a hub into a port on the switch and then connect several devices to the hub, all the systems attached to that hub will be in the same VLAN.
- If you must move a single workstation that is attached to a hub with several workstations, you will have to physically attach the device to another hub or switch port to change its VLAN assignment.
- The more hosts that are attached to individual switch ports, the greater the microsegmentation and flexibility the VLAN can offer.

## Routers and VLANs

Routers can be used with VLANs to increase security and must be used to manage traffic between different VLANs. Typically, a separate subinterface is configured on the router for each VLAN supported. In addition, the routers can implement access lists, which increase inter-VLAN security. Finally, the router allows restrictions to be placed on station addresses, application types, and protocol types. Figure 13-5 illustrates how a router might be implemented in a VLAN configuration.



**Figure 13-5** Router implemented in a VLAN configuration

The router in Figure 13-5 connects the four switches and routes communications among three different VLAN configurations. An access list on the router can restrict the communications between the separate VLANs. To configure a Cisco router for inter-VLAN communications, several steps are involved. First, enable ISL or 802.1q trunking on the switch port that the router is connected to using the `switchport mode trunk` command. Next, assign an IP address to each subinterface on the router that will be associated with a VLAN. Finally, configure 802.1q encapsulation on the router subinterfaces. The following router commands illustrate how to enable inter-VLAN communications for VLANs 1 and 2 on a Cisco router.

```

Router(config)#interface f0/0.1
Router(config-subif)#ip address 164.106.1.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 1
Router(config-if)#exit
Router(config)#interface f0/0.2
Router(config-subif)#ip address 164.106.2.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 2
  
```

VLANs are created to logically segment hosts by function, application, or other common interest without regard to physical location. Grouping devices by VLANs will control the size of the broadcast domain and keep network traffic local. However, sometimes it is necessary to communicate with devices outside the VLAN. Because each VLAN is considered a different

**380** Chapter 13 Advanced Switching Concepts

logical network, a router is required to move traffic between the two VLANs. The required router can either be an onboard **Route Switch Module (RSM)** or an external router. The router will accept the frame tagged by the sending VLAN and determine the best path to the destination address. The router will then switch the packet to the appropriate interface and forward it to the destination address. The router accomplishes the process of routing packets between two VLANs (two logical networks) in the same fashion as packets between two physical networks.

If a single link is used to connect an external router with the switch containing multiple VLANs, trunking is required for inter-VLAN routing. Trunking is the process of using either ISL or 802.1q to allow multiple VLAN traffic on the same link. For instance, an ISL trunk link would encapsulate each packet with the associated VLAN information and allow the router to route the packet accordingly. This scenario is often called a **router-on-a-stick** because of the process of pushing all the inter-VLAN traffic out a single switch port to the router and then having the traffic routed back to the same switch port to the destination VLAN.

You can see an example of routing between VLANs by configuring a 1700 router attached to a trunk link on a 2950XL switch. The configuration for each of these devices is:

## The Router

```

Router>enable
Router#configure terminal
Router(config)#interface fastethernet0/0
Router(config-if)#full-duplex
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastethernet0/0.1
Router(config-subif)#ip address 10.10.1.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#exit
Router(config)#interface fastethernet0/0.2
Router(config-subif)#ip address 10.10.2.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#exit
Router(config)#interface fastethernet0/0.3
Router(config-subif)#ip address 10.10.3.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#exit
Router(config)#interface fastethernet0/0.4
Router(config-subif)#ip address 10.10.4.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 4

```

## The Switch

```
Rm410HL>enable
Rm410HL#configure terminal
Rm410HL(config)#interface vlan 1
Rm410HL(config-if)#ip address 10.10.1.2 255.255.255.0
Rm410HL(config-if)#exit
Rm410HL(config)#ip default-gateway 10.10.1.1
Rm410HL(config)#exit
Rm410HL#vlan database
Rm410HL(vlan)#vtp domain hudlogic
Rm410HL(vlan)#vtp server
Rm410HL(vlan)#vlan 2 name production
Rm410HL(vlan)#vlan 3 name accounting
Rm410HL(vlan)#vlan 4 name marketing
Rm410HL(vlan)#exit
Rm410HL#configure terminal
Rm410HL(config)#interface f0/1
Rm410HL(config-if)#switchport mode trunk
Rm410HL(config-if)#exit
Rm410HL(config)#interface f0/2
Rm410HL(config-if)#switchport access vlan 1
Rm410HL(config-if)#exit
Rm410HL(config)#interface f0/3
Rm410HL(config-if)#switchport access vlan 2
Rm410HL(config-if)#exit
Rm410HL(config)#interface f0/4
Rm410HL(config-if)#switchport access vlan 3
Rm410HL(config-if)#exit
Rm410HL(config)#interface f0/5
Rm410HL(config-if)#switchport access vlan 4
```

Essentially what this configuration allows you to do is build a routed and secure network with only a single router. Building this type of solution offers several advantages. For example, this can provide a low-cost security solution. By simply adding an access list to the router's interface, you can limit the traffic that can be sent to or from the VLANs. This would allow you to protect sensitive data from the other VLANs.

## Chapter Summary

- The Spanning Tree Protocol (STP), which is enabled by default on most bridges and switches, allows administrators to create physical loops between bridges and switches without creating logical loops that would pose a problem for packet delivery.
- The Rapid Spanning Tree Protocol (RSTP) has enhanced STP to reduce the latency associated with convergence.
- Implementing VLANs via switches provides another way to increase the performance, flexibility, and security of a network.
- VLANs are separate broadcast domains that are not limited by physical configurations. Instead, a VLAN is a logical broadcast domain implemented via one or more switches.
- Performance benefits associated with VLANs are derived from limiting the amount of broadcast traffic that would naturally pass through a switch without filtration. The enhanced flexibility to assign any port on any switch to a particular VLAN makes moving, adding, and changing network configurations easier.
- Because traffic on a VLAN broadcast can be limited to a specific group of computers, security is also enhanced by making it more difficult for eavesdropping systems to learn the configuration of a network.
- VLAN information is communicated to switches using the VLAN trunking protocol (VTP).

---

## Key Terms

**access list** A list of criteria to which all packets are compared.

**blocking** A port state on a switch that indicates the port is receiving and sending BPDUs, but is not receiving and forwarding data frames in order to prevent logical loops in the network.

**bridge protocol data unit (BPDU)** An STP management message used to transfer status information about the Spanning Tree configuration of a switched or bridged network. Also known as configuration bridge protocol data unit (CBPDU).

**broadcast domain** A logical or physical group of devices that will receive broadcast traffic from each other on a LAN.

**default VLAN** The default configuration of every port on a switch. Same as VLAN 1.

**disabled** A port state on a switch that indicates the port is neither receiving BPDUs nor forwarding frames.

**forwarding** The state of a port on a switch or bridge that indicates it will learn MAC addresses and forward frames out that port.

**frame filtering** A technique used on early VLAN implementations that employed the use of multiple switching tables.

**frame identification** See frame tagging.

**frame tagging** A method of VLAN identification endorsed by the IEEE 802.1q specification that calls for an additional four-byte field in the VLAN frame after the source and destination addresses in the data packet. Also known as frame identification.

**IEEE 802.10 (FDDI)** A frame-tagging method used to identify VLANs trunked across Fiber Distributed Data Interfaces (FDDI).

**IEEE 802.1q** The IEEE standard that defines VLAN implementations and recommends frame tagging as the way in which switches should identify VLANs. Used by Cisco switches for compatibility with non-Cisco switches.

**IEEE 802.1w** The IEEE standard that governs Rapid Spanning Tree Protocol. *See* Rapid Spanning Tree Protocol.

**Inter-Switch Link (ISL) protocol** A frame-tagging method for VLANs proprietary to Cisco devices; uses a 26-byte header.

**LAN emulation (LANE)** A frame-tagging method used for VLANs on Asynchronous Transfer Mode (ATM) devices.

**learning** A transitory state on a bridge or switch port that indicates it is trying to learn new MAC addresses and correct its bridge table before forwarding frames on the network; used to prevent loops during the election of a new root bridge.

**listening** A transitory state on a bridge or switch port that is used during the election of a new root bridge; the port does not learn MAC addresses, nor does it forward data frames when in this state.

**logical loop** A situation that occurs when a packet can be routed in an endless loop around a network, because bridging tables and routing tables reference each other as the destination for a given address.

**management VLAN** The default configuration of every port on a switch. Same as VLAN 1.

**Per-VLAN Spanning Tree Protocol (PVSTP)** A protocol that operates on VLANs and treats all connected VLANs as separate physical networks.

**physical path loops** A loop that occurs when network devices are connected to one another by two or more physical media links.

**Rapid Spanning Tree Protocol (RSTP)** The enhanced version of STP that reduces the latency experienced by 802.1d devices in regard to convergence. RSTP is governed by the IEEE 802.1w standard.

**root bridge** The bridge or switch that is designated the point of reference (point of origin) in STP operations; also known as a root device.

**root device** *See* root bridge.

**root port** The communications port on a nonroot bridge device that is used for BPDU communication between itself and the root bridge.

**Route Switch Module (RSM)** A router placed on a switch blade; common with high-end Cisco switches such as the Catalyst 6500.

**router-on-a-stick** The process of utilizing one physical router interface (with subinterfaces configured) to route traffic for multiple VLANs.

**Spanning Tree Algorithm (STA)** The algorithm used by STP to ensure that logical loops are not created in the presence of physical loops on a network.

**Spanning Tree Protocol (STP)** The Data Link layer protocol used by switches and bridges to prevent logical loops in a network, even though physical loops may exist.

**stable state** The normal states of ports when the root bridge is available and all paths are functioning as expected.

**transitory state** The operating states of ports that prevent logical loops during a period of transition from one root bridge to another.

**virtual LAN (VLAN)** A logical broadcast domain on a LAN, created by one or more switches, that is not constrained by the physical configuration.

**VLAN trunking protocol (VTP)** A Data Link layer protocol used to track VLAN membership changes across trunk links between VTP-enabled devices.

**VTP client** A VTP device that receives and shares VTP information, but does not add, modify, or delete information and does not store the VTP database in NVRAM.

**VTP domain** A group of VTP-enabled devices configured under one name to share VLAN information.

**VTP pruning** An option configured for an entire VTP domain that prohibits the forwarding of VTP updates about VLANs disabled on specific trunk links.

**VTP server** A VTP device that is capable of adding, modifying, sending, and deleting VTP configuration information.

**VTP transparent** A device that does not participate in receiving or managing VTP domains, but will forward VTP information through its trunk ports.

---

## Review Questions

1. The IEEE standard 802.1q recommends which type of VLAN identification method?
  - a. frame filtering
  - b. frame tagging
  - c. frame segmenting
  - d. frame sequencing
2. What are the five STP port states? (Choose five.)
  - a. learning
  - b. listener
  - c. disabled
  - d. forwarding
  - e. listening
  - f. forwarder
  - g. blocking
3. By default, implementing a switched network increases the number of collision domains. Which switching technology allows for a decrease in the size of broadcast domains?
  - a. Spanning Tree Protocol
  - b. filtering and forwarding
  - c. Virtual LANs
  - d. VTP Pruning
4. For what was the Spanning Tree Protocol developed?
  - a. Prevent bridges from forwarding information out of ports that received the information.
  - b. Prevent routing loops in a routed internetwork.
  - c. Avoid loops in a bridged network with redundant paths.
  - d. Assist in the depletion of IP addresses.

5. Which of the following are reasons that a bridge port would be placed in the forwarding state? (Choose all that apply.)
  - a. The port is on the root bridge.
  - b. The port is connected to multiple bridges.
  - c. The port is the root port.
  - d. The port is not working.
6. In what three VTP modes can a switch be set?
  - a. server, client, virtual
  - b. server, host, transparent
  - c. server, host, volatile
  - d. server, client, transparent
7. Which statements are true about VTP pruning? (Choose all that apply.)
  - a. It is enabled by default.
  - b. It is disabled by default.
  - c. It is used to allow two spanning-trees to work simultaneously on the same segment of wire.
  - d. It increases available bandwidth.
  - e. It increases the amount of needless traffic on a network.
8. For a VLAN to span two or more switches, what must be configured?
  - a. a switch's duplex feature
  - b. a VTP management domain
  - c. a VPMS
  - d. a trunk connection
9. After entering the interface configuration mode for a port on a 2950 switch, which command would assign the port to VLAN 10?
  - a. `vlan-membership static 10`
  - b. `switchport access vlan 10`
  - c. `vlan static 10`
  - d. `vlan 10 static-membership`
10. Which of the following allows you to reorganize broadcast domains no matter what the physical configuration dictates?
  - a. router
  - b. VLAN
  - c. bridge
  - d. switch

**386** Chapter 13 Advanced Switching Concepts

11. If you attach a hub with five stations to a switch port that is configured for VLANs, in how many different VLANs will the devices on the hubs be located?
  - a. five
  - b. three
  - c. two
  - d. one
12. Which of the following are advantages of VLANs? (Choose all that apply.)
  - a. VLANs make relocating devices easier.
  - b. Separate VLANs do not require routers.
  - c. VLANs increase effective bandwidth utilization.
  - d. VLANs restructure broadcast domains.
13. Which of the following is a security benefit that routers provide on a VLAN?
  - a. dividing broadcast domains
  - b. dividing collision domains
  - c. allowing for the creation of access lists
  - d. bridging the IP to IPX layer 3 protocol gap
14. Which of the following are VTP modes of operation? (Choose all that apply.)
  - a. client
  - b. server
  - c. transparent
  - d. blocking
15. Which command would delete the VLAN database on a switch?
  - a. delete vlan.dat
  - b. delete flash:vlan.dat
  - c. erase flash:vlan.dat
  - d. erase vlan.dat
16. Which command allows you to create a VTP domain named XYZDOM?
  - a. VTP XYZDOM Domain
  - b. Domain VTP XYZDOM
  - c. VTP Domain XYZDOM
  - d. Domain XYZDOM VTP
17. Which statement is true about PortFast?
  - a. PortFast is used when you need to delay the amount of time it takes for a port to transition to the forwarding state.
  - b. PortFast is available on Cisco routers only.
  - c. PortFast prevents a port from entering the forwarding state.
  - d. PortFast allows a switch port to move to the forwarding state quicker.

18. Which command allows you to create VLAN 2 and name it AccountingVLAN?

- a. Switch(config-vlan)#Vlan 2 name AccountingVlan
- b. Switch(vlan)#Vlan 2 name AccountingVlan
- c. Switch(config)#Vlan 2 name AccountingVlan
- d. Switch(vlan-config)#Vlan 2 name AccountingVlan

19. Which command allows you to add ports to VLANs?

- a. Switchport mode access
- b. Switchport access mode
- c. Access mode switchport
- d. Mode switchport access

20. Which command allows you to specify a range of ports to add to a VLAN?

- a. Interfacerange
- b. Range interface
- c. Interface-range
- d. Interface range

21. Which command allows you to give a description to a port on a switch?

- a. Name
- b. Information
- c. Description
- d. Named port

22. Which command allows you to see the spanning-tree configuration for VLAN 3 only?

- a. Switch(config)#show spanning-tree
- b. Swithch#show spanning-tree vlan 3
- c. Switch(config)#show spanning-tree vlan 3
- d. Switch#show spanning tree vlan 3

**13**

23. Which VLAN is the default VLAN for a switch?

- a. VLAN A
- b. VLAN 1
- c. VLAN 10
- d. VLAN 100

24. What is the default STP priority for a switch on a network?

- a. 32768
- b. 32769
- c. 8192
- d. 4096

**388** Chapter 13 Advanced Switching Concepts

25. Which command would set VLAN 1 with a priority of 4096?
- Spanning-tree vlan 1 priority 4096
  - Spanning-tree priority vlan 14096
  - Spanning-tree priority 4096 vlan 1
  - Spanning-tree priority 1

---

## Case Projects



- A local company has decided to upgrade its LAN configuration from five hubs and a single router to a network that implements ten switches. The switches the company is planning to buy have many more ports than necessary to support each segment. However, the company wants to divide the ten departments into separate entities. The company is planning on using routers between each switch, thereby dividing the broadcast domains between the switches. What other options for configuring its network should the company consider? Moe has suggested foregoing the routers and using VLANs to divide the departments. What do you think?
- The Flagstone Corporation has purchased a Cisco 1900 series switch and wants you to configure it. What kind of interface is available for configuration? What are the default settings on the switch? Does the switch support VLANs?
- A switch in your network is connected to servers and workstations. It has two uplink ports. You want to ensure that the servers and the workstations do not have to wait for the 50-second convergence time it takes for the port to go into the forwarding state. What can you implement to ensure that the ports are available as soon as possible? What command would you use to configure this in the least amount of time?

# 14

chapter

## Network Security

**After reading this chapter and completing  
the exercises you will be able to:**

- Distinguish between the different types of network security threats
- Explain how to mitigate network security threats
- Implement SSH on Cisco routers and switches
- Configure VPNs with the Cisco Security Device Manager

**This chapter focuses on keeping data secure in a network. It covers** general network security and explains how to protect against common threats. In this chapter, you learn how to configure routers and switches with SSH to allow for secure connections, and how to use the Security Audit Wizard. Finally, you learn how to configure virtual private networks (VPN) with Cisco's Security Device Manager utility.

---

## General Network Security

These days, network security is the highest priority for most organizations. Every piece of data in an organization has a price tag associated with it, and you should assume that many unauthorized people are trying to obtain that data so they can profit from it. Sophisticated crime organizations focus exclusively on stealing data from vulnerable networks. Some of the data these criminals are looking for include credit card numbers, driver license numbers, social security numbers, and any confidential company data available. Protecting this information and the identity of an organization's customers and employees is of utmost importance.

The first step in protecting a network is devising a security policy. A **security policy** is an organization's set of rules regarding how to handle and protect sensitive data. A security policy should include, but is certainly not limited to, the following items:

- Physical security
- Acceptable use of applications
- Safeguarding data
- Remote access to the network
- Data center
- Wireless security

An effective security policy implements multiple layers of security. The more effort required to access data, the less likely that hackers and malicious employees will persevere in their attempts to access data. A good security policy also prepares for the worst. It is safest to assume that, if a hacker exerts enough effort, he will eventually get in.

A security policy should have three goals:

1. To prevent the hacker from getting access to critical data
2. To slow down the hacker enough to be caught
3. To frustrate the hacker enough to cause him or her to quit the hacking attempt

When designing a security policy, take care to specify exactly what you are trying to protect. Generally speaking, you need to protect two things: hardware and software. Common sense and physical security will go a long way toward protecting hardware. Protecting software is quite a bit more complicated because the software has to be protected against multiple threats, with the most prevalent being malicious code and hackers.

### Protecting the Hardware

The first level of security in any network is **physical security**. Critical nodes of an organization should be separated from the general workforce. The nodes should be kept in a central location where only a select group of people, such as trusted employees and administrators,

are allowed. If office space is limited and nodes must be located near employees, the servers should at least be stored in a locked cabinet like the one shown in Figure 14-1.



**Figure 14-1** Server cabinet

## Protecting Software

When you set out to protect the software on a network, you need to think about protecting applications, operating systems, and user data. The primary threats against software are malware and hackers.

**Malware** refers to malicious programs that have many different capabilities. Some might do something relatively harmless, such as opening files on a CD-ROM; others might be extremely destructive, perhaps destroying all of the data on a computer.

Hackers are usually driven by greed, ego, and/or vengeance. They look to make personal gains through system vulnerabilities, access other people's data simply to prove they can, or have malicious intent.

Protecting against hackers requires thinking on two levels. First, it is important to protect against the hacker intrusion; you need to do everything you can to keep a hacker out of your network. Second, you must take action to protect the network in case the hacker does in fact succeed in gaining access. That is, you need to minimize the amount of damage the hacker can inflict by making data difficult to steal through the use of permissions, encryption, and authentication.

## Malware Prevention

Designing a malware prevention plan is a key step in protecting your network against malware. The most important elements of such a plan are installing and maintaining virus prevention software, and conducting virus awareness training for network users.

14

**Types of Malware** Many different types of malware are currently in use around the world. The most common types of malware and their characteristics include the following:

- **Virus**—A computer program that can infect a computer without the knowledge or permission of the user. Malware (derived from the term “*malicious software*”) is sometimes categorized as a virus. Its primary intent is to infiltrate and damage a computer’s software. A virus needs human intervention to spread.
- **Worm**—A worm is different than a virus in that once it is activated it can replicate itself throughout the network by taking advantage of services on computers in the network.
- **Macro Virus**—Macro viruses are written as a macro for a specific application. When a user opens an infected application file or document, the macro virus attaches itself to the application and infects other files accessed by the same application.

- *Polymorphic Virus*—These viruses change their appearance each time they replicate or infect. This makes them difficult for antivirus programs to find as they search for patterns in the code. If the pattern is frequently changing, the antivirus software will not be able to identify it.
- *Stealth Virus*—A stealth virus is so named because it attempts to hide itself from detection. One way it does this is by changing the file it has infected back to its original value. Another method is by redirecting hard drive requests that are initiated by the antivirus software.
- *Boot-Sector Virus*—A boot-sector virus is a virus that infects a computer's master boot record. Once the computer is turned on, the boot-sector virus executes, potentially damaging large amounts of data or actually destroying the master boot record, which in turn will prevent the operating system from loading.
- *Trojan or Trojan Horse*—This type of malware appears to perform a desired function but in fact performs malicious functions.
- *Logic Bomb*—A logic bomb is a piece of code inserted into a program that will perform specific malicious functions when specified conditions are met.

As a network administrator, you must be prepared to protect your network against all types of malware. For an updated list of the malware that are currently in circulation and specific steps on how to clean them, visit antivirus protection software Web sites such as [www.symantec.com](http://www.symantec.com).

**Virus Prevention Software** Virus prevention software is absolutely necessary and should be listed high on the priority list. Virus prevention software is available for installation on entire networks, and usually includes a version that will run on clients as well as servers. Application-specific virus prevention programs are also available. For example, if the network has an e-mail server, a version of the virus protection software will run on the e-mail server and scan all incoming and outgoing messages for malware.

After virus prevention software has been installed, it must be updated regularly to ensure your network is protected against all the latest malware threats. Such software is only as good as its latest update. You should check with the virus prevention software vendor for details about the company's release schedule for updates. Most vendors release updates on a weekly basis, but some will release more often, with special updates released in the event of a large-scale outbreak.

The virus prevention industry is a reactive industry. That means your virus prevention software cannot protect your network until two things happen: 1) the antivirus software vendor puts out an update that will clean the virus; and 2) the virus prevention software on your network is updated. Virus updates can be completed by the end user or by a central virus protection server.

**User Training** User training is paramount in protecting against viruses. First, users must be trained to update their antivirus software daily or, at a bare minimum, weekly. Updates are normally done over the Internet and often take less than five minutes. Antivirus software that is not updated is virtually useless against new malware signatures. Users also must learn how viruses are transmitted between computers. Teach users to scan removable devices (such as jump drives or zip disks) with the virus scanning software before using them, especially if they are from untrusted sources. Also, your security policy should state that if users receive e-mails from unknown sources users should delete them. Also the security policy should instruct users to never open an attachment on an e-mail if they are unaware of the attachment's contents.

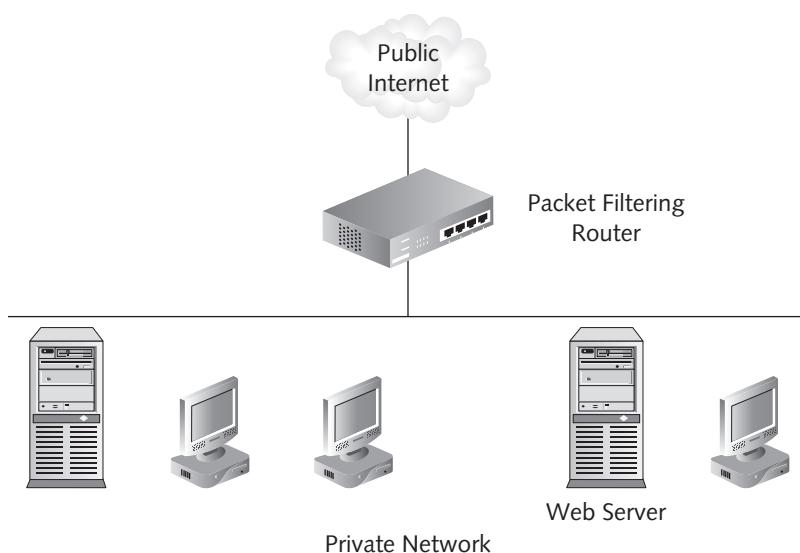
## Firewalls

The primary method of keeping hackers out of a network is to implement a **firewall**. Firewalls are normally placed between a private LAN and the public Internet, where they act like gatekeepers. A firewall can be a hardware device or it can be software. Firewalls also differ according to what they are designed to protect. A personal computer can run a personal firewall that only protects that individual computer from intrusion. An enterprise firewall would sit at the edge of a corporate network and protect the entire network. The CCNA exam focuses on enterprise firewalls.

All data packets entering or exiting the network have to pass through an enterprise-level firewall. As the data pass through, the firewall filters (or analyzes) packets to prevent potentially unapproved data from entering or exiting the network. Firewalls can filter packets based on source address, destination address, port numbers, and other criteria.

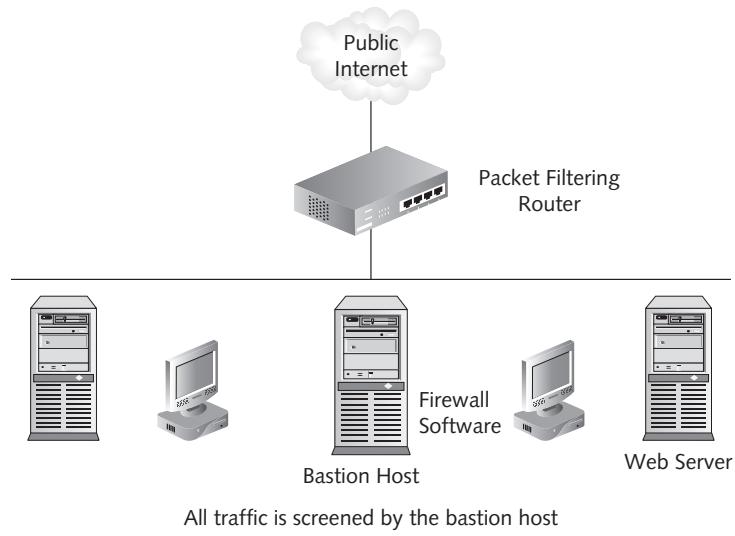
When setting up a firewall, you can choose from four firewall topologies:

- *Packet-filtering router*—This is the least protective of the four topologies. It consists of a router monitoring IP packets as they enter the router from the public side and then allowing or denying them access to the network based on defined rules or criteria (see Figure 14-2). Using access lists on routers, as described in Chapter 10, is an example of creating packet filtering firewalls using a standard Cisco router.



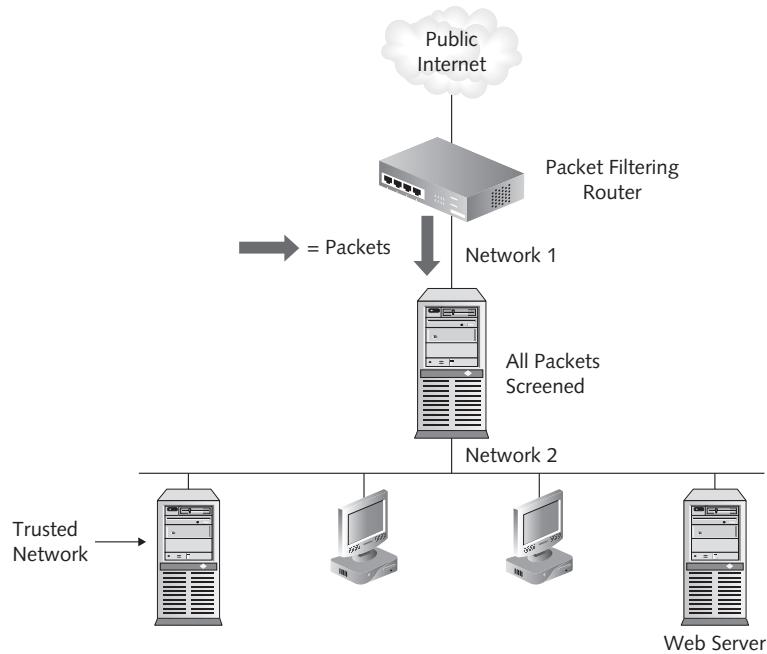
**Figure 14-2** Packet-filtering router

- *Single-homed bastion*—This topology consists of a packet filtering router that forwards all incoming packets to the firewall software on a bastion host. (A **bastion host** is a server running a single application, such as a proxy server or specialized firewall software.) The bastion host then determines whether or not the data can be forwarded to a host on the network. See Figure 14-3. A single-homed bastion only has one network interface card and is assigned only one IP address.



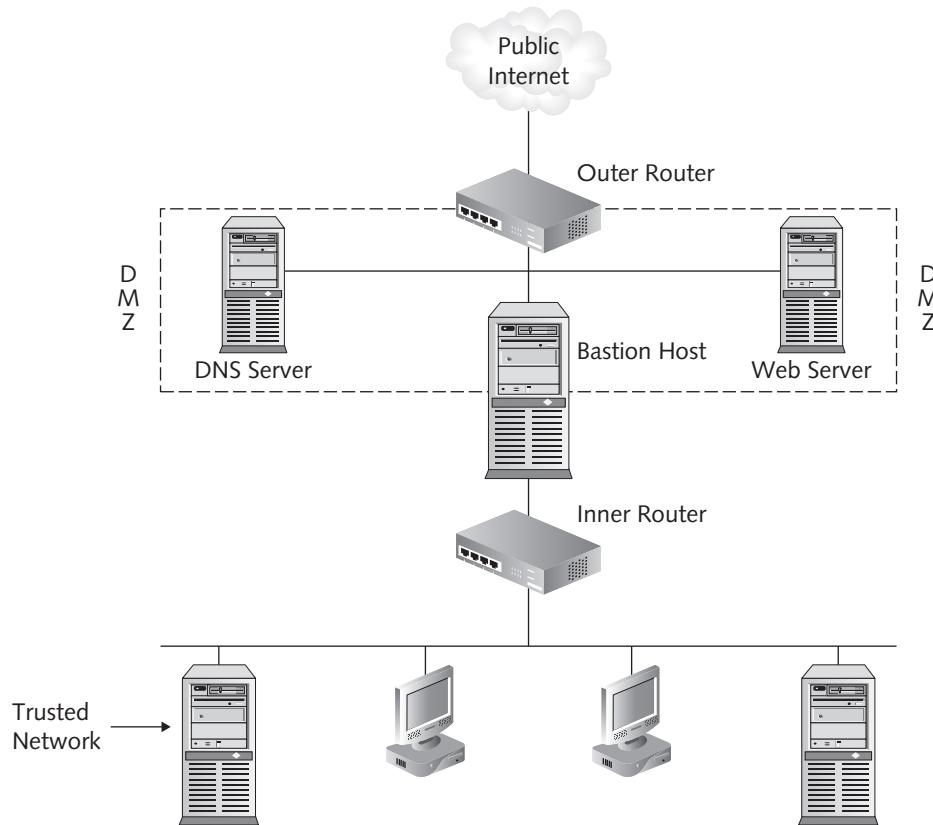
**Figure 14-3** Single-homed bastion

- *Dual-homed bastion*—A dual-homed bastion topology works like a single-homed bastion topology, except that it has two network adapter cards in it and two IP addresses, one for each network it is connected to. One attaches to the packet filtering router and the other connects to the internal network. This physical division of networks adds increased security (see Figure 14-4).



**Figure 14-4** Dual-homed bastion

- *Demilitarized zone (DMZ)*—A DMZ consists of two packet filtering routers. One is positioned between the Internet and the Internet-accessible servers in a screened subnet. The other is a packet filtering router that connects the internal network to the screened subnet. This is the most secure firewall solution. See Figure 14-5.



**Figure 14-5** Demilitarized zone

14

Other popular hacker prevention devices include **Intrusion Detection Systems (IDS)** and **Intrusion Prevention Systems (IPS)**. An IDS is a security device that can detect a hacker's attempts to gain access to the network. They can also detect virus outbreaks, worms, and distributed denial of service (DDoS) attacks. Traditionally, an IDS is not placed in line on the network, so it is not capable of dropping packets. It is actually designed to listen to all traffic on the network, similar to a network management station. An IPS is like an IDS, except that it is placed in line so all packets coming in or going out of the network pass through it. This allows an IPS to drop packets based on rules defined by the network administrator.

## Permissions, Encryption, and Authentication

If a hacker is able to find a line of attack through the firewall, you want to be sure that he encounters a series of frustrating mechanisms that prevent him from actually accessing data. These mechanisms include permissions that control access to network resources, data encryption, and the authentication requirement.

**Permissions** In network security, a **permission** is an official approval that allows a user to access a specific network resource. For example, a user must have permission to access a Cisco router or switch. Typically, permissions governing such devices require the user to supply a password before access is granted. Many Cisco devices do not allow remote access without a password.



Approximately 80 percent of all malicious hacking of resources takes place from users within the internetwork.

NOTE

**Encryption** Encryption at the network level often consists of using security algorithms to scramble and descramble data. Algorithms used include symmetric-key encryption and asymmetric-key encryption.

- **Symmetric key**—Symmetric key encryption is a single-key encryption method. A message is encrypted and decrypted through the use of the same key. The drawback of this method is that, if a malicious user learns the key, all encrypted messages become compromised (see Figure 14-6).

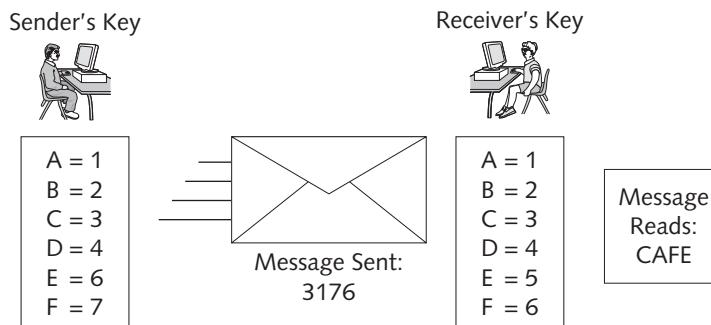


Figure 14-6 Symmetric key encryption

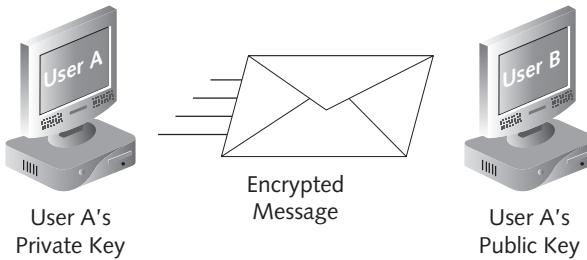
- **Asymmetric key**—Asymmetric, or public key encryption, is more secure than symmetric key encryption, however it is slower. Public key encryption uses a mathematically matched key pair. Each user in this instance would have a public and a private key. The private key remains private to the individual user, whereas the public key can be shared. Data encrypted with the private or public key must be decrypted with the opposite key, as shown in Figure 14-7.

If a hacker attempts to steal data from the network through the use of a packet sniffer, encryption keys will not allow the data packets to be read unless the user has the correct key.



Most advanced encryption methods today use hybrid encryption, which is a combination of both symmetric and asymmetric methods.

NOTE



- Message is encrypted with user A's Private key
- User B must have user A's public key to decrypt the message

**Figure 14-7** Asymmetric key encryption

- *Secure Sockets Layer*—SSL is a means of encrypting a session between two hosts through the use of digital certificates, which are based on asymmetric key encryption. Digital certificates can provide authentication for organizations that transmit data over the Internet.

**Authentication** Authentication is the process by which users verify to a server that they are who they say they are. There are several types of authentication. The password authentication protocol (PAP) and the challenge handshake authentication protocol (CHAP) are both authentication protocols. Cisco also supports additional authentication services such as the Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+). RADIUS is an industry-standard protocol that simply provides authentication service.

You can configure RADIUS on Cisco devices or on other devices such as servers. For example, you can have the RADIUS service running on a server and you can define the RADIUS parameters on a firewall. When a user connects to the firewall, they will be required to authenticate themselves against the RADIUS server.

TACACS+ provides the same service, but is proprietary to Cisco. These two common security protocols are based on the **Authentication, Authorization, and Accounting (AAA)** model. The steps of the AAA model are as follows:

- *Authentication*—The process of validating users.
- *Authorization*—The process of regulating a user's allowable activities on a device, based on the permissions defined for that user.
- *Accounting*—The process of tracking user activity on the network. Also known as auditing.

RADIUS and TACACS+ are services that apply these principles by maintaining a user database that users authenticate against when logging in. The RADIUS protocol is governed by RFC 2865 and can be used with cross-platform integration, meaning that not all devices in a RADIUS authentication stream have to be Cisco devices.

14

## Mitigating Security Threats

The three basic strategies for mitigating security threats are: using the SSH protocol to connect to your routers and switches rather than telnet; turning off unnecessary services; and keeping up-to-date on security patches (software releases) with a patch management initiative. Taking these three steps is paramount in your effort to maintain a secure network.

## Secure Shell (SSH) Connections

In Chapter 5, you learned how to connect to a router via the telnet protocol. One interesting fact about the telnet protocol is that all data that traverses the connection is in clear text. In other words, if someone is running a packet sniffer (software that can analyze data packets) on your network, they can capture all of the data (including passwords) that travels from the host to the router you are connecting to. Once the hacker has the information required to login to the router, he would have free access to the network. One way to prevent such a potentially devastating security breach is to connect to a router or switch using only the Secure Shell (SSH) protocol.

The two version of SSH are SSH Version 1 and SSH Version 2. SSH Version 2 is the recommended version, because it incorporates corrections to vulnerabilities identified in SSH Version 1. Setting up SSH is fairly straightforward, requiring only a few commands to enter at the CLI.

Be aware that some SSH commands are mandatory and others are optional. For example, a hostname and a domain name must be configured for the router. You must also generate an RSA key pair (asymmetric key encryption), which enables SSH. You have the option to set time out values and authentication retries as well as the option of implementing SSH on as many VTY lines as you would like. The preferred method is to implement SSH on all VTY lines, which ensures that all remote IP sessions to the router will be protected in the SSH tunnel. The command sequence for enabling SSH is:

```
Router(config)#hostname SshRouter
SshRouter(config)#ip domain-name sshtest.com
SshRouter(config)#crypto key generate rsa
The name of the keys will be: SshRouter.sshtest.com
[output omitted]
```

After you enter the preceding commands, you are prompted to enter the size of the key generated. The options range from 360 to 2048 bits—the greater the number, the more complex the key. The remaining commands for implementing SSH are as follows:

```
SshRouter(config)#ip ssh time-out 60
SshRouter(config)#ip ssh authentication-retries 3
SshRouter(config)#line vty 0 4
SshRouter(config-line)#transport input ssh
```

## Disabling Unnecessary Services

Many services that run on a Cisco device can be used for malicious purposes. Some of these services are turned on by default. You should disable the services unless your organization uses them, using one of two methods. First, you can go through the CLI and enter a series of commands for each service. This is effective but time-consuming. The second method is to use the Security Audit Wizard in the Cisco Security Device Manager (SDM). This service will examine your router and recommend which services should be disabled. It will also enter the commands for you. The SDM Audit Wizard is covered later in this chapter.

The following services are unnecessary on most networks:

- Finger Service
- PAD Service
- TCP Small Servers Service
- UDP Small Servers Service
- IP Bootp Server Service
- Cisco Discovery Protocol (CDP)
- IP Source Route
- Maintenance Operations Protocol (MOP)
- Directed Broadcast
- ICMP Redirects
- Proxy ARP
- IDENT
- IPv6

Remember, if your organization uses these services, you should not disable them. For example, if your network runs in an IPv6 environment, you would obviously not disable IPv6.

---

## Patch Management

Ensuring that your organization has a successful patch management program is critical to protecting sensitive data and equipment. New worms and viruses are unleashed by the hour, and they often attack security vulnerabilities that have been publicized by software vendors. Thus, your organization's patch management program should account for all software in the organization, including operating systems for servers, workstations, routers, switches, and any other device connected to the network, even printers. It should also take into account commercial applications as well as applications developed in-house.

A patch management program should take into account the major software vendor's patch release schedules as well as your organization's business goals and needs. For example, if a vendor releases security patches on the second Tuesday of every month, but your organization also has a critical billing cycle on the second Wednesday of every month, then it would not be advisable to implement the patches so close to a critical business function. However, it is possible to install the patch in a test environment and let it run through a test billing cycle. This way you will be ensured that the patch will not adversely affect next month's billing cycle.

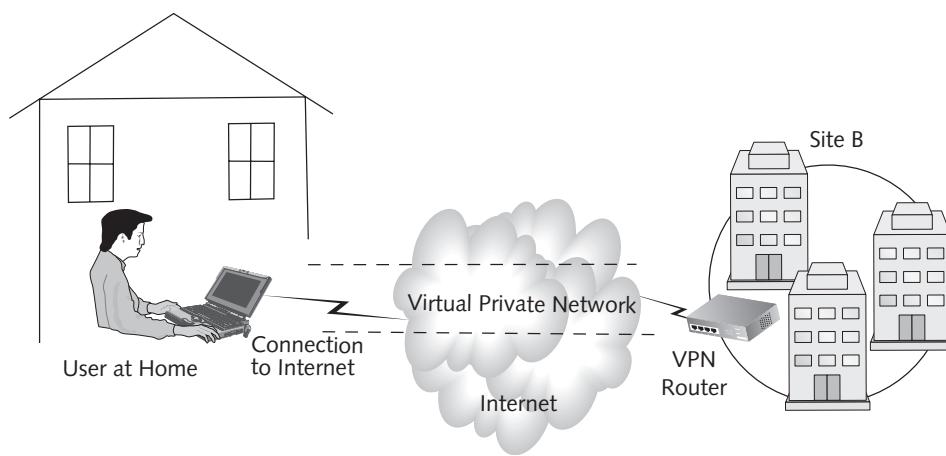
Not all patches released by vendors are flawless, so it is imperative that you establish a test environment. In addition to creating a test environment for each patch, you should establish a realistic patch schedule that your organization can follow.

Patch management can be done manually or it can be done by a patch management software package. Many packages are available, including Symantec's Altiris or Microsoft's SMS server. The decision to use manual or automated patch management will be driven by several factors, including available manpower, cost of software, and reliability of the software versus reliability of the technician doing the updates.

## Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) are a popular technology for creating a connection between an external computer and a corporate site over the Internet. To establish a VPN connection, you need VPN-capable components such as VPN-enabled firewalls and, depending upon the configuration, a VPN software client. VPNs can also be set up with popular vendor operating systems. For example, Microsoft's server operating systems have supported VPN creation for years. The two main types of VPNs are Client-to-Site VPNs and Site-to-Site VPNs.

A client-to-site VPN (also known as remote user VPN) is a VPN that allows designated users to have access to the corporate network from remote locations. These types of VPNs are extremely popular with companies that allow users to telecommute or that have a traveling sales staff. The requirements for a client-to-site VPN include a permanent Internet connection at the corporate site and an Internet connection for the user. The user's Internet connection does not necessarily have to be a permanent connection. It can be a dial-up connection or an Internet connection in a public area. Figure 14-8 shows a client-to-site or a remote user VPN.

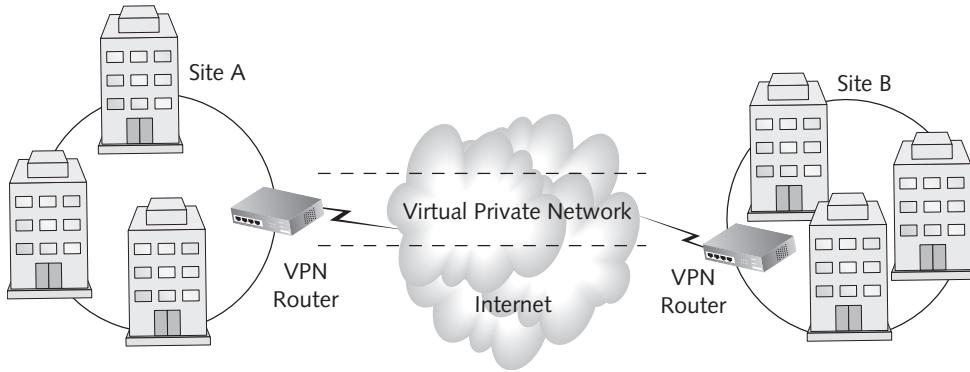


**Figure 14-8** A client-to-site or a remote user VPN

A site-to-site VPN is a VPN that allows multiple corporate sites to be connected over low-cost Internet connections. The requirements for a site-to-site VPN include a permanent Internet connection and VPN-compatible devices such as firewalls at each location. VPNs can also be used with encryption-based technologies to secure the virtual tunnel over which data travels. Figure 14-9 shows a site-to-site VPN.

You can choose from several tunneling protocols to create secure, end-to-end tunnels. The three most popular tunneling protocols are:

- *Point-to-Point Tunneling Protocol (PPTP)*—PPTP is a tunneling protocol that was developed by Microsoft and was extremely popular at one time for remote users who had to dial in to the corporate network on a secure channel. One interesting fact about this protocol was that it could carry multiple other protocols within the tunnel, including NetBEUI, which is a Microsoft proprietary, nonroutable protocol.
- *Layer 2 Tunneling Protocol (L2TP)*—L2TP is a newer tunneling protocol based on Cisco's L2F protocol and Microsoft's PPTP. It is now preferred over PPTP.



**Figure 14-9** Site-to-site VPN

- *Generic Routing Encapsulation (GRE)*—GRE was developed by Cisco as a proprietary protocol but is currently governed by several RFCs. GRE is not designed to provide a secure tunnel. It is designed to allow multicast traffic to pass through the VPN tunnel. To create an encrypted tunnel you would use additional protocols. The protocol of choice to encrypt the unencrypted data is IPSEC, which is covered next.

## IPSec

IPsec is a suite of protocols, accepted as an industry standard, which provides secure data transmission over layer 3 of the OSI model. IPsec is an IP standard and will only encrypt IP-based data. In the event you needed to encrypt protocols other than IP, you would have to create a separate tunnel and then encrypt the entire tunnel with IPsec.

IPsec supports two modes of operation: transport mode and tunnel mode. **Transport mode** is primarily geared toward encrypting data that is being sent host-to-host. It only encrypts and decrypts the individual data packets, which results in quite a bit of overhead on the processor. **Tunnel mode**, on the other hand, encrypts all data in the tunnel and is the mode supported by Cisco components. IPsec includes various protocols and hashing algorithms, all of which are covered in the following sections.

### IPSec Protocols

Two IPsec protocols have been developed to provide packet-level security. They include the following characteristics:

- *Authentication Header (AH)*—This authentication protocol does not provide encryption, but it does ensure the integrity and origin of the data. This is done by computing a hash-based message authentication code over the fields of the IP packet. It then stores this information in its own AH header embedded within the IP Packet. The values at both ends of the communication string must match.
- *Encapsulating Security Payload (ESP)*—This encryption protocol, which optionally supports authentication as well, works differently than AH. Whereas AH only adds header information to the data packet to ensure integrity and origin, ESP encrypts the data by surrounding the payload. It uses cryptographic algorithms to encrypt the data and ensures confidentiality. These algorithms are covered next.

## IPSec Authentication Algorithms

IPSec uses several algorithms to provide authentication services. The authentication algorithms use one of two **Hashed Message Authentication Codes** (HMAC) called **MD5** (message-digest algorithm 5) and **SHA-1** (secure hash algorithm). An HMAC is a secret key authentication algorithm that ensures data integrity and originality based on the distribution of the secret key. Cryptographic software keys are exchanged between hosts using an HMAC. When a transfer of data between the two hosts occurs, the value of the keys is checked; if the value is correct, then the origin and integrity of the data are intact. MD5 and SHA-1 are the two HMACs supported by the AH protocol and optionally with the ESP protocol.

## IPSec Encryption Algorithms

For encryption, the two most popular algorithms on IPSec networks are **3DES** (tripleDES) and **AES**. These protocols are used solely with the IPSec ESP protocol. Remember, AH does not support encryption.

## IPSec Key Management

When managing an encrypted network, you need to give careful thought to the encryption keys. In particular, you need to pay attention to how keys are handed from node to node during IPSec authentication. Two options are available. One option is to deliver the secret keys to all parties involved via e-mail or on disk. The second option is to utilize a key management protocol. Key management is defined by the **Internet Security Association and Key Management Protocol (ISAKMP)** and governed by RFC 2407 and 2408. Although ISAKMP provides the framework for key exchange, the actual **Internet Key Exchange (IKE)** protocols are governed by RFC 4306.

## IPSec Transform Sets

To configure a Cisco router in order to incorporate an IPSec VPN into your internetwork, you need to use an IPSec transform set. A **transform set** is a configuration value (or simply stated, a command) that allows you to establish an IPSEC VPN on a Cisco firewall. You can create a transform set through the CLI or you can simply use the SDM GUI.

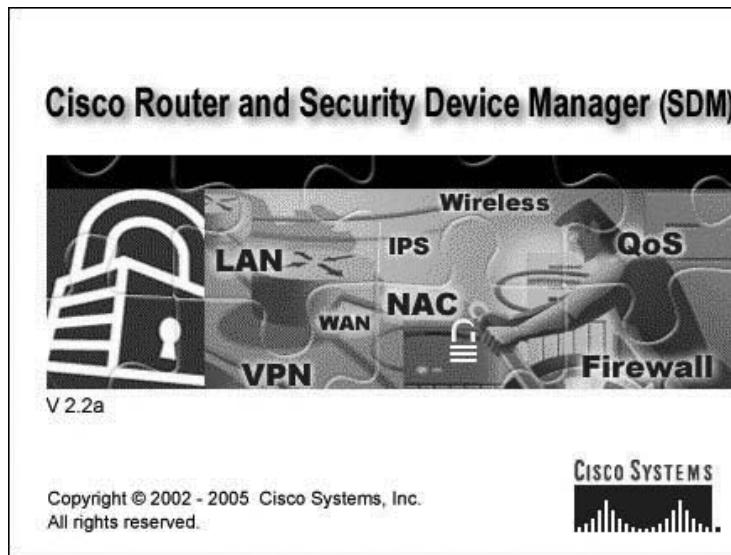
When creating an IPSec VPN you must specify a protocol, the algorithm, and the method of key management. If you use the SDM to build the VPN, dealing with all these details is not as complicated as it sounds. The SDM builds the transform sets for you.

## Creating VPNs with the Security Device Manager (SDM)

Cisco supports VPNs with several different devices. For example, VPNs can be created on firewalls, routers, computers, and even on a device specifically made for VPNs, called a VPN concentrator. This book focuses on using the Cisco Security Device Manager (SDM) Web utility to create a VPN on a Cisco router.

The following example shows how to configure one side of the VPN. These steps assume that the remote site has already been configured. The figures included in the following example were created on a Cisco 2611 series router.

1. From a supported Web browser, enter the IP address of the router interface that you want to connect to the SDM. Enter your username and password when prompted.
2. The SDM flash screen (as shown in Figure 14-10) appears, and then you are prompted to enter your username and password again.



**Figure 14-10** SDM Flash Screen

3. The SDM home page appears, as shown in Figure 14-11. Take a moment to review this page, which provides a great deal of valuable information.

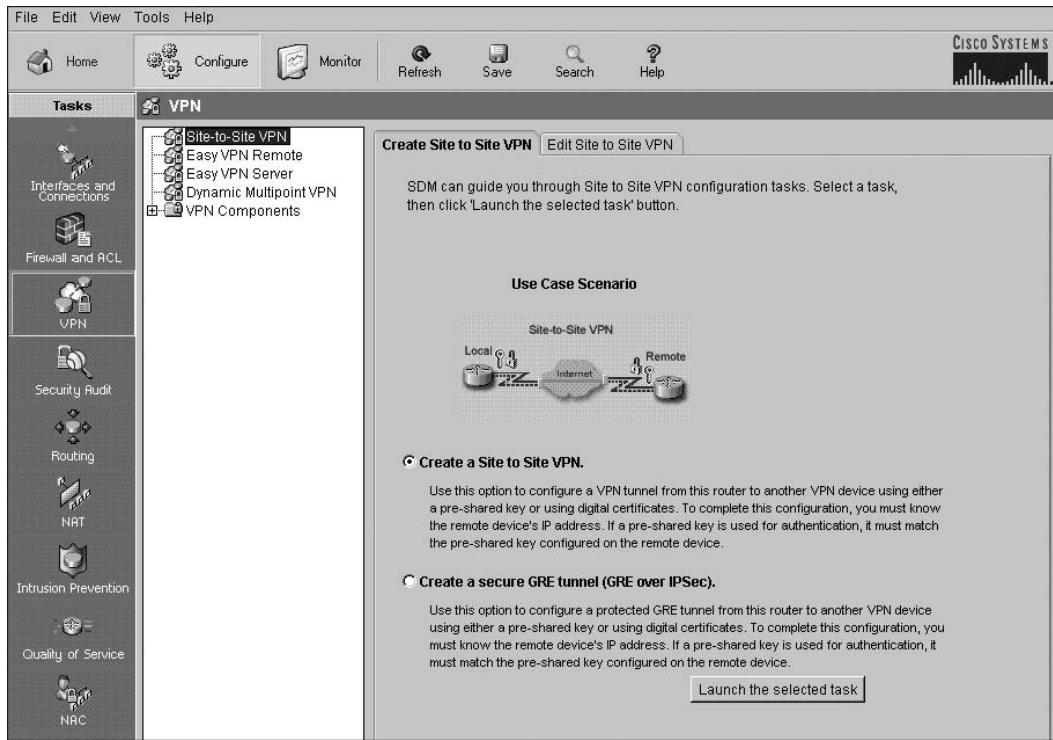
The image shows the Cisco SDM Home page. The interface has a standard Windows-style menu bar at the top: File, Edit, View, Tools, Help. Below the menu is a toolbar with icons for Home, Configure, Monitor, Refresh, Save, Search, and Help. The main content area is divided into several sections:

- About Your Router**: Displays the router's model (Cisco 2611XM), hardware details (Available / Total Memory: 768/28 MB, Total Flash Capacity: 32 MB), and software details (IOS Version: 12.3(3), SDM Version: 2.1). It also shows feature availability for IP, Firewall, VPN, IPS, and NAC.
- Configuration Overview**: Shows the number of up and down interfaces, total supported WAN connections (1 Serial, 1 FR), and various policy counts for Firewall Policies, VPN, and Routing.
- View Running Config**: A link located in the Configuration Overview section.
- Links**: A sidebar on the left containing links to "About SDM", "SDM Home Page", "Cisco Support", "Cisco Product Support", "Cisco Product Support", and "Cisco Product Support".

**Figure 14-11** SDM Home page

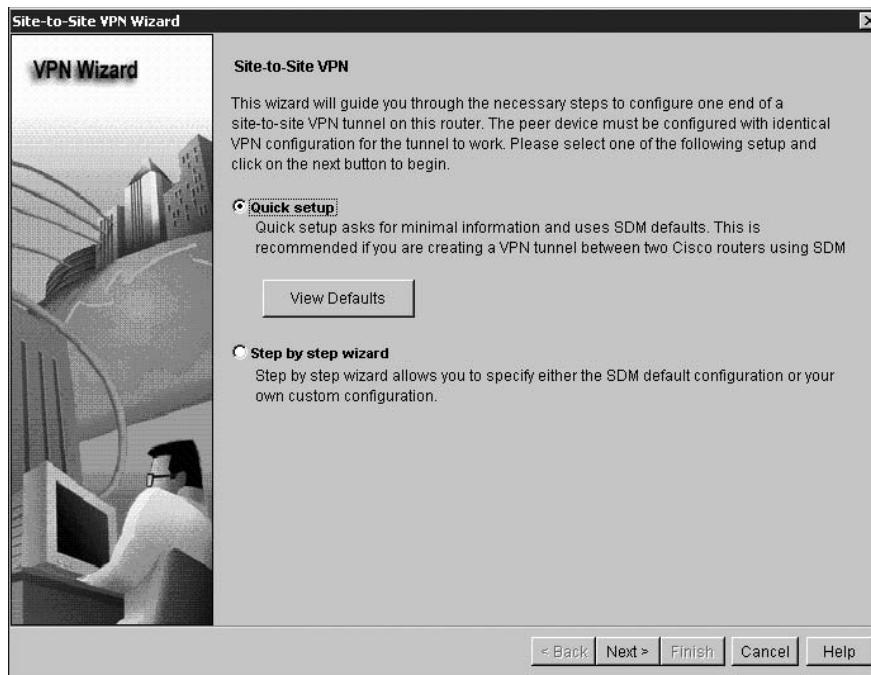
## 404 Chapter 14 Network Security

4. To configure a router from within the SDM, click the **Configure** button at the top of the Home page. Configuration options appear on the left side of the window. You can click an option in the Tasks pane (on the far left side of the window) and then review the options related to that task on the right side of the window.
5. Click **VPN** in the Tasks pane. To the right of the Tasks pane, a list of options related to VPN is displayed. You can select any option in this list, and read more about that particular option on the right side of the window.
6. In the middle (white) pane, click **Site-to-Site VPN**. Information about creating site-to-site VPNs is displayed on the right side of the window, as shown in Figure 14-12.

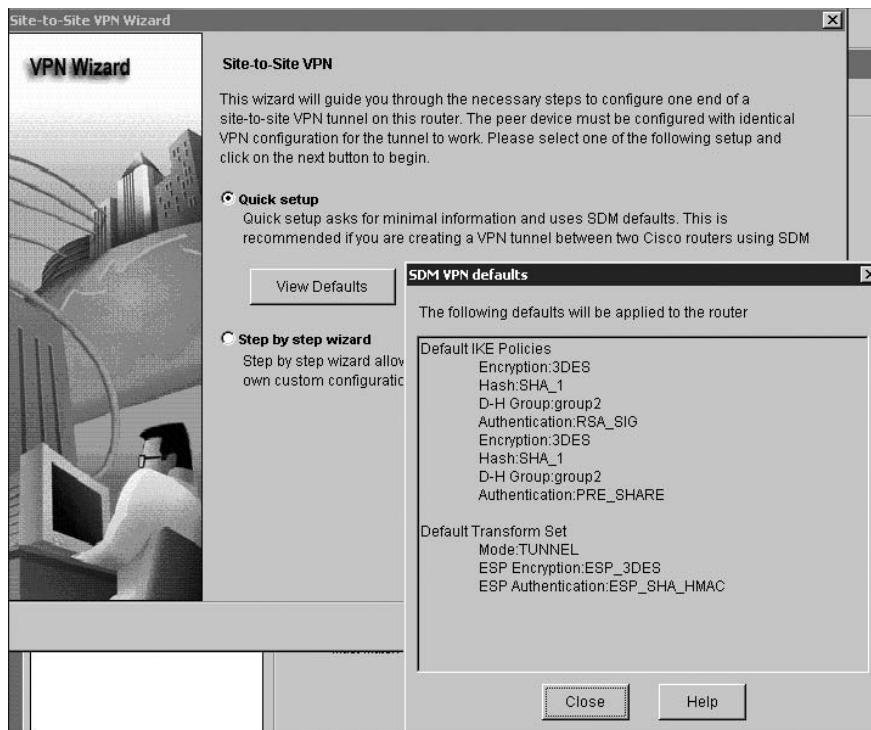


**Figure 14-12** VPN button selected in the Tasks pane

7. In the bottom-right corner of the window, click the **Launch the selected task** button to display the Site-to-Site VPN page shown in Figure 14-13. This is the first page of the Site-to-Site VPN Wizard.
8. You have the option of using Quick setup or building the VPN using the step-by-step wizard. It is recommended that you use Quick setup, but first you should review the default settings used by Quick setup.
9. Click the **View Defaults** button. Figure 14-14 shows the default VPN settings.



**Figure 14-13** First page of the Site-to-Site VPN Wizard



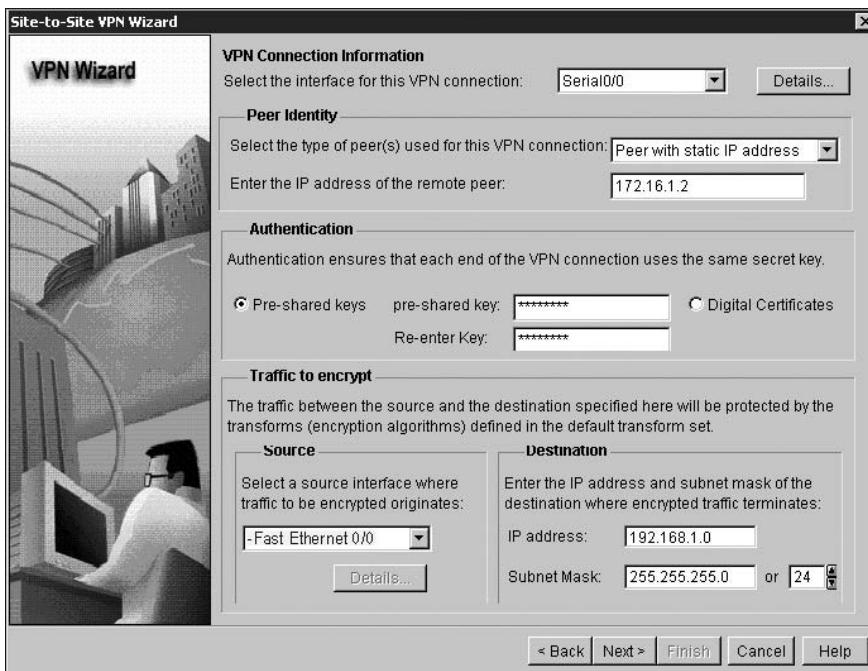
**Figure 14-14** Default VPN Settings



**NOTE**

The VPN settings applied to this router must be the same VPN settings applied to the remote site router. Remember, when configuring a site-to-site VPN, you need to make sure both routers use the same settings; otherwise, the VPN authentication will fail.

10. Document the default VPN settings by printing the screen or writing the information down.
11. Click **Close** to close the page displaying the default VPN settings, and then click **Next** to proceed with Quick setup. This displays the VPN connection information screen shown in Figure 14-15. This screen is divided into several sections, where you can supply information about the IP addresses that will be affected by this VPN tunnel. (Note that Figure 14-15 shows this page after the desired settings have been selected. You should refer to this figure for steps 11 through 16.)



**Figure 14-15** VPN Connection Information Screen

12. In the **Select the interface for this VPN connection** drop-down menu (at the top of the screen), select the interface that you want to connect to the remote router. This is most likely an external (WAN) interface. In Figure 14-15, Serial0/0 is selected.
13. In the **Peer Identity** configuration section of the screen, click the **Select the type of peer(s) used for this VPN connection** drop-down menu, choose **Peer with a static IP address** (as shown in Figure 14-15) and enter the IP address of the remote peer. In this example we are using private IP addresses. However, in a real-world situation, you likely will have to enter a public routed IP address in the **Peer Identity** section. You can obtain that information from the remote site router.
14. In the **Authentication** configuration section choose **Pre-shared keys** and enter a secure key twice. Be sure to use a complex string of characters for security purposes. You should

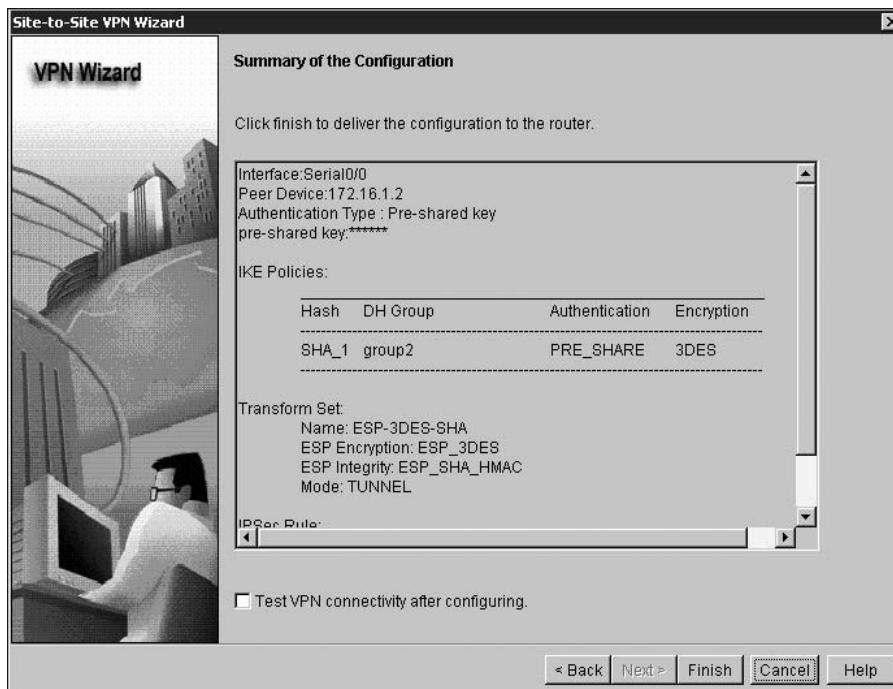
also write this key down and keep it somewhere safe. You should use the same key here as you use (or used) on the remote router.



NOTE

An example of a secure key is Z7p@Week9N. The mix of uppercase and lowercase letters, numbers, and special characters make this a secure key.

15. In the **Traffic to encrypt** section of the configuration page you need to identify the traffic you want to encrypt. The two subcategories to configure are the source of the traffic (that is, the internal interface) and the destination. Under Source, click the down arrow button and choose the internal interface that the traffic will be coming from—for example, Fast Ethernet 0/0. The traffic that travels from the internal interface you specify is eligible for encryption over the tunnel.
16. In the Destination section, you need to add the subnet information for the location where the VPN tunnel ends. Figure 14-15 shows an address other than the Peer IP address. That means the tunnel will be encrypted through the router and onto the private (internal) network of the remote peer. When entering this information you need to know how far the VPN tunnel goes. For example, if the encryption can stop at the entrance point of your network, then you would enter the remote peer's IP address that is assigned to the external interface (172.16.1.2 in this example).
17. Review the page to make sure you have supplied all the necessary information, and then click **Next**. Figure 14-16 shows the Summary of the Configuration page. It also displays

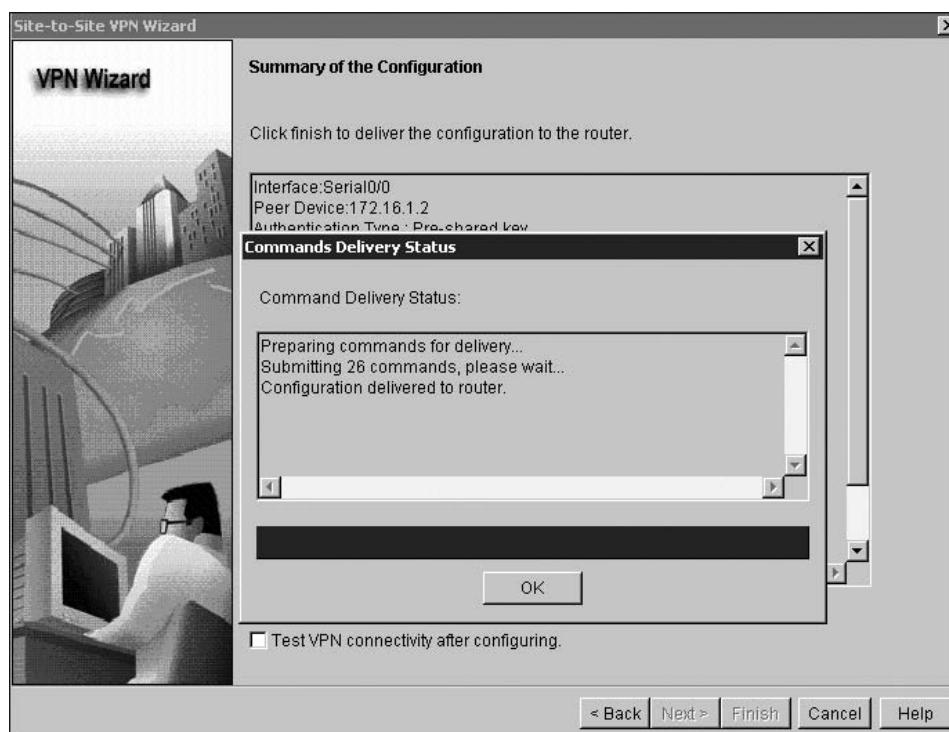


**Figure 14-16** Summary of the Configuration

the Transform Set parameters, which explain what goes into the transform set. The parameter information includes:

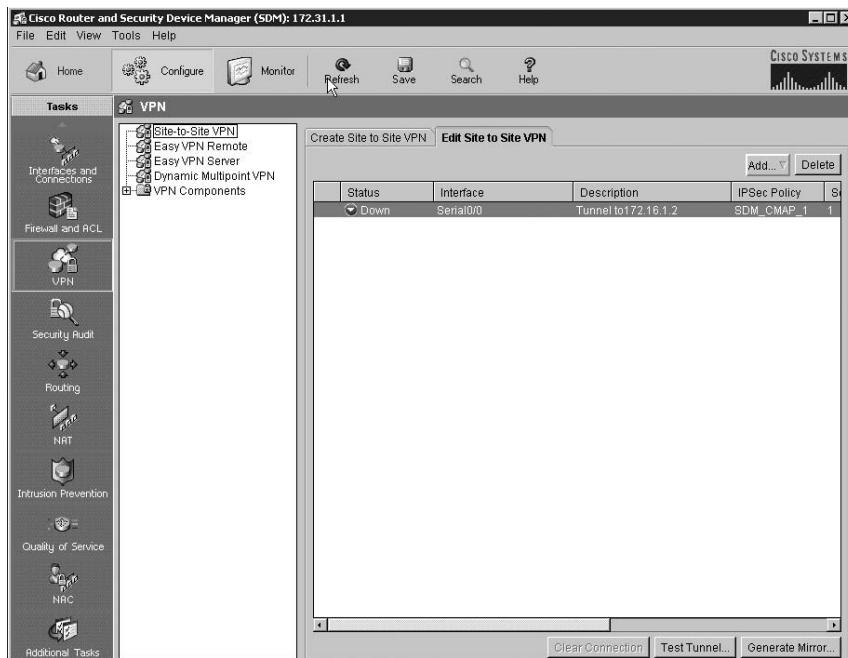
- Transform Set Name : ESP-3DES-SHA
- ESP Encryption algorithm used: ESP\_3DES
- ESP Integrity (authentication) algorithm used: ESP\_SHA\_HMAC
- Mode: TUNNEL

18. Review the settings to make sure they are correct. If there is a problem with your configuration, use the Back button to reconfigure the settings. Once you are sure everything is correct, click the Finish button. The Commands Delivery Status dialog box opens, as shown in Figure 14-17. This tells you that the VPN is being created. In Figure 14-17, the message states that 26 commands are being written to the router's configuration. (This suggests that, by using the Quick Setup option, we avoided quite a bit of command-line configuration.)



**Figure 14-17** Commands Delivery Status dialog box

19. Finally, the SDM indicates that the VPN has been created, but that it is currently inoperable (or down). Cisco VPNs do not become operational (come up) until traffic is sent through the VPN. Notice, also, the Test Tunnel button at the bottom of the Edit Site to Site VPN tab, which you can use to test your configuration. Use the Test Tunnel button to verify connectivity at any time or when troubleshooting your VPN. See Figure 14-18.



**Figure 14-18** VPN Down



To generate traffic through the VPN, use the ping command to ping hosts that are located on opposite ends of the tunnel. Once that has been completed, the VPN will be active.

Remember, you can also build a VPN by using the CLI. This takes more work, but some technicians prefer this method because it allows you to see each command as it is entered into the router. Regardless of whether you enter the commands in the CLI or use the SDM, the result is the same: Data travels over an end-to-end encrypted tunnel, which is the ultimate goal for securing information.

## Cisco Security Audit Wizard

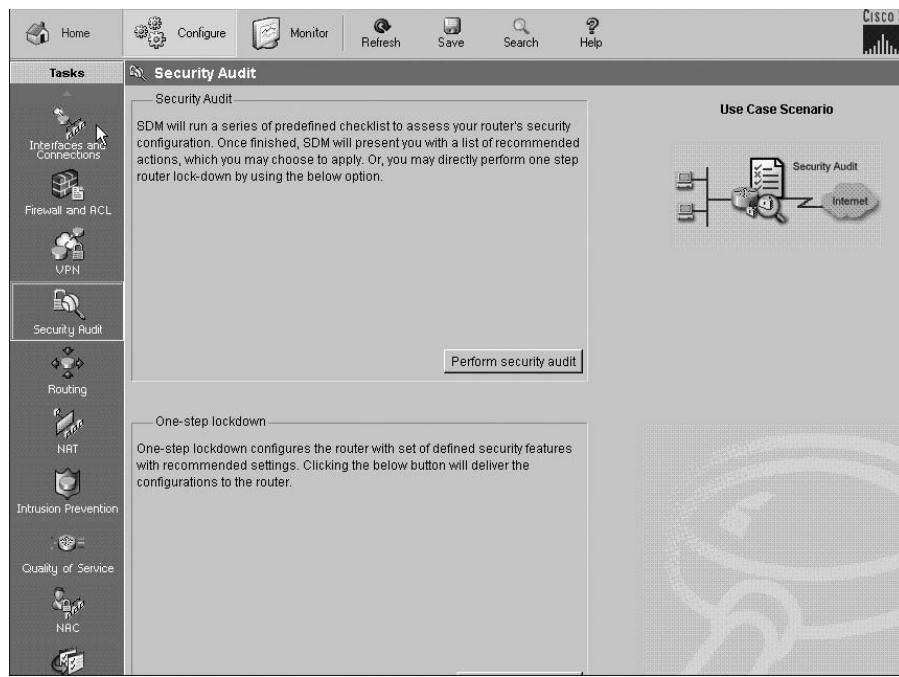
14

In addition to configuring VPNs, you can use the Cisco SDM to conduct security audits. The SDM's Security Audit Wizard can be used to verify your router's configuration and determine what security settings have and have not been configured. It will also make recommendations as to which settings should be enabled. Finally, it provides an easy to use GUI that allows you to make those changes.

To utilize the SDM Security Audit Wizard, perform the following steps:

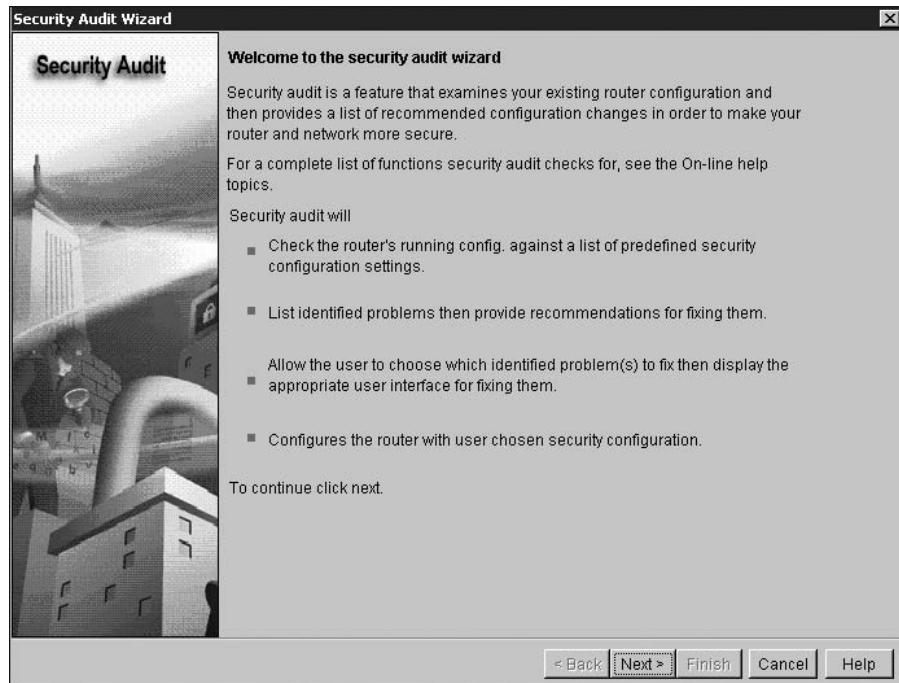
1. Connect to the router's SDM with a supported browser, click the **Configure** button, and then click **Security Audit** in the Tasks pane. Information about security audits is displayed to the right of the Tasks pane, as shown in Figure 14-19. Two options are available: Security Audit and One-step lockdown. One-step lockdown applies any security settings the wizard deems appropriate without your intervention. In this example, your goal is to learn about the Security Audit.

## 410 Chapter 14 Network Security



**Figure 14-19** SDM Security Audit Screen

2. Click the **Perform security audit** button. This launches the Security Audit wizard, as shown in Figure 14-20.



**Figure 14-20** SDM Security Audit Wizard

3. Click the **Next** button. If you are prompted to select interfaces, do so, and then click **Next**. The audit begins. Once it is complete, you see a list of items that have and have not passed the security audit, as shown in Figure 14-21. The results shown in Figure 14-21 indicate that the security audit definitely did its job. The router in this example was set up with only a basic configuration, so security is certainly an area that needs to be addressed.

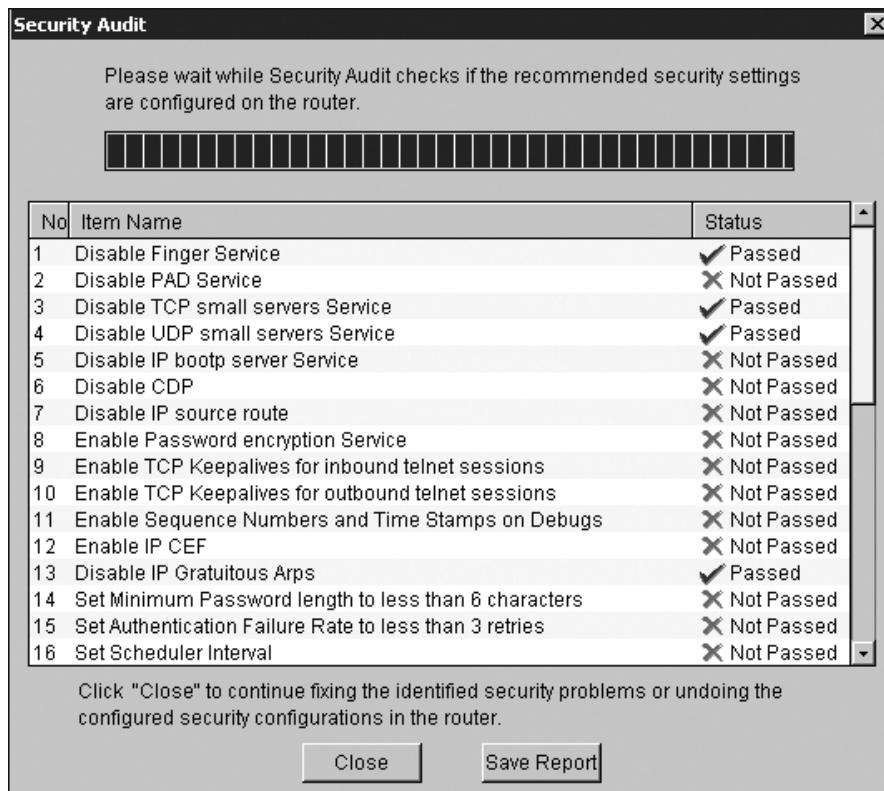


Figure 14-21 Security Audit Results

14

4. Click the **Close** button. A new screen is displayed, allowing you to make the changes required to improve security. See Figure 14-22.
5. Check the boxes for the items you want to fix. In Figure 14-23, the “CDP is enabled” check box has been selected. Selecting this check box tells the Security Audit Wizard that you want to *disable* CDP.

## 412 Chapter 14 Network Security

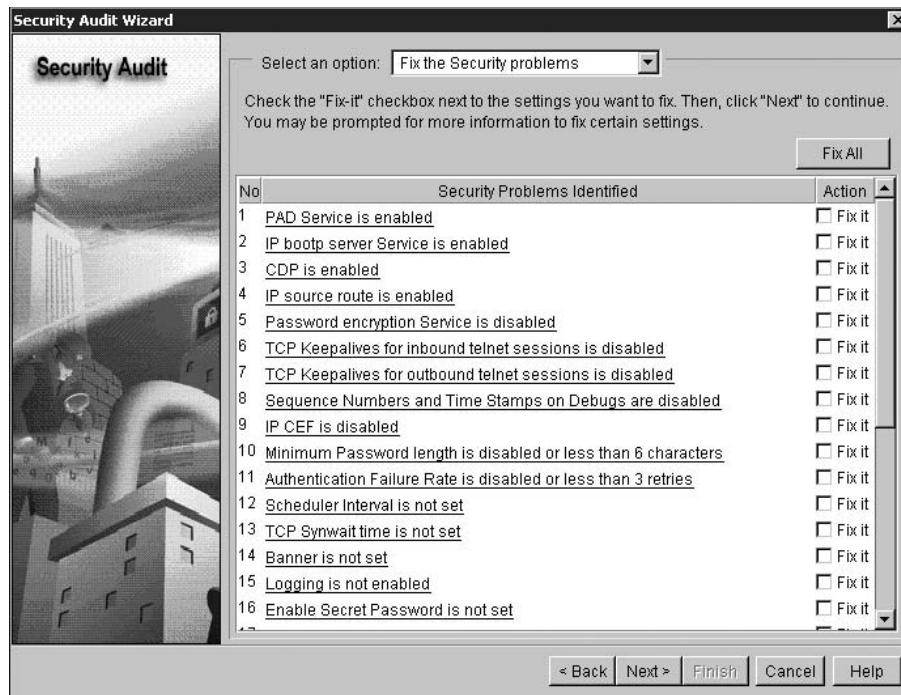


Figure 14-22 Fix the Security problems option

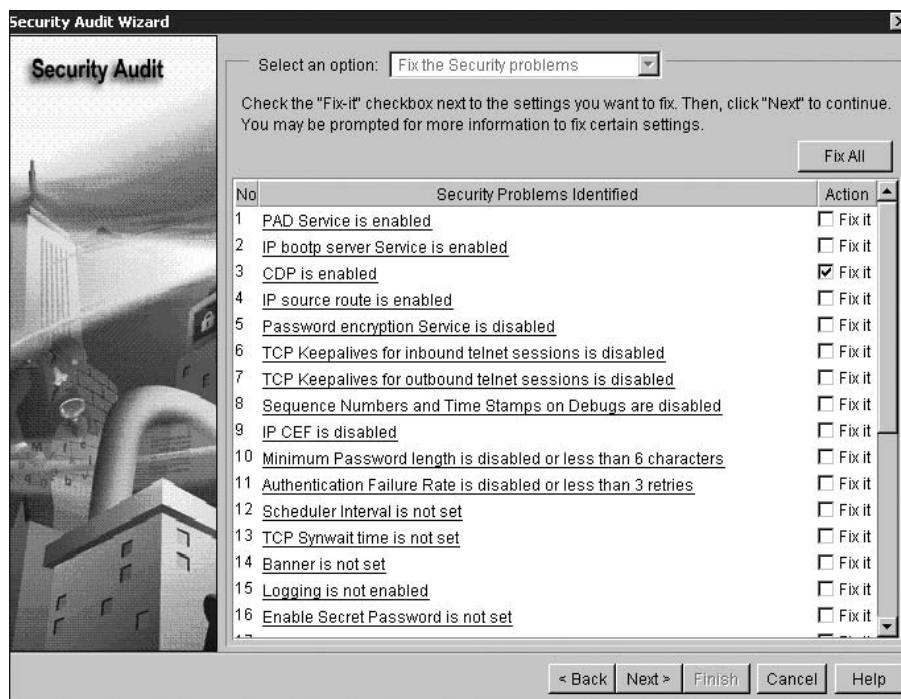


Figure 14-23 CDP check box

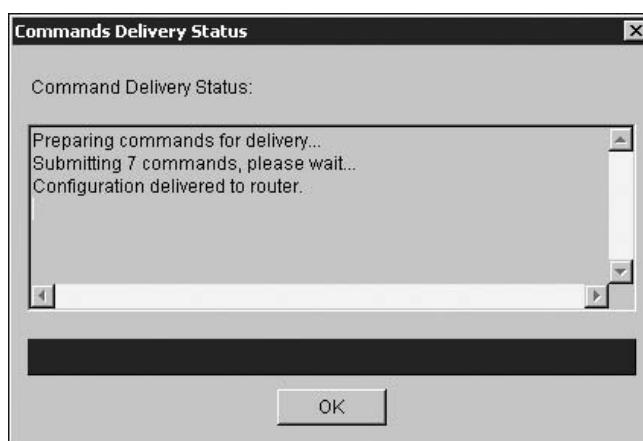
6. After you are finished selecting options to improve your network's security, click **Next**. The Summary screen appears, as shown in Figure 14-24, to confirm your selections.



**Figure 14-24** Summary Screen

7. Click the **Finish** button on the Summary screen. The **Commands Delivery Status** dialog box appears, showing you the status of the commands as they are executed. In Figure 14-25, seven commands are currently being entered into the router to disable only one service.

8. Click the **OK** button to return to the SDM.



**Figure 14-25** Commands Delivery Status

In this example, it only took several clicks of the mouse button to secure a router. As you can see, the SDM Security Audit Wizard is an excellent resource, saving both time and effort.

---

## Chapter Summary

- Protecting the physical equipment where sensitive data resides is as important as protecting the data itself.
- When securing an organization's network, you must be sure to protect it against external threats as well as internal threats.
- User training is a key element to protecting the network and the data within it.
- Using an SSH connection to a router is a much more secure method of connecting to a router than clear text telnet.
- Disabling unnecessary services increases a router's security.
- IPSec is an industry-standard suite of protocols and algorithms that allow for secure encrypted VPN tunnels.
- Cisco's SDM is a multifunction Web utility that allows you to create VPNs and complete a security audit.

---

## Key Terms

**3DES** Encryption algorithm supported by IPSEC.

**AAA (Authentication, Authorization, and Accounting)** A model designed by Cisco to enhance network security.

**advanced encryption standard (AES)** Encryption algorithm supported by IPSEC.

**asymmetric key** A form of encryption that uses a private and public key pair to encrypt and decrypt data.

**authentication handler (AH)**. IPSec protocol that provides authentication services only by adding a header before the payload of an IP datagram.

**authentication** The process of users verifying to a directory services server on the network that they are who they say they are.

**bastion host** A computer built to withstand an attack.

**boot-sector virus** A virus that infects the master boot record of a computer.

**client-to-site VPN** A VPN that allows designated users to have access to the corporate network from remote locations (also known as remote user VPN).

**DDoS** Distributed Denial-of-Service attack. A denial-of-service attack launched by multiple affected computers. The attack is specifically aimed at flooding the destination's available bandwidth.

**demilitarized zone (DMZ)** A firewall design that consists of having two packet filtering routers with a screened subnet available to the Internet.

**dual-homed bastion** A computer on the network that has two network cards in it. This computer is designed to withstand attacks from outside parties.

**encapsulating security payload (ESP)** IPSec protocol that supports encryption and authentication services if needed.

**encryption** The conversion or scrambling of data into a format readable only by descrambling it.

**firewall** A device used to permit or deny traffic between two security domains.

**generic routing encapsulation (GRE)** An unencrypted, Cisco proprietary tunneling protocol.

**hacker** An individual interested in stealing data or breaking into a network for malicious intent.

**hashed message authentication code (HMAC)** Secret key authentication algorithm that ensures data integrity and originality based on the distribution of the secret key.

**internet key exchange (IKE)** IPSec key management protocol.

**internet security association and key management protocol (ISAKMP)** The authority that governs IPSec key management.

**intrusion detection systems (IDS)** A network device that analyzes data packets to detect malicious behavior. An IDS is not installed inline with the network. Therefore it cannot take action on malicious data. However, it can report it.

**intrusion prevention system (IPS)** A network device that analyzes data packets to detect malicious behavior. An IPS is installed inline with the network and has the ability to drop packets that are malicious.

**IPsec** A suite of protocols that has been accepted as an industry standard and provides secure data transmission over layer 3 of the OSI model.

**layer 2 tunneling protocol (L2TP)** An extension of the point-to-point protocol used to create a secure tunnel for data to go through when remotely connecting to a network.

**logic bomb** A piece of code inserted into a program that will perform specific malicious functions when specified conditions are met.

**macro virus** A virus disguised as a macro for a specific application.

**malware** Malicious code that can infect a network. Types of malware include viruses, worms, Trojan horses, and logic bombs.

**message-digest algorithm 5 (MD5)** An authentication algorithm supported by IPsec.

**packet-filtering router** A router designed to examine data packets as they enter the network.

**permissions** Access rights given to a user to determine whether or not that user can access a resource.

**physical security** Physically securing your organization's computer equipment and network devices.

**point-to-point tunneling protocols (PPTP)** A tunneling protocol that creates a secure tunnel for data to go through when remotely connecting to a network.

**polymorphic virus** A virus that changes its appearance (or signature) each time it replicates or infects.

**RADIUS** An industry standard authentication service that can be configured on Cisco devices.

**secure shell (SSH)** A cryptographic protocol that uses public key encryption to secure the communications channel between two hosts on the network.

**secure sockets layer (SSL)** A cryptographic protocol that provides secure communication for data that traverses a network.

**security policy** An organization's set of rules around data management.

**secure hash algorithm (SHA-1)** An authentication algorithm supported by IPSec

**single-homed bastion** A computer built to withstand an attack. This computer has one network card installed in it and forwards all data to a firewall after inspecting it.

**site-to-site VPN** A VPN that allows multiple corporate sites to be connected together over low-cost Internet connections.

**stealth virus** A virus that attempts to hide itself from detection.

**symmetric key** Symmetric key encryption is a single-key encryption method enabling data to be encrypted and decrypted through the use of one key.

**TACACS+** A proprietary authentication service that can be configured on Cisco devices.

**transform set** The configuration parameters in a Cisco firewall IPSEC VPN.

**transport mode** An IPSec mode that is primarily geared toward encrypting data that is being sent host-to-host. It only encrypts and decrypts the individual data packets. It does not provide tunneling services.

**Trojan horse** Malware that appears to perform a desired function but in fact performs malicious functions.

**tunnel mode** An IPSec mode that supports the secure tunneling of all data sent through it.

**virus** Malware that is used to steal or damage data. Requires user intervention to propagate.

**virtual private network (VPN).** VPNs provide for low-cost secure data connections between multiple sites. VPNs can be built as a site-to-site connection, remote user connections, and even between two separate companies' networks (that have a common business requirement), which is considered an extranet.

**worm** Malware that once activated can replicate itself throughout the network by taking advantage of services on the computers in the network.

## Review Questions

1. Which statement accurately defines IPsec?
  - a. IPSec is an authentication protocol.
  - b. IPSec is a Cisco-proprietary suite of protocols that allows for secure communication.
  - c. IPSec is an industry-standard suite of protocols that allows for secure communication.
  - d. IPSec supports RADIUS and TACACS+.
2. Which command establishes an SSH key pair?
  - a. SshRouter(config)#crypto key generate rsa
  - b. SshRouter(config)#crypto-key generate rsa
  - c. SshRouter(config)#crypto generate rsa
  - d. SshRouter(config)#crypto key-generate rsa
3. What two methods can be used to configure VPNs on a Cisco router?
  - a. IPSec
  - b. RADIUS
  - c. CLI
  - d. SDM
  - e. ESP
4. What services are provided by an IPS? (Choose all that apply.)
  - a. examine data packets
  - b. authenticate users
  - c. account for users time on the network
  - d. drop malicious packets
5. What services are provided by an IDS?
  - a. examine data packets
  - b. authenticate users
  - c. account for users time on the network
  - d. insert malicious packets
6. What is the correct command sequence to protect all five of a router's VTY lines with SSH?
  - a. SshRouter(config)#line vty 0 1  
SshRouter(config-line)#transport input ssh
  - b. SshRouter(config)#line vty 0 4  
SshRouter(config-line)#transport ssh

**418** Chapter 14 Network Security

- c. SshRouter(config)#line con 0  
SshRouter(config-line)#transport input ssh
  - d. SshRouter(config)#line vty 0 4  
SshRouter(config-line)#transport input ssh
7. Which three protocols are supported by IPSec?
- a. ESP
  - b. 3DES
  - c. MD5
  - d. SHA
  - e. IKE
  - f. AH
8. What two modes are supported by IPSec?
- a. traversing mode
  - b. forwarding mode
  - c. tunnel mode
  - d. transport mode
9. Which command successfully sets the SSH Timeout for connections to 1 minute and 30 seconds?
- a. ip ssh-time-out 90
  - b. ip ssh time-out 1min 30sec
  - c. ip ssh-time-out 1min 30sec
  - d. ip ssh time-out 90
10. What functionality is supported by the Cisco SDM? (Choose all that apply.)
- a. RADIUS
  - b. Security Audit
  - c. PPTP
  - d. VPN configuration
11. What authentication algorithms are supported by IPSec? (Choose all that apply.)
- a. ESP
  - b. 3DES
  - c. MD5
  - d. SHA
  - e. IKE
  - f. AH

12. What encryption algorithms are supported by IPSec? (Choose all that apply.)
- a. ESP
  - b. 3DES
  - c. MD5
  - d. SHA
  - e. IKE
  - f. AH
  - g. AES
13. Which tunneling protocols provide a secure tunnel for the data to travel through? (Choose all that apply.)
- a. AH
  - b. IPSec
  - c. GRE
  - d. L2TP
  - e. PPTP
14. Which protocols provide AAA services on Cisco routers? (Choose all that apply.)
- a. SSH
  - b. RADIUS
  - c. SSL
  - d. TACACS+
  - e. ESP
15. The term “authentication” in Cisco’s AAA model refers to what service?
- a. regulation of a user’s allowable activities on a device
  - b. process to validate users
  - c. the ability to verify data as it traverses the network
  - d. the ability to verify data as it traverses the network
16. The term “authorization” in Cisco’s AAA model refers to what service?
- a. the ability to verify data as it traverses the network
  - b. the ability to track user activity
  - c. process to validate users
  - d. regulation of a user’s allowable activities on a device
17. The term “accounting” in Cisco’s AAA model refers to what service?
- a. process to validate users
  - b. regulation of a user’s allowable activities on a device

**420** Chapter 14 Network Security

- c. the ability to track user activity
  - d. the ability to verify data as it traverses the network
18. What is the key reason for using SSH connections when connecting remotely to a router?
- a. SSH provides authentication services.
  - b. SSH encrypts data that would be clear text if using telnet.
  - c. SSH creates a VPN between the two nodes.
  - d. SSH examines data packets and reports malicious behavior.
19. What are you configuring when building a Cisco VPN with IPSec?
- a. an IPSec transform set
  - b. an SSH transform set
  - c. an ESP-AH-MD5 transform set
  - d. an SSL transform set
20. After building a default VPN with the SDM, your transform set name would be ESP-3DES-SHA. What does this tell you about the protocols and algorithms used?
- a. You are using 3DES as the authentication algorithm and SHA as the encryption algorithm.
  - b. You are using ESP as the authentication algorithm and SHA as the encryption algorithm.
  - c. You are using 3DES as the authentication algorithm and SHA as the encryption protocol.
  - d. You are using 3DES as the encryption algorithm and SHA as the authentication algorithm.

---

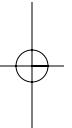
## Case Studies

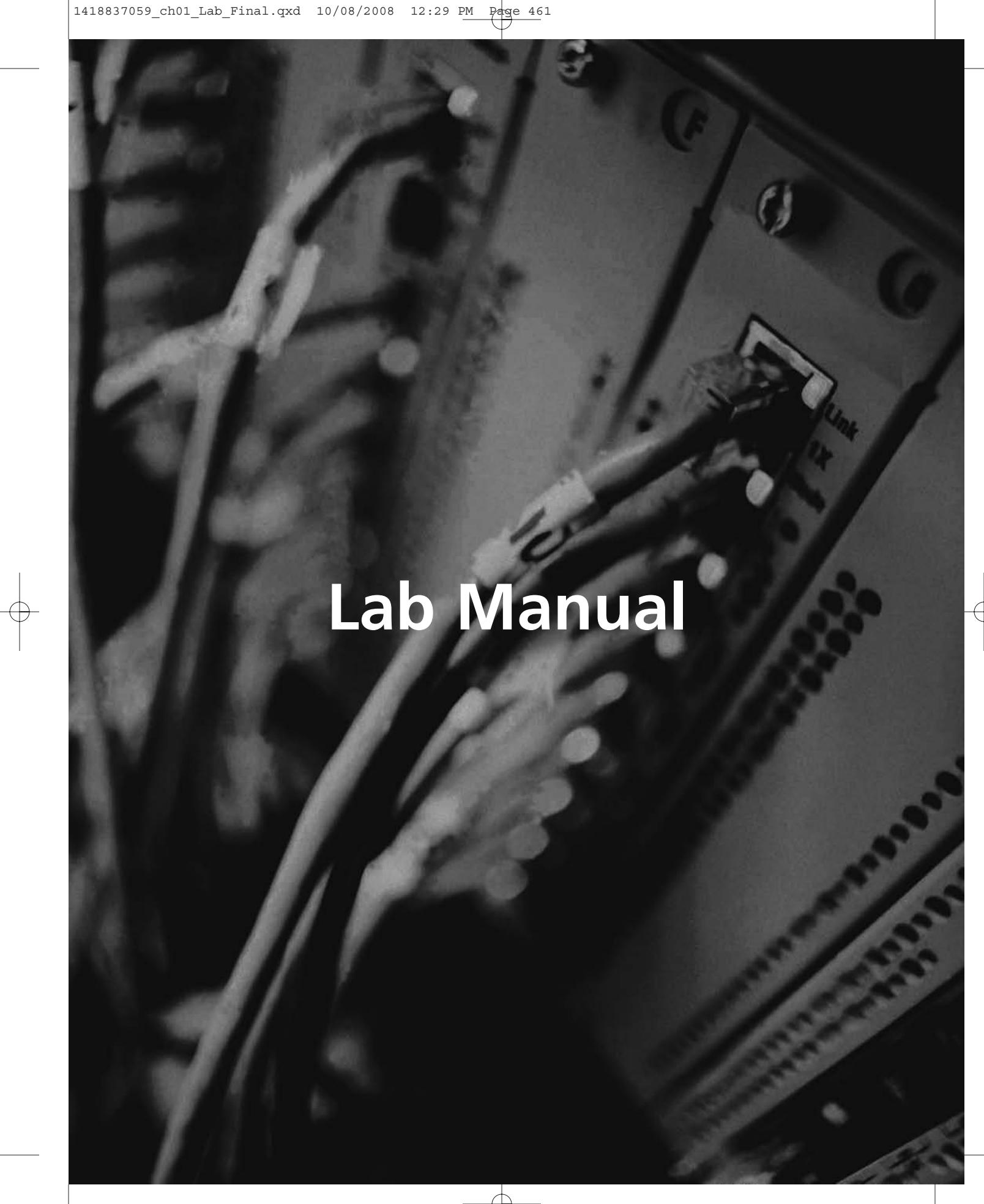


1. Your current organization has 200 employees. The company has seven offices and approximately 20 employees that work from home. As is the case with many organizations today, the company cannot afford dedicated leased lines to connect all of its locations. It is your job to devise a low-cost plan that would allow all employees to work together in the current geographic setting. What do you recommend?
2. You are considering a firewall solution for a customer. As the presales engineer, it is your responsibility to explain to customers the differences between the various firewall options. Write a few paragraphs outlining the options and then explain which option is most secure and why.

3. You must design a patch management program for your organization. The network consists of a Development Environment, a Quality Assurance (QA) Environment, and a Production Environment. You must address the following requirements for the program:

- Patches cannot be installed in two environments at once.
  - Patches must be tested for one month in each environment.
  - A back out plan must be provided in case the patches fail.
- Given these requirements, develop a plan that will carry your organization through the next 24 months.





# Lab Manual



## C H A P T E R O N E

# INTRODUCING NETWORKS

## Labs included in this chapter

- Lab 1.1 Understanding the OSI Model
- Lab 1.2 Understanding the Five Steps of Data Encapsulation
- Lab 1.3 Identifying Data Link and Network Layer Addresses
- Lab 1.4 Connection-Oriented Versus Connectionless Communications

## CCNA Exam Objectives

| Objective                                                                                           | Lab      |
|-----------------------------------------------------------------------------------------------------|----------|
| Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network | 1.1, 1.2 |
| Describe the components required for network and Internet communications                            | 1.2      |
| Describe the purpose and functions of various network devices                                       | 1.3      |
| Describe the purpose and basic operation of the protocols in the OSI and TCP models                 | 1.4      |

## Lab 1.1 Understanding the OSI Model

### Objectives

The OSI seven-layer model has been widely adopted within the networking world. This adoption has facilitated the teaching of networking principles and the development of networking software and hardware. The OSI seven-layer model is an open standard that has been accepted worldwide. The goal of this lab is to make sure you understand what happens at each of the seven layers so that you are successful as a network troubleshooter and as a CCNA candidate.

After completing this lab, you will be able to:

- Identify the OSI model layer associated with various network functions
- Describe the reasons for using the layered model

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: **20 minutes**

1. Relate the following networking descriptions to their correct OSI layer by placing them in the correct cell in the Description column of Table 1-1. There may be more than one term or phrase for each layer.

- |                                |                            |                       |
|--------------------------------|----------------------------|-----------------------|
| • Bits                         | • LLC                      | • Datagram            |
| • Where communications begin   | • Frames                   | • Cable               |
| • End-to-end transmission      | • Encoding                 | • Best path selection |
| • CSMA/CD                      | • NIC software functions   | • MAC address         |
| • Compression                  | • Synchronization          | • Formatting          |
| • Logical address              | • Voltage                  | • ACK                 |
| • Signals                      | • Services to applications | • Hubs                |
| • Request for network services | • Internetwork travel      | • ASCII               |
| • Duplex                       | • SQL                      | • Encryption          |
| • CRC                          | • Data segmentation        | • MTU                 |
|                                | • Connectionless service   |                       |

| OSI Layer    | Description |
|--------------|-------------|
| Application  |             |
| Presentation |             |
| Session      |             |
| Transport    |             |
| Network      |             |
| Data Link    |             |
| Physical     |             |

**Table 1-1** OSI model layer functions

## Certification Objectives

Objectives for the CCNA exam:

- Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network

## Review Questions

1. How does using the OSI model facilitate teaching and learning about networking?
2. How does using the OSI model facilitate the development of networking hardware and software?
3. How does using the OSI model provide compatibility and standardization between networking products?
4. How does the user fit into the OSI model?

5. What is the importance of the Network layer?
6. At which layer do the ultimate sender and receiver of data make contact?
7. If you are browsing the Web and the networking cable gets pulled out of the computer, the connection to the Web site can often be restored if you plug the cable back in. Which layer is responsible for maintaining the connection?
8. What are the two sublayers of the Data Link layer? Which one is closer to the Physical layer?
9. What is meant by “peer communication” with respect to the OSI model?
10. Is networking software more closely related to the upper layers or lower layers of the OSI model?

---

## Lab 1.2 Understanding the Five Steps of Data Encapsulation

### Objectives

During transport from the source node to the destination node, data makes its way down the protocol stack and is wrapped, or enclosed, at each layer by a header. This wrapping is called encapsulation.

Five steps of data encapsulation occur during the data’s journey from the Application layer through the Physical layer. The goal of this lab is to make sure you understand what happens at each of the five steps. Remember that this process begins with the user initiating network access. This is at the top of the OSI model.

After completing this lab, you will be able to:

- Define encapsulation in terms of networking
- Describe the five steps of data encapsulation

### Materials Required

This lab requires the following:

- A pen or pencil

## Activity

Estimated completion time: **20 minutes**

- The following bulleted list contains data encapsulation descriptions. Match these descriptions to their correct step numbers by placing them in the correct cell in the Description column of Table 1-2. There may be more than one term or phrase for each step.
 

|                                                                                                                                                                                                                                              |                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Conversion to standard data format</li> <li>• Encoding</li> <li>• Frame</li> <li>• Datagram</li> <li>• Maximum transmission units</li> <li>• Logical address</li> <li>• Bit transmission</li> </ul> | <ul style="list-style-type: none"> <li>• Upper layers</li> <li>• IP header</li> <li>• Trailer</li> <li>• Segments</li> <li>• Packet creation</li> <li>• Pulses</li> <li>• Physical address</li> </ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- For each step number in Table 1-2, give the associated OSI model layer(s).

| Step Number | Description | Associated OSI Model Layer(s) |
|-------------|-------------|-------------------------------|
| 1           |             |                               |
| 2           |             |                               |
| 3           |             |                               |
| 4           |             |                               |
| 5           |             |                               |

**Table 1-2** Data encapsulation

## Certification Objectives

Objectives for the CCNA exam:

- Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- Describe the components required for network and Internet communications

## Review Questions

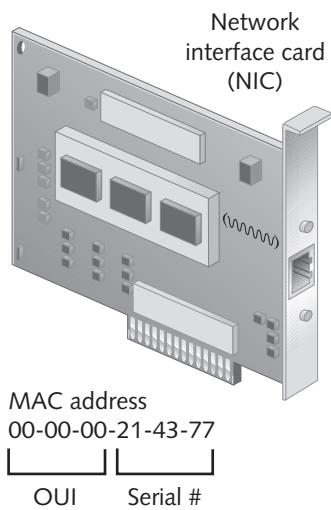
1. Which layers of the OSI model are involved in data encapsulation?
2. Which layers generally constitute the upper layers of the OSI model?
3. Encapsulation is often called “wrapping.” Why?
4. During the encapsulation process, do upper layers provide services for the layers below them or do lower layers provide services for layers above them?
5. What is the most common logical address used in networking today?
6. What is another name for the physical address?
7. What is a maximum transmission unit?
8. What is the process of encoding?
9. What is a PDU?
10. How does the Network layer facilitate data encapsulation?

---

## Lab 1.3 Identifying Data Link and Network Layer Addresses

### Objectives

Networks use two different kinds of addresses: physical addresses at the Data Link layer and logical addresses at the Network layer. Typically, the physical address is a MAC address and the logical address is an IP address. The goal of this lab is finding and identifying these different addresses on a Windows computer and defining the purpose of a MAC address. The MAC address is also known as the physical address or burned-in address (BIA), because it is burned onto the NIC during the manufacturing process. A NIC and a MAC address are shown in Figure 1-1.



**Figure 1-1** MAC address and NIC

After completing this lab, you will be able to:

- Describe Data Link and Network addresses and identify key differences between them
- Define and describe the function of the MAC address

## Materials Required

This lab requires the following:

- A computer running Microsoft Windows 2000, Windows 2003, Windows XP, or Windows Vista with Internet access

## Activity

Estimated completion time: **20 minutes**

1. Turn on the computer.
2. Click the **Start** button, click **Run**, type **cmd**, and then press **Enter**. *Note:* If you are using Windows Vista, you will not need to click Run; just type the **cmd** command and press Enter.
3. Type the command **ipconfig/all** at the prompt, press **Enter**, and then answer the following questions:
  - a. What brand of NIC (Ethernet adapter) is in the computer?
  - b. What is the MAC (physical) address of the NIC (Ethernet adapter)?
  - c. What constitutes the OUI portion of the MAC address?

**470** Chapter 1 Introducing Networks

d. What constitutes the serial number portion of the MAC address?

---

e. What is the IP address?

---

f. What is the subnet mask?

---

g. What is the default gateway?

---

4. Close the **cmd** window.

5. Open a Web browser, type [standards.ieee.org/regauth/oui](http://standards.ieee.org/regauth/oui) in the Address box, and then press **Enter**.

6. In the OUI listing Search for: text box, type **Cisco**, and then press **Enter**.

7. What is one of the six-digit OUI codes for Cisco?

---

8. Repeat Step 6 and search for **3COM**.

9. What is one of the six-digit OUI codes for 3COM?

---

10. Close the browser window.

## Certification Objectives

Objectives for the CCNA exam:

- Describe the purpose and functions of various network devices

## Review Questions

1. Which layer of the OSI model is associated with the physical address?

2. Who assigns the first six digits of the MAC address?

3. Who assigns the second six digits of the MAC address?

4. What alphanumeric characters are acceptable in a MAC address?

5. What does an IP address look like?

6. Who assigns a logical address?
7. Which layer of the OSI model is associated with the logical address?
8. Which address is displayed as hexadecimal numbers?
9. Which address allows transport between networks?
10. Which address does every host on a LAN segment evaluate?



---

## Lab 1.4 Connection-Oriented vs. Connectionless Communications

### Objectives

Protocols that reside at the Transport layer of the OSI model can be connection-oriented or connectionless. The type of transport is usually determined by the application being used. Some applications, such as e-mail, require connection-oriented transfer. While others, such as Internet gaming, are best used with connectionless transfer.

The objective of this lab is to make sure you understand the characteristics of connection-oriented and connectionless communications.

After completing this lab, you will be able to:

- Understand the differences between connection-oriented and connectionless communications

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: **20 minutes**

1. The first column of Table 1-3 contains terms relating to either connection-oriented or connectionless communications. Match these terms to their correct Transport method by adding either “connection-oriented” or “connectionless” in the second column of each row.

### Certification Objectives

Objectives for the CCNA exam:

- Describe the purpose and basic operation of the protocols in the OSI and TCP models

| Description                           | Transport Method |
|---------------------------------------|------------------|
| ACK                                   |                  |
| Unreliable                            |                  |
| Regular mail is an example            |                  |
| Reliable                              |                  |
| Datagram                              |                  |
| Return receipt for mail is an example |                  |
| Sessions                              |                  |
| TCP                                   |                  |
| UDP                                   |                  |

**Table 1-3** Connection-oriented versus connectionless communications

## Review Questions

1. Where do connection-oriented and connectionless communications fit into the OSI model?
2. What typically decides whether connection-oriented or connectionless communications are used during a data transfer?
3. Which type of communications (connection-oriented or connectionless) do you think is faster and why?
4. What is the benefit of using connection-oriented communications?

## C H A P T E R T W O

# NETWORK DEVICES

## Labs included in this chapter

- Lab 2.1 Simulating a Network by Connecting a CSU/DSU, Router, Switch, Bridge, Three Hubs, and Nine Computers
- Lab 2.2 Understanding Various Device Functions
- Lab 2.3 Understanding the Difference Between Bridges and Switches
- Lab 2.4 Understanding Wireless Parameters and Terminology

## CCNA Exam Objectives

| Objective                                                                                                          | Lab                |
|--------------------------------------------------------------------------------------------------------------------|--------------------|
| Describe the purpose and functions of various network devices                                                      | 2.1, 2.2, 2.3, 2.4 |
| Interpret network diagrams                                                                                         | 2.1, 2.3           |
| Differentiate between LAN/WAN operation and features                                                               | 2.1, 2.2           |
| Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts | 2.1                |
| Explain network segmentation and basic traffic management concepts                                                 | 2.2                |
| Explain basic switching concepts and the operation of Cisco switches                                               | 2.2, 2.3           |
| Describe standards associated with wireless media (including IEEE, Wi-Fi Alliance, ITU/FCC)                        | 2.4                |
| Identify and describe the purpose of the components in a small wireless network (including SSID, BSS, ESS)         | 2.4                |
| Compare and contrast wireless security features and capabilities of WPA security (including open, WEP, WPA 1/2)    | 2.4                |

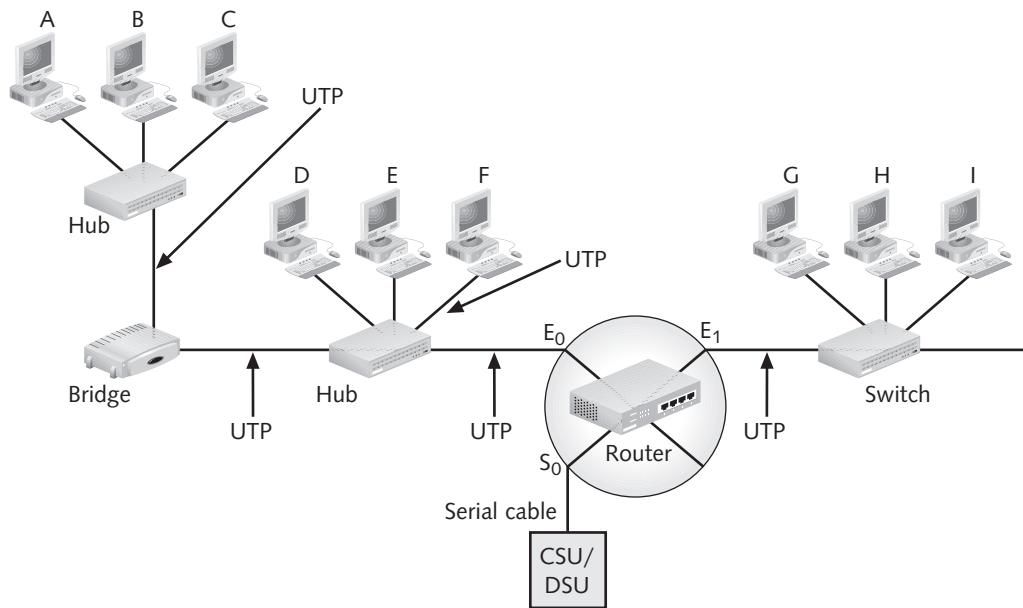
## Lab 2.1 Simulating a Network by Connecting a CSU/DSU, Router, Switch, Bridge, Three Hubs, and Nine Computers

### Objectives

As networks grow and become more complex, various devices such as hubs, bridges, switches, and routers may need to be added. It is important to know how devices interconnect and operate on a LAN and WAN. It is also important to understand how these devices affect network traffic.

The objective of this lab is to provide you with the opportunity to connect a network using various WAN and LAN hardware. Although this is just a simulation, it provides insight into the hardware connections required in a LAN/WAN relationship and how various devices affect network operations.

Figure 2-1 shows the configuration you will attempt to duplicate. In this lab, you will connect a CSU/DSU to a router with a standard serial cable. On one side of the router there will be two hubs separated by a bridge. A switch is located on the other side of the router. (You will simulate the nine workstations in Figure 2-1 with old NICs.)



**Figure 2-1** Network simulation setup

After completing this lab, you will be able to:

- Identify various WAN and LAN devices
- Connect the WAN and LAN devices, as shown in Figure 2-1
- Understand how various devices affect network communications

## Materials Required

This lab requires the following:

- One CSU/DSU (may substitute a router if necessary)
- One Cisco router with two Ethernet ports and at least one serial port
- Transceivers for the router Ethernet ports, if these Ethernet ports use an AUI connection instead of RJ-45
- Transceivers for the bridge connections, if the bridge uses AUI connections instead of RJ-45
- Two hubs
- One switch
- One bridge
- Nine NICs with RJ-45 transceivers for simulating the nine host computers in Figure 2-1
- Thirteen UTP patch cables
- One serial cable with a compatible connector for the serial interface on a router on one end and a v.35 connector on the other end to attach to the CSU/DSU. If another router is used instead of the CSU/DSU, the cable connector should match the serial interface on the additional router.

**2**

## Activity

Estimated completion time: **20 minutes**

1. Lay out the devices on a table, as shown in Figure 2-1.
2. Connect the CSU/DSU to a serial interface on the router using the serial cable.
3. Connect an Ethernet port on the router to a hub using UTP cable.
4. Connect the other Ethernet port on the router to the switch using UTP cable.
5. Connect the hub on the left to the bridge using UTP cable. There may be a toggle on the bridge that needs to be configured, depending on the type of cable you have connected to it. Make sure the switch is in the correct position.
6. Connect the bridge to the next hub using UTP cable.
7. Connect three patch cables to a hub using UTP patch cables. Make sure none of the patch cables are connected to the uplink port of the hub. The uplink port is used for hub-to-hub connections when using a straight-through patch cable instead of a crossover cable. You cannot use this port for workstations. The uplink port is usually marked. Sometimes a switch is available that can be positioned to configure a regular port as an uplink port.
8. Connect the other end of the patch cables used in Step 7 to the NICs to simulate connecting workstations.
9. Repeat Steps 7 and 8 for the other hub and the switch and NICs to complete your simulated network as shown in Figure 2-1.

## Certification Objectives

Objectives for the CCNA exam:

- Describe the purpose and functions of various network devices
- Interpret network diagrams
- Differentiate between LAN/WAN operation and features
- Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts

## Review Questions

1. Which of the devices that you used in this lab are considered LAN equipment?
2. Which of the devices that you used in this lab are considered WAN equipment?
3. In Figure 2-1, are computers A, B, and C on the same network as D, E, and F?
4. In Figure 2-1, are computers A, B, and C on the same network as G, H, and I?
5. How does the bridge operate to filter traffic between the two attached segments in your network?
6. In Figure 2-1, how does the router operate to filter traffic between the segments off of  $E_0$ ,  $E_1$ , and  $S_0$ ?
7. What kind of domains do bridges and switches create?
8. What kind of domains do routers create?
9. If the LANs in Figure 2-1 are 100 Mbps systems, which computers are sharing this bandwidth?
10. What kind of traffic is a bridge or a switch unable to filter?

## Lab 2.2 Understanding Various Device Functions

### Objectives

It is important to understand how all devices operate on a network. These devices include repeaters, hubs, bridges, switches, brouters, routers, and gateways. The purpose of this lab is to make sure you understand the characteristics of all network devices.

After completing this lab, you will be able to:

- Identify characteristics of repeaters, hubs, bridges, switches, brouters, routers, and gateways

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: **20 minutes**

- Fill in the Device(s) column of Table 2-1 with the device being described. You can fill in the table with **repeater**, **hub**, **bridge**, **switch**, **brouter**, **router**, or **gateway**. Note that more than one device might match a specific characteristic.

| Characteristic                                                                         | Device(s) |
|----------------------------------------------------------------------------------------|-----------|
| Operates at upper layers to translate between different protocol suites                |           |
| Filters traffic based on MAC address                                                   |           |
| Introduces the most latency on a network                                               |           |
| Boosts the signal but does not segment the network                                     |           |
| Operates differently depending on whether nonroutable or routable protocols are in use |           |
| Creates broadcast domains                                                              |           |
| Creates a virtual circuit between sender and receiver                                  |           |
| Forwards broadcast traffic                                                             |           |
| Filters traffic based on logical address                                               |           |
| Associated with the term "microsegmentation"                                           |           |
| Creates subnetworks                                                                    |           |
| Connects computers in a physical star and uses "shared bandwidth"                      |           |
| Creates collision domains                                                              |           |
| Operates at layer 1 of the OSI model                                                   |           |
| Operates at layer 2 of the OSI model                                                   |           |
| Operates at layer 3 of the OSI model                                                   |           |

**Table 2-1** Network device characteristics

## Certification Objectives

Objectives for the CCNA exam:

- Describe the purpose and functions of various network devices
- Differentiate between LAN/WAN operation and features
- Explain network segmentation and basic traffic management concepts
- Explain basic switching concepts and the operation of Cisco switches

## Review Questions

1. When is it appropriate to introduce a router into your network?
2. What can bridges do that hubs and repeaters cannot do?
3. When would introducing a brouter on your network be appropriate?
4. What are the advantages and disadvantages of using a gateway on your network?
5. What is the benefit of replacing hubs on your network with switches?

---

## Lab 2.3 Understanding the Difference Between Bridges and Switches

### Objectives

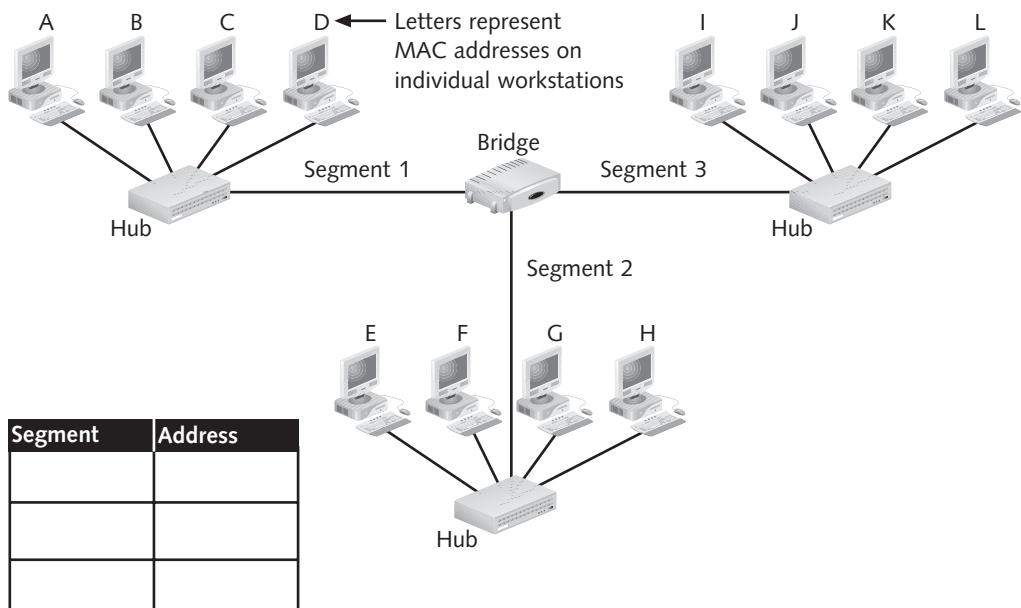
Bridges and switches operate at the Data Link layer of the OSI model and filter traffic using the MAC address; however, the two components operate somewhat differently. The goal of this lab is for you to understand exactly how bridges and switches operate on a network. You will use Figures 2-2 and 2-3 to learn about properties of bridges and switches.

After completing this lab, you will be able to:

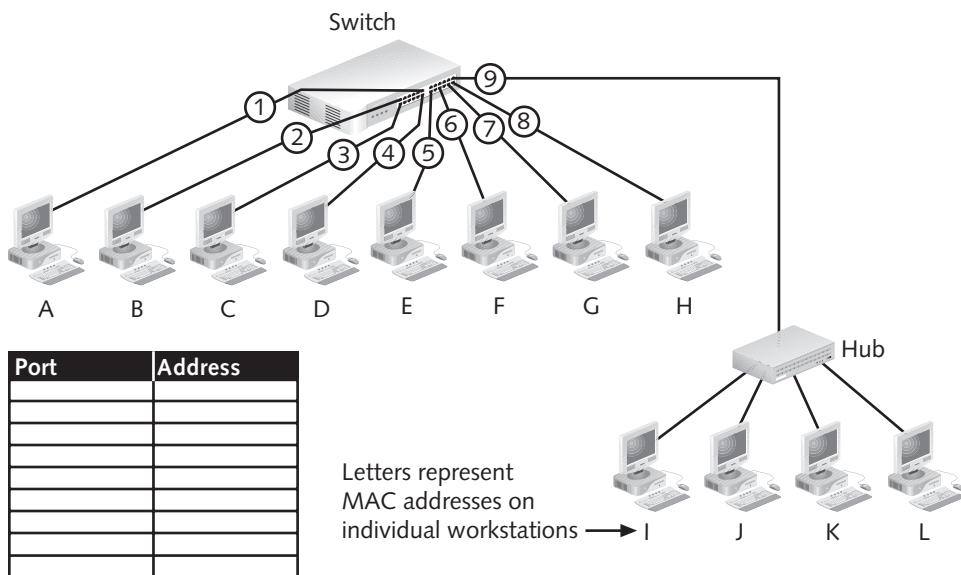
- Describe the tables that bridges and switches use to filter traffic
- Explain why switches are the device of choice for enhancing network performance

## Lab 2.3 Understanding the Difference Between Bridges and Switches

479



2

**Figure 2-2** Bridge with bridging table**Figure 2-3** Switch with switching table

## Materials Required

This lab requires the following:

- A pen or pencil

## Activity

Estimated completion time: **20 minutes**

1. Review Figure 2-2. In particular, note how the workstations, represented by letters, connect to the bridge.
2. Complete the bridging table shown in Figure 2-2 by filling in the columns in the table. Note that the letters in the figure represent MAC addresses on workstations.
3. Review Figure 2-3. In particular, note how the workstations, represented by letters, connect to the switch.
4. Complete the switching table shown in Figure 2-3 by filling in the columns in the table. The letters in the figure represent MAC addresses on workstations.

## Certification Objectives

Objectives for the CCNA exam:

- Describe the purpose and functions of various network devices
- Interpret network diagrams
- Explain basic switching concepts and the operation of Cisco switches

## Review Questions

1. How many collision domains are defined in Figure 2-2?
2. How many collision domains are defined in Figure 2-3?
3. Examine Figure 2-2. If a frame from computer A has a destination MAC address for computer D, which devices will see the layer 2 information?
4. Examine Figure 2-3. If a frame from computer A has a destination MAC address for computer D, which devices will see the layer 2 information?
5. Examine Figure 2-3. In terms of network performance, what is the difference between computers A through H and I through L?

6. What will a bridge and switch do with a frame for which it has no information about the destination in its table?

7. How do bridges and switches handle broadcast frames?

**2**

8. Why is a switch considered more effective than a bridge in terms of increasing network performance?

9. In general, how do bridges and switches dynamically create their tables?

10. What happens to tables when bridges and switches are turned off?

---

## Lab 2.4 Understanding Wireless Parameters and Terminology

### Objectives

Wireless is the fastest growing area of networking. You need to understand how wireless devices operate, the associated standards and organizations, wireless security measures, and wireless troubleshooting tips. In this lab, you will match the correct wireless term with a definition.

After completing this lab, you will be able to:

- Describe how wireless works
- Explain the various 802.11 standards and the associated organizations
- Understand wireless security and troubleshooting methods

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: **20 minutes**

Match each term in the following bulleted list with a definition in the numbered list. Each bulleted term is used only once. Use the Internet and Web sites such as [www.whatismyip.com](http://www.whatismyip.com) and [www.webopedia.com](http://www.webopedia.com) if you need to search for a definition.

- Wi-Fi Alliance
- IEEE

**482** Chapter 2 Network Devices

- 802.11a
  - 802.11b
  - 802.11g
  - 802.11n
  - 802.11i
  - 802.1x
  - Ad hoc mode
  - Infrastructure mode
  - CSMA/CA
  - BSS
  - ESS
  - SSID
  - WEP
  - WPA
1. Organization that developed the 802.11 specifications \_\_\_\_\_
  2. Wireless security standard that replaced WEP and uses the TKIP algorithm \_\_\_\_\_
  3. The latest and fastest 802.11 standard \_\_\_\_\_
  4. This mode specifies that the client device associates with an access point \_\_\_\_\_
  5. The wireless network name that is often broadcast so that clients can associate using it \_\_\_\_\_
  6. The IEEE port-blocking specification \_\_\_\_\_
  7. The network access method used by 802.11 devices \_\_\_\_\_
  8. The IEEE security standard based on WPA2 \_\_\_\_\_
  9. The IEEE standard that specifies 54 Mbps in the 5 GHz range \_\_\_\_\_
  10. This mode specifies that the client device communicate directly with other client devices and that no access point is used \_\_\_\_\_
  11. A single access point in infrastructure mode \_\_\_\_\_
  12. The original security standard for 802.11 \_\_\_\_\_
  13. The IEEE standard that specifies 11 Mbps in the 2.4 GHz range \_\_\_\_\_
  14. Multiple access points connected in infrastructure mode \_\_\_\_\_
  15. The IEEE standard that specifies 54 Mbps in the 2.4 GHz range \_\_\_\_\_
  16. Organization developed to promote 802.11 usage \_\_\_\_\_

## Certification Objectives

Objectives for the CCNA exam:

- Describe the purpose and functions of various network devices
- Describe standards associated with wireless media (including IEEE, Wi-Fi Alliance, ITU/FCC)
- Identify and describe the purpose of the components in a small wireless network (including SSID, BSS, ESS)
- Compare and contrast wireless security features and capabilities of WPA security (including open, WEP, WPA 1/2)

**2**

## Review Questions

1. What is the greatest advantage of using wireless?
2. What is the greatest disadvantage of using wireless?
3. In terms of bandwidth, is an access point more like a switch or a hub? Explain.
4. Which is more efficient and why? CSMA/CD or CSMA/CA?
5. How does a wireless client know which access point to associate with?



## C H A P T E R      T H R E E

# TCP/IP

## Labs included in this chapter

- Lab 3.1 Determine IP and MAC Header Information in an ARP Request and ARP Reply
- Lab 3.2 Determine IP and MAC Header Information in a RARP Request
- Lab 3.3 Determine IP and MAC Header Information for a Data Packet

## CCNA Exam Objectives

| Objective                                                                              | Lab           |
|----------------------------------------------------------------------------------------|---------------|
| Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models | 3.1, 3.2, 3.3 |
| Describe the components required for network and Internet communications               | 3.1, 3.2, 3.3 |

## Lab 3.1 Determine IP and MAC Header Information in an ARP Request and ARP Reply

### Objectives

The objective of this lab is to help you understand the information contained in the IP and MAC header of an ARP request and ARP reply. In this lab, you will determine the IP and MAC information for an ARP request being issued by Computer A to determine the MAC address of Computer C, as illustrated in Figure 3-1.

#### Computer A



I want to send a message to Computer C, but I don't know C's MAC address.  
C's IP address is 193.19.20.36.

My MAC: 05:61:8c:01:05:12  
My IP: 193.19.20.45

**Figure 3-1** Computer A

After completing this lab, you will be able to:

- Determine the IP and MAC header for an ARP request, given the known addresses indicated in Figure 3-1
- Determine the IP and MAC header for an ARP reply, given the known addresses indicated in Figures 3-1 and 3-3

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: **10 minutes**

1. Record the destination and source IP addresses in the IP header in Figure 3-2.
2. Record the destination and source MAC addresses in the MAC header in Figure 3-2.

| MAC header |        | IP header |        | ARP request               |
|------------|--------|-----------|--------|---------------------------|
| Dest       | Source | Dest      | Source | What is your MAC address? |
|            |        |           |        |                           |

**Figure 3-2** ARP request frame

3. Examine Figure 3-3, then record the destination and source IP addresses in the IP header in Figure 3-4.

**Computer C**

I'm the one you're looking for.  
My MAC address is  
09:01:02:98:91:80.

**3****Figure 3-3 Computer C**

4. Record the destination and source MAC addresses in the MAC header in Figure 3-4.

| MAC header |        | IP header |        | ARP reply               |
|------------|--------|-----------|--------|-------------------------|
| Dest       | Source | Dest      | Source | Here is my MAC address. |
|            |        |           |        |                         |

**Figure 3-4 ARP reply frame**

## Certification Objectives

Objectives for the CCNA exam:

- Describe the components required for network and Internet communications
- Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models

## Review Questions

1. Explain your destination MAC address entry in Figure 3-2.
2. What will all hosts that see an ARP request do with the information?
3. How does a sending computer know the IP address of a destination computer?

4. What type of frame is the ARP reply—unicast or broadcast?
5. Because ARP uses bandwidth by broadcasting, exactly how does ARP save bandwidth overall?

---

## Lab 3.2 Determine IP and MAC Header Information in an RARP Request

### Objectives

The objective of this lab is to help you understand the information contained in the IP and MAC header of a Reverse ARP (RARP) request. In this lab, you will determine the IP and MAC information for the RARP request issued by Computer D, as shown in Figure 3-5.

**Computer D**



I know my MAC address is  
01:09:42:71:93:64, but I  
don't know my IP address.

**Figure 3-5 Computer D**

After completing this lab, you will be able to:

- Determine the IP and MAC header for an RARP request, given the known MAC address indicated in Figure 3-5

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: **10 minutes**

1. Examine Figure 3-5. Then, record the destination and source IP addresses in Figure 3-6 using the information in Figure 3-5.
2. Record the destination and source MAC addresses in Figure 3-6.

| MAC header |        | IP header |        | RARP request           |
|------------|--------|-----------|--------|------------------------|
| Dest       | Source | Dest      | Source | What is my IP address? |
|            |        |           |        |                        |

**Figure 3-6** RARP request frame

3

## Certification Objectives

Objectives for the CCNA exam:

- Describe the components required for network and Internet communications
- Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models

## Review Questions

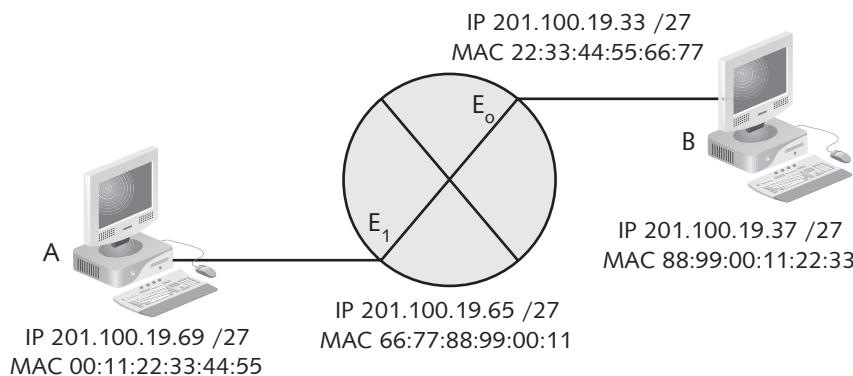
1. What kind of address is the destination MAC address in an RARP request?
2. How does a computer know its own MAC address?
3. Based on your lab activity, explain your entry for the source IP address in the RARP request.
4. What kind of address is the destination IP address in an RARP request?
5. How does the RARP server know which IP address to assign to an RARP client?

---

## Lab 3.3 Determine IP and MAC Header Information for a Data Packet

### Objectives

The objective of this lab is to help you understand the information contained in the IP and MAC header of a data packet as it travels from the source to the destination host through a router. In this lab, you will determine the IP and MAC information between Computer A and router interface E<sub>1</sub> and again between router interface E<sub>0</sub> and Computer B, as shown in Figure 3-7.

**Figure 3-7** MAC and IP header information

After completing this lab, you will be able to:

- Determine the IP and MAC header for a data packet as it travels through a router, given the known MAC and IP information indicated in Figure 3-7
- Understand the concept of a default gateway

## Materials Required

This lab requires the following:

- A pen or pencil

## Activity

Estimated completion time: **10 minutes**

1. Record the destination and source IP addresses in Figure 3-8 for a frame transmitted from Computer A to interface E<sub>1</sub> on the router that is destined for Computer B.
2. Record the destination and source MAC address in Figure 3-8 for a frame transmitted from Computer A to interface E<sub>1</sub> on the router that is destined for Computer B.

| MAC header |        | IP header |        | Data |
|------------|--------|-----------|--------|------|
| Dest       | Source | Dest      | Source |      |
|            |        |           |        |      |

**Figure 3-8** Frame from Computer A to router interface E<sub>1</sub>

3. Record the destination and source IP addresses in Figure 3-9 for a frame transmitted from the  $E_0$  interface on the router to Computer B during its journey from Computer A to Computer B.
4. Record the destination and source MAC address in Figure 3-9 for a frame transmitted from  $E_0$  on the router to Computer B during its journey from Computer A to Computer B.

3

| MAC header |        | IP header |        | Data |
|------------|--------|-----------|--------|------|
| Dest       | Source | Dest      | Source |      |
|            |        |           |        |      |

**Figure 3-9** Frame from router interface  $E_0$  to Computer B

## Certification Objectives

Objectives for the CCNA exam:

- Describe the components required for network and Internet communications
- Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models

## Review Questions

1. In Figure 3-7, what is the default gateway for Computer A?
2. In Figure 3-7, what is the default gateway for Computer B?
3. What can you say about the source and destination IP addresses in a frame as the data travels across routers in its journey from original sender to ultimate receiver?
4. What can you say about the source and destination MAC addresses in a frame as the data travels across routers in its journey from original sender to ultimate receiver?
5. Where do routers get the information necessary to make forwarding decisions?
6. Why do computers usually need a default gateway, and when is it used?



## C H A P T E R F O U R

# IP ADDRESSING

## Labs included in this chapter

- Lab 4.1 Determine an IP Addressing Scheme for Network 192.3.2.0
- Lab 4.2 Decode the IP Address 172.16.31.255 /20
- Lab 4.3 Decode the IP Address 120.15.179.255 /18
- Lab 4.4 Design an Efficient IP Addressing Scheme for Network 176.10.0.0
- Lab 4.5 Perform Binary/Decimal/Hexadecimal Conversions

## CCNA Exam Objectives

| Objective                                                                                  | Lab                |
|--------------------------------------------------------------------------------------------|--------------------|
| Implement static and dynamic addressing services for hosts in a LAN environment            | 4.1, 4.4           |
| Identify and correct common problems associated with IP addressing and host configurations | 4.1, 4.2, 4.3, 4.4 |

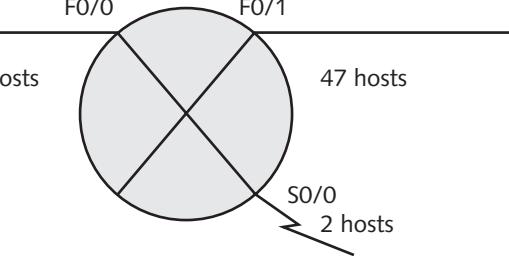
## Lab 4.1 Determine an IP Addressing Scheme for Network 192.3.2.0

### Objectives

The objective of this lab is to demonstrate a logical way of determining an IP addressing scheme for the network shown in Figure 4-1. In this lab, you determine the subnet mask, the multiplier, subnetwork addresses, and the broadcast, interface, and host addresses. You will add labels to Figure 4-1 as you determine specific information.



The “F0/0” and “F0/1” in Figure 4-1 represent Fast Ethernet links. The “S0/0” in Figure 4-1 represents a serial link.



**Figure 4-1** Example network with 2 Fast Ethernet interfaces and 1 serial interface

After completing this lab, you will be able to:

- Determine the minimum number of bits to borrow when subnetting a given network
- Determine and assign IP addresses to the router interfaces and the hosts
- Understand which IP addresses are reserved and why

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: 20 minutes

1. Review Figure 4-1. In particular, note the number of networks, the number of hosts, and the structure of the network number.
2. Determine the class of the network by examining the first octet of the network number given.

## Lab 4.1 Determine an IP Addressing Scheme for Network 192.3.2.0

**495**

3. Notice that there are three interfaces, F0/0, F0/1, and S0/0. How many subnets do you need?

- 
4. Use the formula  $2^y = \# \text{ of subnetworks}$  to solve for  $y$ , where  $y =$  the number of bits borrowed. Borrow just enough to cover the number of subnets you determined in Step 3.

- 
5. Use the formula  $2^x - 2 = \# \text{ of usable host addresses}$  (where  $x$  is the number of bits remaining in the host portion after borrowing) to make sure you have enough bits available for the hosts shown in Figure 4-1.

4

- 
6. Write the subnet mask in dotted decimal and in binary notation.

- 
7. Determine the multiplier by looking at the decimal value of the last bit borrowed as you move from left to right. The multiplier is either 128, 64, 32, 16, 8, 4, 2, or 1.

- 
8. Use the multiplier determined in Step 7 to determine the subnetwork addresses. The subnetwork addresses will increment by the value of the multiplier. Incrementing occurs in the octet in which borrowing broke off (the octet where the multiplier was determined).

- 
9. The last address on any subnet is always a broadcast address. Find this last possible IP address for each subnet. What are the broadcast addresses?

- 
10. Use the remaining addresses (all available addresses minus the subnet addresses and the broadcast addresses) for hosts. What is the range of hosts on each subnet?

---

---

---

- 
11. Assign the first host IP address in each subnet address to a router interface. This first address is available for hosts, but is traditionally used for the router interface connected to the subnet. What addresses did you assign?

- 
12. Write the last octet of the subnet addresses in binary. How many bits are in the host portion? What does the host portion of these addresses look like?

---

---

---

- 
13. Write the last octet of the broadcast addresses in binary. What does the host portion of these addresses look like?

---

## Certification Objectives

Objectives for the CCNA exam:

- Implement static and dynamic addressing services for hosts in a LAN environment
- Identify and correct common problems associated with IP addressing and host configurations

## Review Questions

1. When working with IP addresses and subnetting, why is it important to first identify the class of address and the default subnet mask for that class?
2. What values can a multiplier be?
3. How do you find the multiplier?
4. Why must you subtract 2 from  $2^x$  when determining the number of hosts per subnet?
5. How do you know where to begin incrementing when determining subnet numbers?
6. When working with IP addresses, which addresses can never be assigned to a host?
7. How can you tell if an IP address is a network or subnetwork number if you write out the address in binary?
8. How can you tell if an IP address is a broadcast address if you write out the address in binary?
9. Must router interfaces be assigned the first available host address in a range?

---

## Lab 4.2 Decode the IP Address 172.16.31.255 /20

### Objectives

The objective of this lab is to help you become more familiar with subnetting and to expose you to the bit-count notation used to express the subnet mask. Instead of writing out the subnet mask in dotted decimal notation, the bit-count method simply uses a forward slash

followed by the number of consecutive ones in the mask. Bit-count notation is also known as CIDR notation. In this lab you will decode the IP address 172.16.31.255 /20 and determine the subnet mask, the multiplier, the network number, the subnetwork addresses, and broadcast addresses.

After completing this lab, you will be able to:

- Recognize the subnet mask of an IP address given in bit-count format
- Determine the network number
- Determine subnetwork numbers and broadcast addresses
- Identify whether a given IP address is a broadcast, network, or host address
- Identify on which subnetwork a given IP address is located

4

## Materials Required

This lab requires the following:

- A pen or pencil

## Activity

Estimated completion time: 20 minutes

1. Determine the class of the network address given by examining the first octet.  
\_\_\_\_\_
2. Determine the subnet mask by writing 1s for the first 20 bits of the address and 0s for the last 12 bits. How would you write this subnet mask in dotted decimal notation? How many bits have been borrowed?  
\_\_\_\_\_
3. Use the formula  $2^y$  (where  $y$  is the number of bits borrowed from the default host portion) to calculate how many subnetworks can be created.
4. Use the formula  $2^x - 2$  (where  $x$  is the number of bits remaining in the host portion) to calculate how many usable hosts per subnetwork can be created.  
\_\_\_\_\_
5. Determine the multiplier by looking at the decimal value of the last bit borrowed as you move from left to right. The multiplier is either 128, 64, 32, 16, 8, 4, 2, or 1.  
\_\_\_\_\_
6. Determine the major network number in dotted decimal notation by substituting 0s for the default host portion of the given IP address.  
\_\_\_\_\_

**498** Chapter 4 IP Addressing

7. Use the multiplier determined in Step 5 to increment up through the first six subnetwork addresses. Incrementing occurs in the octet in which borrowing broke off.

---

---

---

8. Determine the broadcast addresses on the six subnetworks listed in Step 7. The broadcast address on each subnetwork is the last possible address before the next subnet begins.

---

---

---

9. What does the address 172.16.31.255 /20 represent?

---

10. On what network is the given address in Step 9?

---

## Certification Objectives

Objectives for the CCNA exam:

- Identify and correct common problems associated with IP addressing and host configurations

## Review Questions

1. Where do you think the term “bit-count” comes from?
2. What is a benefit of using bit-count notation to express the subnet mask?
3. What would the bit-count notation of the IP address given in this lab have been if there were no subnetting?
4. If there were no subnetting in this lab, what would the given IP address have represented?

## Lab 4.3 Decode the IP Address 120.15.179.255 /18

### Objectives

The objective of this lab is to help you become familiar with subnetting and the bit-count notation used to express the subnet mask. In this lab you will decode the IP address 120.15.179.255 /18 and determine the subnet mask, multiplier, network number, subnet-network addresses, and broadcast addresses.

After completing this lab, you will be able to:

- Recognize the subnet mask of an IP address given in bit-count format
- Determine the network number
- Determine subnetwork numbers and broadcast addresses
- Identify whether a given IP address is a broadcast, network, or host address
- Identify on which subnetwork a given IP address is located

4

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: 20 minutes

1. Determine the class of the network by examining the first octet of the network address given. What is the default mask?
2. Determine the subnet mask by writing 1s for the first 18 bits of the address and 0s for the last 14 bits. How would you write this subnet mask in dotted decimal notation?
3. Use the formula  $2^y$  (where  $y$  is the number of bits borrowed from the default host portion) to calculate how many subnetworks can be created.
4. Use the formula  $2^x - 2$  (where  $x$  is the number of bits remaining in the host portion) to calculate how many usable hosts per subnetwork can be created.
5. Determine the multiplier by looking at the decimal value of the last bit borrowed as you move from left to right. The multiplier is either 128, 64, 32, 16, 8, 4, 2, or 1.
6. Determine the major network number in dotted decimal notation by substituting 0s for the default host portion of the given IP address.

**500** Chapter 4 IP Addressing

7. Use the multiplier determined in Step 5 to determine the first seven subnetwork addresses. The incrementing occurs in the octet in which borrowing broke off.

---

8. Determine the broadcast addresses on the subnetworks listed in Step 7. The broadcast address on each subnetwork is the last possible address before the next subnet begins.

---

9. What does the address 120.15.179.255 /18 represent?

---

10. On what network is the IP address given in Step 9?

---

## Certification Objectives

Objectives for the CCNA exam:

- Identify and correct common problems associated with IP addressing and host configurations

## Review Questions

1. What makes subnetting with Class A and Class B addresses more difficult than subnetting with Class C addresses?
  
2. What is the maximum number of bits that can be borrowed with a Class C address?
  
3. What is the maximum number of bits that can be borrowed with a Class B address?
  
4. What is the maximum number of bits that can be borrowed with a Class A address?
  
5. What would the subnet mask be in dotted decimal notation for a Class C address if there were 30 hosts per subnet?

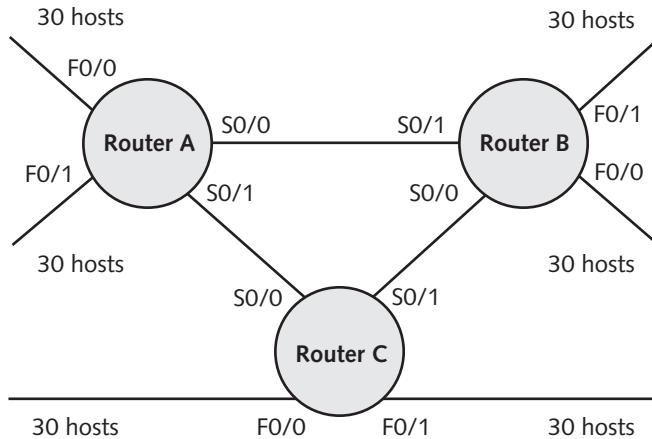
---

## Lab 4.4 Design an Efficient IP Addressing Scheme for Network 176.10.0.0

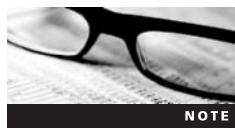
### Objectives

The objective of this lab is to give you a chance to use the subnetting formulas demonstrated in Labs 4.1 through 4.3 and to do so with less guidance. Use what you have learned to logically determine an efficient IP addressing scheme for network 176.10.0.0, shown in Figure 4-2, which allows 100% growth in the subnets.

## Lab 4.4 Design an Efficient IP Addressing Scheme for Network 176.10.0.0

**501****Figure 4-2** Network 176.10.0.0**4**

In this lab you will determine the subnet mask, multiplier, subnetwork addresses, and the broadcast, interface, and host addresses. You will add labels to Figure 4-2 as you determine specific information.



The “S0/0” and “S0/1” in Figure 4-2 represent serial links. Even though there are no hosts on these connections, they must be considered a subnet and the serial interfaces must be given IP addresses.

**NOTE**

After completing this lab, you will be able to:

- Determine the minimum number of bits to borrow when subnetting a given network and allowing for 100% growth
- Determine and assign IP addresses to the router interfaces and the hosts
- Determine the subnet addresses and broadcast addresses on each subnet

## Materials Required

This lab requires the following:

- A pen or pencil

## Activity

**Estimated completion time: 30 minutes**

1. Determine the class of the network by examining the first octet of the network address given.

---

2. Determine the number of subnets needed in Figure 4-2, and increase this number by 100% to allow for growth. For how many subnets do you allow?

---

**502** Chapter 4 IP Addressing

3. Determine how many bits must be borrowed in order to accommodate the number calculated in Step 2. How many subnets are available?

---

4. Determine if borrowing the number of bits calculated in Step 3 leaves enough bits to accommodate the number of hosts per subnet, as indicated in Figure 4-2. How many usable hosts per subnetwork are available?

---

5. Determine the new subnet mask in dotted decimal and in binary notation.

---

6. Determine the subnet numbers of the nine existing subnets.

---

---

---

---

---

7. Determine the broadcast addresses on each of the nine existing subnets.

---

---

---

---

---

8. Determine the usable range of host addresses on each of the nine existing subnets.

---

---

---

---

---

9. Assign IP addresses to the following router interfaces:

- Router A: F0/0, F0/1, S0/0, and S0/1

---

---

## Lab 4.4 Design an Efficient IP Addressing Scheme for Network 176.10.0.0

**503**

- Router B: F0/0, F0/1, S0/0, and S0/1
- 
- 

- Router C: F0/0, F0/1, S0/0, and S0/1
- 
- 

10. Prove that 176.10.24.0 is a subnet number by using binary notation.

**4**

## Certification Objectives

Objectives for the CCNA exam:

- Implement static and dynamic addressing services for hosts in a LAN environment
- Identify and correct common problems associated with IP addressing and host configurations

## Review Questions

1. Interfaces attached by point-to-point links such as the one between Router A's S0/0 and Router B's S0/1 in Figure 4-2 are on the same network (or subnetwork). True or False?
2. What kind of IP address is indicated by all binary ones in the host portion?
3. What kind of IP address is indicated by all binary zeroes in the host portion?
4. What is the purpose of a subnet mask?
5. What might you do if, when you borrowed enough bits for subnet numbers, you were not left with enough bits for host numbers?

## Lab 4.5 Perform Binary/Decimal/Hexadecimal Conversions

### Objectives

The objective of this lab is to help you understand the relationships between binary, decimal, and hexadecimal numbering systems and to teach you how to convert between them. In this lab you will convert a decimal number to binary and then to hexadecimal. Next, you will convert a hexadecimal number to binary and then to decimal.

After completing this lab, you will be able to:

- Convert from decimal to binary
- Convert from hexadecimal to binary to decimal
- Convert from binary to hexadecimal

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: 30 minutes

1. The place values for the eight binary digits used in IPv4 addressing are as follows: 128, 64, 32, 16, 8, 4, 2, 1. Expand this range to include an additional four bits. Do this by recording the place values for  $2^{11}$ ,  $2^{10}$ ,  $2^9$ , and  $2^8$ .
2. Express the decimal value 2001 in binary by placing 1s in the binary positions requiring the addition of the corresponding place value. Place 0s in the binary positions where the corresponding place value should not be added.
3. To express this binary number in hexadecimal, you must first group the digits in sets of four. If you have 11 digits, begin by adding a leading zero to your binary number so that you have 12 binary digits. The decimal equivalent should still be 2001. It should not change because of the added leading zero. Record your binary 12-digit number below.
4. Group the 12 binary digits into three sets of four binary digits.
5. Convert each group of binary digits to a hexadecimal digit using Table 4-1. The result should be a three-digit hex number.

## Lab 4.5 Perform Binary/Decimal/Hexadecimal Conversions

**505**

| Binary | Hexadecimal | Decimal |
|--------|-------------|---------|
| 0000   | 0           | 0       |
| 0001   | 1           | 1       |
| 0010   | 2           | 2       |
| 0011   | 3           | 3       |
| 0100   | 4           | 4       |
| 0101   | 5           | 5       |
| 0110   | 6           | 6       |
| 0111   | 7           | 7       |
| 1000   | 8           | 8       |
| 1001   | 9           | 9       |
| 1010   | A           | 10      |
| 1011   | B           | 11      |
| 1100   | C           | 12      |
| 1101   | D           | 13      |
| 1110   | E           | 14      |
| 1111   | F           | 15      |

**Table 4-1** Binary to hex to decimal conversion**4**

6. Check your answer by multiplying the hexadecimal digits in your answer by their corresponding place value to get the decimal equivalent. For example:  $(3\text{rd hex digit} * 16^2) + (2\text{nd hex digit} * 16^1) + (1\text{st hex digit} * 16^0)$ . Your decimal equivalent should equal 2001. Did you get the correct result? If not, double-check your decimal to binary and binary to hexadecimal conversions.
7. Next, try converting a hexadecimal number (CD4) to binary and then to decimal. First, treat each hexadecimal digit as four binary digits, using Table 4-1 as necessary. Record your answer below. You should have 12 binary digits grouped in three sets of four.

---

8. To convert the binary number recorded in Step 7, add the decimal place values of the 1's binary digits. Record your answer below.

---

9. To double-check your answer, multiply the decimal value of each hexadecimal digit in CD4 with the corresponding place value, as you did in Step 6.

## Certification Objectives

Objectives for the CCNA exam:

- This lab does not map to a certification objective; however, it contains information that is covered on the CCNA exam.

## Review Questions

1. For what purposes is the binary numbering system used in networking?
2. For what purposes is the hexadecimal numbering system used in networking?
3. Why does it require fewer hexadecimal numerals than binary numerals to express any given number?
4. Some numbers are too large to be expressed in binary. True or False?

## C H A P T E R F I V E

# ROUTER AND IOS BASICS

## Labs included in this chapter

- Lab 5.1 Connect the Internetwork Lab
- Lab 5.2 Configure HyperTerminal to Access a Cisco Router
- Lab 5.3 Use the System Configuration Dialog to Configure a Cisco Router
- Lab 5.4 Configure Console and Aux Passwords
- Lab 5.5 Use Help, the Command History, Enhanced Editing Features, and the Show Command

## CCNA Exam Objectives

| Objective                                                                                                         | Lab |
|-------------------------------------------------------------------------------------------------------------------|-----|
| Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts | 5.1 |
| Access and utilize the router to set basic parameters                                                             | 5.2 |
| Connect, configure, and verify operation status of a device interface                                             | 5.3 |
| Implement basic router security                                                                                   | 5.4 |
| Verify router hardware and software operation using <code>show</code> and <code>debug</code> commands             | 5.5 |

## Lab 5.1 Connect the Internetwork Lab

### Objectives

The objective of this lab is to give you experience in making the hardware connections necessary to configure the Cisco router lab. This includes connecting computers, hubs, and routers to each other. In this lab you will connect five Cisco routers, five hubs, and five computers in preparation for router configuration.

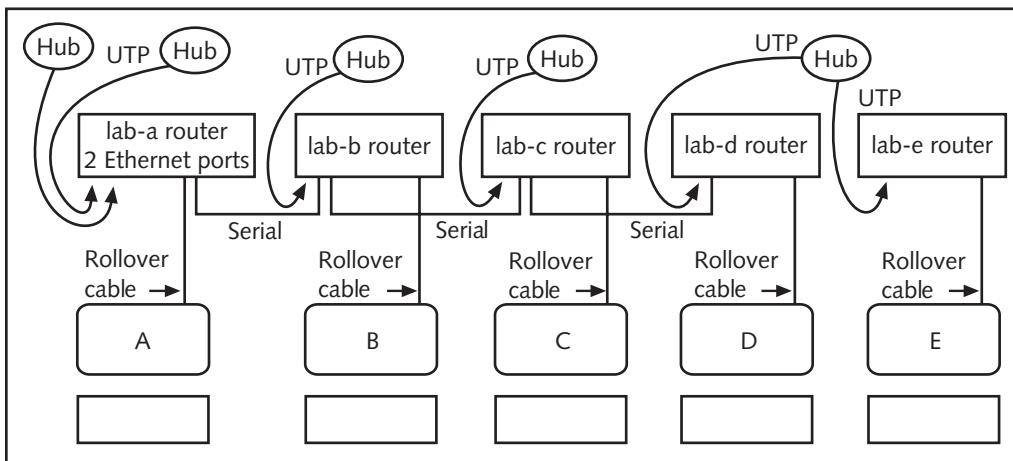
After completing this lab, you will be able to:

- Identify routers, hubs, transceivers, DCE/DTE cables, rollover cables, DB-9 connectors, and the COM ports on the computers
- Correctly connect the hardware using the proper cables

### Materials Required

This lab requires the following:

- Four 2620 series routers with power cables (could substitute a different series but must have two serial interfaces and one Ethernet or Fast Ethernet interface)
- One 2621 series router with power cable (could substitute a different series but must have two serial interfaces and two Ethernet or Fast Ethernet interfaces)
- Five hubs with power cables (can substitute switches)
- Three V.35 DTE cables (male) with serial ends to match serial interfaces on routers
- Three V.35 DCE cables (female) with serial ends to match serial interfaces on routers
- Six UTP patch cables
- Six Ethernet 10BaseT UTP-to-AUI transceivers (you will not need these if the Ethernet or Fast Ethernet interfaces on the routers are RJ-45 transceivers)
- Five RJ-45 to RJ-45 rollover cables
- Five RJ-45 to DB-9 connectors
- Power strips
- Five Windows computers with a COM port available. Computers should be set up and labeled lab-a through lab-e, as shown in Figure 5-1. Routers and hubs can be placed in a rack.
- Routers labeled lab-a through lab-e. Lab-a should be the router with the two Ethernet or Fast Ethernet interfaces.
- Long table or equipment rack



**Figure 5-1** Standard internetwork lab configuration

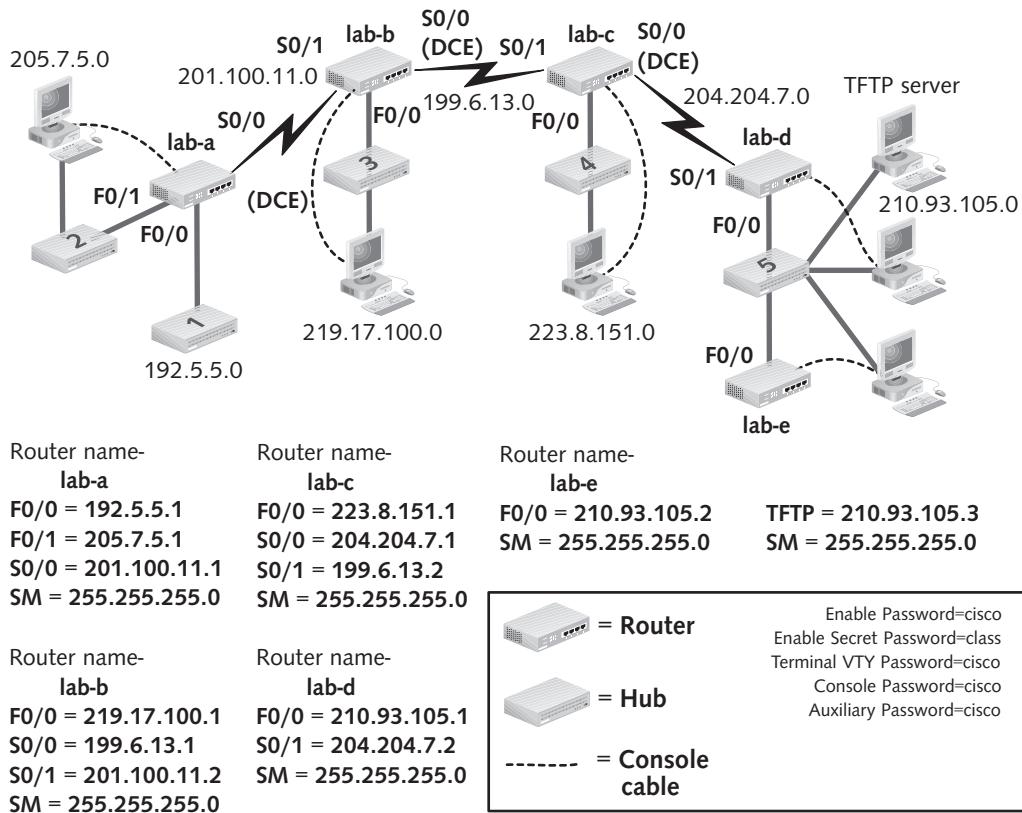
5

## Activity

Estimated completion time: 30 minutes

1. Lay the five routers on the long table behind the computers with the routers' port sides facing the back of the computers. Alternatively, load the routers in a rack in order from the lab-a router at the top to the lab-e router at the bottom.
2. Place a hub behind or on top of each router.
3. Refer to Figure 5-2 for help with the next steps regarding cabling. The TFTP server will be connected in Lab 6.2.
4. Connect the lab-a router's first Fast Ethernet interface (F0/0) to the hub behind it using a UTP patch cable. You may need a transceiver on the AUI0 port on the router to accept the RJ-45 connector. At the hub, make sure the UTP is not plugged into an uplink port. Ask your instructor for help if you cannot determine which port is the uplink port.
5. Connect the lab-a router to a second hub via its second Fast Ethernet port (F0/1) or AUI1 port, as outlined in Step 4.
6. Connect the lab-b router to a third hub, as outlined in Step 4.
7. Connect the lab-c router to a fourth hub, as outlined in Step 4.
8. Connect both the lab-d and lab-e routers to the fifth hub, as outlined in Step 4 and shown in Figure 5-2.
9. Connect the console port of the lab-a router to a COM port on computer A using the router rollover cable and Figure 5-1 as your guide. At the COM port, you will need a DB-9 connector between the RJ-45 rollover cable and the COM port.
10. Repeat Step 9 for the remaining routers and computers.

## 510 Chapter 5 Router and IOS Basics

**Figure 5-2** Connection Information

11. The DTE and DCE cables should be marked as such. Connect each V.35 end of a DTE cable to the V.35 end of a DCE cable. You should now have three cables, each with a DTE end and a DCE end.
12. The 60-pin ends (or other serial end types) of the DTE and DCE serial cables should be connected to the serial ports on the routers. Be extremely careful to line up the connections correctly. Pins can easily be damaged if a connection is forced. Connect the lab-a router to the lab-b router using Figure 5-2 as a reference. Notice that the DCE end goes in the lab-a router's S0 port, and the DTE end goes in the lab-b router's S1 port. In this lab setup, the DCE ends always go into the S0 ports.
13. Repeat Step 12 to connect the lab-b router to the lab-c router, and again to connect the lab-c router to the lab-d router.
14. Connect all devices to the power strips using the correct power cables.
15. Ask your instructor to check your lab setup.

**Certification Objectives**

Objectives for the CCNA exam:

- Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts

## Review Questions

1. For what purpose is a transceiver used?
2. This lab connects routers directly to each other via serial cables. Is this a typical configuration? If not, to what equipment does the DCE end of the serial cable usually connect?
3. What does a rollover (console) cable look like?
4. What kind of port does the console cable attach to on the computer?
5. What kind of port does the UTP patch cable attach to on the router?

**5**

---

## Lab 5.2 Configure HyperTerminal to Access a Cisco Router

### Objectives

The objective of this lab is to give you experience configuring the Windows HyperTerminal program, which is frequently used to configure routers. In this lab you will configure HyperTerminal on a computer connected to a router via the console port. The computer was connected to the router in Lab 5.1.

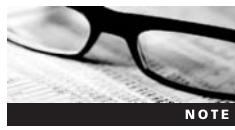
After completing this lab, you will be able to:

- Configure HyperTerminal on a Windows computer for use in configuring Cisco routers

### Materials Required

This lab requires the following:

- The internetworking lab setup in Lab 5.1 and shown in Figure 5-2, or a Windows computer connected to a Cisco router via the console port on the router
- HyperTerminal installed on a Windows computer



HyperTerminal is not included with Windows Vista, however you can download a free copy from <http://www.hilgraeve.com/htpe/download.html>

**NOTE**

### Activity

|                                       |
|---------------------------------------|
| Estimated completion time: 30 minutes |
|---------------------------------------|

1. Make sure the router connected to the computer is turned off.
2. Turn on the Windows computer.

**512** Chapter 5 Router and IOS Basics

3. Click **Start**, point to **All Programs**, point to **Accessories**, point to **Communications**, and then click **HyperTerminal**. This is the procedure for most Windows computers, however, the procedure may be slightly different on your Windows computer. Click **Yes** if prompted to make HyperTerminal your default telnet program.
4. If necessary, click **File** on the menu bar, and then click **New Connection** to open the New Connection window.
5. Enter an area code if prompted, and then click **No** if asked to install a modem.
6. In the Connection Description dialog box, enter the name **Cisco** for the connection. Click **OK** to continue.
7. You must now configure your connection to the router via the Connect To dialog box. In the **Connect using** selection box, choose the COM port to which the RJ-45 to DB-9 connector is attached. Click **OK** to continue.
8. Configure these settings for the COM port: Bits per second: **9600**; Data bits: **8**; Parity: **None**; Stop bits: **1**; Flow control: **None**. Click **OK** to complete the configuration.
9. Click **File** on the menu bar, and then click **Save** to save the connection.
10. Close HyperTerminal, click **Yes** if prompted to confirm, and then double-click the connection to reopen it.
11. Turn on the connected router.
12. Watch for the router startup information. You may need to press **Enter** on the computer keyboard to initiate this process.
13. When you know HyperTerminal is correctly configured, you may turn off the router and exit HyperTerminal and Windows or continue with the next lab.

## Certification Objectives

Objectives for the CCNA exam:

- Access and utilize the router to set basic parameters

## Review Questions

1. What program on a Windows computer is typically used for configuring a Cisco router?
2. What are the important settings to configure in HyperTerminal to access a Cisco router?
3. Where is the HyperTerminal program in most Windows computers?

4. Which port on a router do you use to connect the rollover cable when configuring the router with HyperTerminal?
5. You can use the auxiliary port on a router to access it with HyperTerminal. How would you be accessing the router if you used this port?

---

## Lab 5.3 Use the System Configuration Dialog to Configure a Cisco Router

**5**

### Objectives

The objective of this lab is to give you experience with the initial configuration of a Cisco router using the system configuration dialog. This dialog is a type of “wizard” that prompts you to enter the information that configures the router. This is easier than direct configuration using the command line.

Although most professionals do not use this method to configure Cisco routers, knowledge of the system configuration dialog is a CCNA objective. It is important to know how to use it and what it does. Remember that setting up the router using this method makes the router operational; however, it may not be completely configured.

After completing this lab, you will be able to:

- Use the system configuration dialog to configure the routers in the internetworking lab shown in Figure 5-2
- Know how to access the system configuration dialog
- Understand the capabilities and limitations of the system configuration dialog

### Materials Required

This lab requires the following:

- Completion of Labs 5.1 and 5.2
- HyperTerminal configured to access the routers via the console port, per Lab 5.2

### Activity

Estimated completion time: **45 minutes**

1. Refer to Figure 5-2. What will the host name of your router be?

---

2. Which interfaces is your router using?

---

3. What are the IP addresses and subnet masks for those interfaces?

**514** Chapter 5 Router and IOS Basics

4. What is the enable secret password?

---

5. What is the enable password?

---

6. What is the VTY password?

---

7. Turn the router off, if it is on. The router's startup configuration file should already be erased. Doing so makes the router prompt you to enter the initial configuration dialog, another term for the system configuration dialog.

8. Start Windows on the attached computer, if necessary. To open the HyperTerminal connection you created in Lab 5.2, click **Start**, point to **All Programs**, point to **Accessories**, point to **Communications**, and then click **HyperTerminal**. Double-click the Cisco connection icon. Alternatively, you may have to click the File menu then click Open to find the saved Cisco connection.

9. Turn on the router attached to your PC. If necessary, press **Enter** to get screen output. In a few seconds, you should see router activity display.

10. You may see a message that the NVRAM is invalid, possibly due to write erase. That is because your instructor has erased the startup configuration file or because the router is new and has never had a startup configuration.

11. Next, you are asked if you want to enter the initial configuration dialog. Press **y** for yes and press **Enter**. Notice that using the **Ctrl+C** key combination on the keyboard takes you out of the initial configuration dialog. This is sometimes necessary, as there is no way to go back and reenter an incorrect entry.

12. Next you are asked if you want to enter basic management setup. The basic management setup configures only enough connectivity to manage the router. The router will not be fully functional. You should press **n** for no and then press **Enter**. This puts you into extended setup.

13. When asked if you want to see the current interface summary, press **Enter** to accept the default answer shown in square brackets, which in this case is yes. The summary shows which interfaces are physically on the router. Remember that you will not necessarily configure all the displayed interfaces. Your configuration depends on the router you are configuring and the information in Figure 5-2.

14. Continue to configure your router, using the responses shown in Table 5-1 as your guide. The responses in the table are for the lab-c router. Tailor them to your router as shown in Figure 5-2 and the information you recorded in Steps 1 through 6 of this lab. As you move through the configuration process, note that valuable information is presented on the screen and be aware that some prompts in the table may not display. In addition, you may be prompted for information not in the table. This is because the system configuration dialog prompts you see are dependent on the particular IOS your router is using. Be sure to read everything that comes up. Eventually, your configuration is displayed and you are prompted to end the system configuration dialog by choosing option 0, 1, or 2. Choose **2** and press **Enter**. This saves your configuration to NVRAM and exits the system configuration dialog.

## Lab 5.3 Use the System Configuration Dialog to Configure a Cisco Router

**515**

| When You See This                                     | Enter the Following |
|-------------------------------------------------------|---------------------|
| Enter host name [Router] :                            | lab-c               |
| Enter enable secret:                                  | class               |
| Enter enable password:                                | cisco               |
| Enter virtual terminal password:                      | cisco               |
| Configure SNMP Network Management?                    | n                   |
| Configure DECnet?                                     | n                   |
| Configure AppleTalk?                                  | n                   |
| Configure IP?                                         | y                   |
| Configure IGRP routing?                               | n                   |
| Configure RIP routing?                                | y                   |
| Configure bridging?                                   | n                   |
| Configure IPX?                                        | n                   |
| Configure ASync lines?                                | n                   |
| Do you want to configure FastEthernet0/0 interface?   | y                   |
| Use the 100Base-TX (RJ-45) connection?                | y                   |
| Operate in full-duplex mode?                          | n                   |
| Configure IP on this interface?                       | y                   |
| IP address for this interface:                        | 223.8.151.1         |
| Subnet Mask for this interface [255.255.255.0] :      | Enter               |
| Do you want to configure Serial0/0 interface?         | y                   |
| Choose encapsulation type [hdlc] :                    | Enter               |
| Choose speed from above:                              | 56000               |
| Configure IP on this interface?                       | y                   |
| Configure IP unnumbered on this interface?            | n                   |
| IP address for this interface:                        | 204.204.7.1         |
| Subnet Mask for this interface [255.255.255.0] :      | Enter               |
| Do you want to configure Serial0/1 interface?         | y                   |
| Choose encapsulation type [hdlc] :                    | Enter               |
| Configure IP on this interface?                       | y                   |
| Configure IP unnumbered on this interface?            | n                   |
| IP address for this interface:                        | 199.6.13.2          |
| Subnet Mask for this interface [255.255.255.0] :      | Enter               |
| Would you like to go through AutoSecure configuration | n                   |

**5****Table 5-1** Configuration responses

**516** Chapter 5 Router and IOS Basics

15. There is another way to access the initial configuration dialog other than being prompted for it automatically as a consequence of having erased the contents of NVRAM. You can use the **setup** command at the privileged EXEC mode prompt. Press **Enter** if necessary to reach the user EXEC mode prompt. What does this prompt look like?

---

16. Type **enable** and press **Enter** to access privileged EXEC mode, which is also known as enable mode. You should be prompted for the enable secret password you configured in the system configuration dialog. How do you know you are being prompted for the enable secret password and not the enable password?

---

---

17. Type **class** and press **Enter**. How did the prompt change?

---

18. Enter the **setup** command to access the initial configuration dialog. When prompted to enter the initial configuration dialog, press **y** for yes and press **Enter**.

19. Press **Ctrl+C** to abort the configuration and exit the system configuration dialog.

20. Type **logout**, press **Enter**, close HyperTerminal, and then turn off the router.

## Certification Objectives

Objectives for the CCNA exam:

- Connect, configure, and verify operation status of a device interface

## Review Questions

1. When configuring a router, when would you choose basic management setup rather than extended setup?

2. Which passwords are you prompted for when using the initial configuration dialog?

3. What does the current interface summary show you?

4. How can you break out of setup if you make a mistake?

5. What do square brackets [ ] in a prompt for input indicate?

6. Under what condition are you automatically prompted to enter the initial configuration dialog?
7. What command and prompt puts you into the initial configuration dialog?
8. Why is it important to configure an enable or enable secret password on a router?

**5**

---

## Lab 5.4 Configure Console and Aux Passwords

### Objectives

In Lab 5.3 you were prompted for the VTY (virtual terminal) password in addition to the enable and enable secret passwords when configuring the router using the system configuration dialog. The VTY password restricts access to the router via telnet. The VTY password is an example of a line password because you are getting a line into the router.

Besides VTY, two additional lines provide access into the router. You can access the router through the console line and use a console password, which restricts access to the router through the console port. You can also access it through the auxiliary line by using the aux password, which restricts access through the aux port via a modem. Note that neither password is configured when using the system configuration dialog. Note also that a console password is not currently required when accessing your router via the console port.

In this lab, you will configure the console and aux passwords for the internetworking lab shown in Figure 5-2.

After completing this lab, you will be able to:

- Configure the console and aux passwords on a router

### Materials Required

This lab requires the following:

- Completion of Labs 5.1, 5.2, and 5.3
- HyperTerminal configured to access the routers via the console port, per Lab 5.2

### Activity

|                                       |
|---------------------------------------|
| Estimated completion time: 45 minutes |
|---------------------------------------|

1. If necessary, boot the computer into Windows and begin the HyperTerminal session with the router.
2. Turn on the router if necessary. Press **Enter** to get the user EXEC mode prompt, which should be the name of the router (for example, lab-e) and the greater-than sign (>).

**518** Chapter 5 Router and IOS Basics

3. Type **ena** and press **Enter** to access privileged EXEC mode. Why didn't you have to type the entire command?

---

4. Type **class** and press **Enter** when prompted for the password. The prompt should change. For example, if the router name is **lab-e**, the prompt should change to **lab-e#**.
5. Type **configure terminal** and press **Enter** to enter global configuration mode. What did the prompt change to?

---

6. Type **line console 0** and press **Enter**. This tells the router that you want to configure the console port. The prompt should change to indicate that you are in line configuration mode. What did the prompt change to?

---

7. Type **password cisco** and press **Enter**.
8. Type **login** to require users to log in when accessing this port, and press **Enter**.
9. Type **exit** and press **Enter**. How many levels does the **exit** command take you back?

---

10. Type **line aux 0** and press **Enter**. This tells the router that you want to configure the aux port.
11. Type **password cisco** and press **Enter**.
12. Type **login** to require users to log in when accessing this port, and press **Enter**.
13. Press **Ctrl+Z**. To what prompt does this key combination take you back?

---

14. Press **Enter** after you receive the message that the router has been configured by the console.
15. Type **show run** and press **Enter** to see the running configuration. Notice that the enable secret password is encrypted and looks nothing like "class," which is the password you entered during the system configuration dialog.
16. Press the **spacebar** to see more of the display.
17. Notice the console, aux, and VTY password information. Are these passwords encrypted?

---

18. Type **copy run start** and press **Enter**. Press **Enter** again to accept startup-config as the destination filename. What does the **copy run start** command do?

---

19. Is it really necessary to use this **copy run start** command, or are the configuration changes automatically saved?

---

20. Type **logout** and press **Enter** to exit the router.

## Certification Objectives

Objectives for the CCNA exam:

- Implement basic router security

## Review Questions

1. Which passwords are you not prompted for when using the system configuration dialog?
2. Which mode must you be in to configure the VTY, console, and auxiliary passwords?
3. What does the prompt look like if you are in the mode that is the correct answer for Review Question 2?
4. What two commands are used to create the line passwords after you are at the prompt you specified in Review Question 3?
5. What is the only router password encrypted by default?

**5**

---

## Lab 5.5 Use Help, the Command History, Enhanced Editing Features, and the Show Command

### Objectives

The objective of this lab is to give you experience in accessing command-line help, using the Cisco enhanced editing features and command history, and using the very important show commands to determine information about your router.

With a little experience, you can figure out how to do almost anything on a Cisco router or switch using command-line help. In addition, the enhanced editing features of the Cisco command executive allow you to move around commands quickly and avoid retyping previously used commands. You use show commands to monitor and verify what you have configured in the router. In this lab, you will use command-line help and various show commands, and you will edit the command line using the editing features of the Cisco command executive.

After completing this lab, you will be able to:

- Get help with commands
- Navigate the command line more efficiently
- Understand the kinds of information you can obtain using the most popular show commands

## Materials Required

This lab requires the following:

- Completion of Labs 5.1, 5.3, and 5.4
- HyperTerminal configured to access the routers via the console port, per Lab 5.2

## Activity

Estimated completion time: 60 minutes

1. Boot the computer into Windows if necessary, and begin the HyperTerminal session with the router.
2. Turn on the router if necessary. Press **Enter**. Which password are you being prompted for?

---

3. Enter the password you configured in Lab 5.4.

---

4. After the correct password is entered, your cursor should be at the user EXEC mode prompt, which should be the name of the router and the greater-than sign (for example, `lab-e>`). Verify that this has occurred.

5. Type `?`. There is no need to press Enter. A list of commands should be displayed. Press the **spacebar** to scroll through the list. What do these commands represent?

---

6. Type `show ?`. A list of commands should appear. Press the **spacebar** to scroll through the list. What do these commands represent?
- 



Notice that the `show start` and `show run` commands cannot be used in user EXEC mode.

NOTE

7. Complete the `show` command by typing `hosts` and pressing **Enter**. Does your router know the names of any other routers? Why or why not?
- 
- 

8. Type `show version` and press **Enter**. What is the name of the IOS image file?
- 
- 

9. What version of the IOS is your router running?
-

## Lab 5.5 Use Help, the Command History, Enhanced Editing Features, and the Show Command

**521**

10. Press the **spacebar** to scroll through the display if necessary.
11. Type **enable** and press **Enter** to access enable mode.
12. Type **class** and press **Enter** when prompted for the enable secret password. How did the prompt change?

---

13. Type **?**. Press the **spacebar** to scroll through the commands. What do these commands represent?

---

14. Type **show ?**. What do these commands represent? Why are there so many more commands in enable mode than in user mode?

**5**

---

15. Use the **show flash** command to display information about the flash. What is the IOS filename? Your answer should be the same as what you recorded in Step 8.

---

How big is the file?

---

16. Type **show protocol** and press **Enter**. What protocol is enabled on your router?

---

17. What interface and address information appears?

---

18. Type **show arp** and press **Enter**. What information does this command display?

---

19. Type **clear ?** and look for the command to clear the contents of the ARP table. What do you think the command is?

---

20. Backspace over the word **clear** to erase it if necessary. Type **show start** and press **Enter**. What are you viewing the contents of?

---

21. What is the host name of the router?

---

22. What interfaces are available for configuration on the router?

---

23. What interfaces are actually configured on the router?

**522** Chapter 5 Router and IOS Basics

24. Is a routing protocol configured on the router? If so, what is it?

---

25. Type **show run** and press Enter. What are you viewing the contents of?

---

26. Is the running configuration supposed to be the same as the startup configuration? Explain your answer.

---

---

---

27. Type **show history** and press Enter. What appears?

---

28. Press the **up arrow** until you see the **show start** command. What does the up arrow do?

---

29. Press the **down arrow** until you see the **show history** command. What does the down arrow do?

---

30. Press **Ctrl+A**. What does this do?

---

31. Press **Ctrl+E**. What does this do?

---

32. Press **Esc+B**. What does this do?

---

33. Press **Esc+F**. What does this do?

---

34. Delete the command by pressing the **backspace** key. Type **terminal his** and press the **Tab** key. What does this do?

---

---

35. Use context-sensitive help to determine why the terminal history size command is used.

---

36. Change the history buffer size to 20 using the **terminal history size 20** command.

37. Enter the **show history** command again. You changed the buffer from the default of 10 to 20. Are there more than 10 entries in the buffer? Do you expect that an increased buffer size would require more router memory use?
- 
38. Type **logout** and press Enter to exit the router. Close HyperTerminal and turn off the router.

## Certification Objectives

Objectives for the CCNA exam:

**5**

- Verify router hardware and software operation using show and debug commands

## Review Questions

1. Within the lab exercise, what exactly did the “?” show you?
2. Is the “?” prompt sensitive?
3. Which two commands display information about the IOS file?
4. What command increases the history size?
5. What is the key combination that has the same result as pressing the up arrow?



## C H A P T E R S I X

# ROUTER STARTUP AND CONFIGURATION

## Labs included in this chapter

- Lab 6.1 Configure IP Addresses and IP Hosts
- Lab 6.2 Install, Configure, and Use a TFTP Server
- Lab 6.3 Configure a Message and Interface Description
- Lab 6.4 Use the CDP, Ping, Trace, and Telnet Commands
- Lab 6.5 Use Boot System Commands and the Configuration Register
- Lab 6.6 Investigate the Security Device Manager (SDM) Interface

## CCNA Exam Objectives

| Objective                                                                                                    | Lab                     |
|--------------------------------------------------------------------------------------------------------------|-------------------------|
| Access and utilize the router to set basic parameters (including CLI/SDM)                                    | 6.1, 6.2, 6.3, 6.5, 6.6 |
| Connect, configure, and verify operation status of a device interface                                        | 6.1, 6.4, 6.6           |
| Configure and verify a basic WAN serial connection                                                           | 6.1                     |
| Manage IOS configuration files (including save, edit, upgrade, restore)                                      | 6.2                     |
| Manage Cisco IOS                                                                                             | 6.2, 6.5                |
| Verify device configuration and network connectivity using ping, traceroute, telnet, SSH, or other utilities | 6.4                     |
| Troubleshoot WAN implementation issues                                                                       | 6.4                     |

## Lab 6.1 Configure IP Addresses and IP Hosts

### Objectives

The objective of this lab is to give you experience in configuring IP addresses without the aid of the system configuration dialog. In addition, you will make IP to host name mappings. These mappings can be configured using a name server, or in this case, the router. In this lab, you will use the IP address command to configure the router interfaces, and the IP host command to provide IP to host name mappings.

After completing this lab, you will be able to:

- Configure IP addresses for each interface on the router
- Configure IP to host name mappings using the IP host command

### Materials Required

This lab requires the following:

- The internetworking lab setup shown in Figure 6-1
- Completion of all labs in Chapter 5

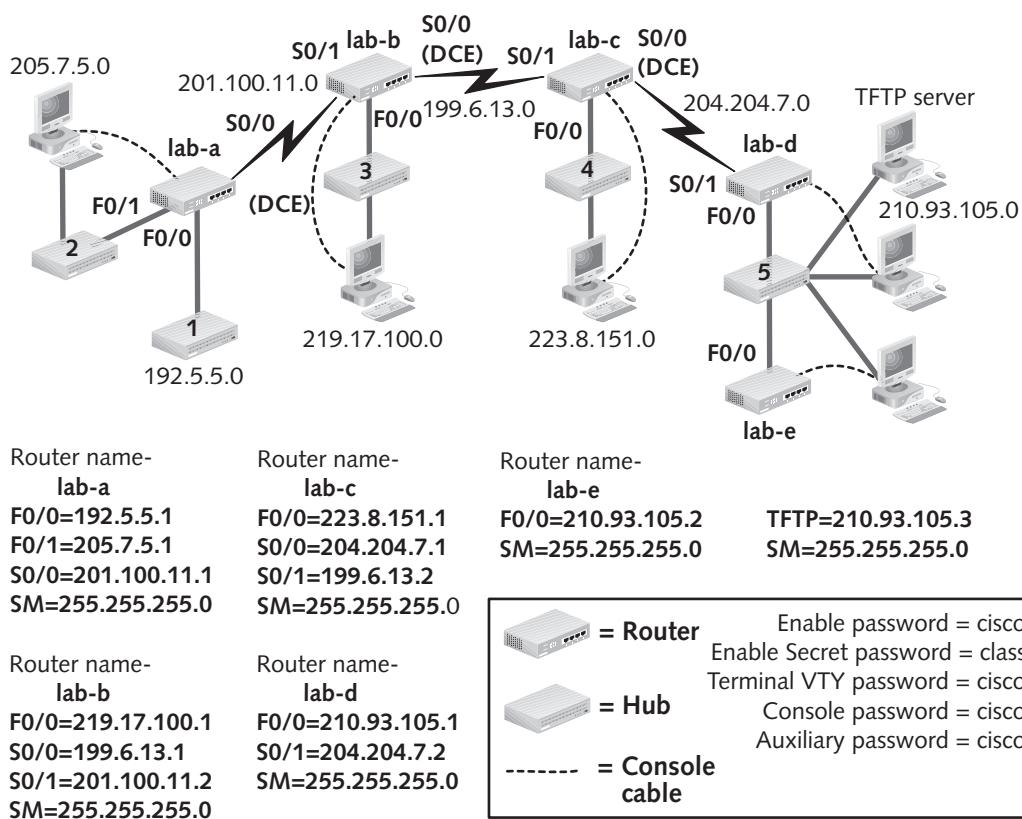


Figure 6-1 Connection information

## Activity

Estimated completion time: **45 minutes**

1. Boot the computer into Windows, and begin the HyperTerminal session with the router.
2. Turn on the router and switches or hubs if necessary. Press **Enter** to start, and type the console line password **cisco** to get to the user EXEC mode prompt.
3. Type **enable** and press **Enter** to access privileged EXEC mode.
4. Type **class** and press **Enter** when prompted for the enable secret password.
5. Type **conf t** and press **Enter**. What is the name of this mode?
6. Enter a name table into the router. Put all routers in the name table, including the one you are configuring. Refer to Figure 6-1 for router host name and IP addressing information. Type **ip host**, then the name of the first router in the lab, which is **lab-a**, and all IP addresses associated with the interfaces on this first router. Remote routers will attempt to access the named router via the IP addresses in the order you list them. Press **Enter**. The first lab router is the **lab-a** router, so you should have typed the following:  
**ip host lab-a 192.5.5.1 205.7.5.1 201.100.11.1**  
Note that the addresses in this example are the interfaces listed in the network diagram in Figure 6-1.  
7. Repeat Step 6 for all routers. Each router should eventually have the IP addresses of all router interfaces in the internetwork.
8. Press **Ctrl+Z** to exit global configuration mode. Press **Enter** to clear the message.
9. What is the value of the IP host command?

---

10. Type **show hosts** and press **Enter**. What hosts does your router know about?

---
11. Next, you will configure the active router interfaces for IP addresses. Type **conf t** and press **Enter**.  
12. Type **int f0/0** (to represent the first FastEthernet interface) and press **Enter**. What mode are you in, and what will the next commands you type affect?

---
13. To configure the IP address of the FastEthernet 0/0 interface, type the following:  
**ip address [IP address of your router's f0/0 interface] [subnet mask]**  
**no shutdown**  
Use Figure 6-1 to determine the IP address of your router's f0/0 interface.
14. What does the first command line do in the example in Step 13?

---
15. What does the second line do?

---

## 528 Chapter 6 Router Startup and Configuration

16. Using Steps 12 and 13 as an example, configure the IP addresses of any additional interfaces that are to be configured on your router, per Figure 6-1. If you are configuring an s0/0 interface, you will need three commands instead of two. s0/0 has arbitrarily been chosen to perform the clocking function for the WAN links. Typically, the telco's CSU/DSU or other device does the clocking (DCE) outside of the lab environment. Make sure to add the following configuration command for s0/0 if you have an active s0/0 interface:

```
clock rate 56000
```



Depending on the IOS version, the `clock rate` command can also be written as `clockrate`.

17. When finished configuring all interfaces on your router, as shown in Figure 6-1, press **`Ctrl+Z`** to return to the enable prompt.
18. Type **`show run`** to view the running configuration. There will be additional information in the running configuration that you did not configure. This consists of default router settings that are automatically configured and beyond the scope of the CCNA exam. Figure 6-2 displays the correct running configuration for the lab-c router.

```
Lab-c#show run
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname lab-c ←
!
enable secret 5 $1$ULYh$6L5jeGvqj8OuPZ0Hu0nRI/
enable password cisco ←
!
!
ip subnet-zero
ip host lab-e 210.93.105.2
ip host lab-d 210.93.105.1 204.204.7.2 ←
ip host lab-c 223.8.151.1 204.204.7.1 199.6.13.2
ip host lab-b 219.17.100.1 199.6.13.1 201.100.11.2
ip host lab-a 192.5.5.1 205.7.5.1 201.100.11.1
ip audit notify log
ip audit po max-events 100
!
interface FastEthernet0/0
  ip address 223.8.151.1 255.255.255.0
  no ip directed-broadcast
  speed auto
  half-duplex
  no mop enabled
```

The hostname for this router is lab-c

The enable secret password, which is class, is encrypted and unrecognizable; the enable password cisco is in clear text

The host name table allows you to use names rather than IP addresses when referring to the routers

Figure 6-2 Output of the `show run` command

```

!
interface Serial0/0
 ip address 204.204.7.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
clockrate 56000 ← Notice the clockrate command
 configured on the S0/0 interface
!
interface Serial0/1
 ip address 199.6.13.2 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0/3
 no ip address
 no ip directed-broadcast
 shutdown
!
router rip
 redistribute connected
network 199.6.13.0 ← RIP is configured using major network
network 204.204.7.0 numbers of connected networks
network 223.8.151.0
!
ip classless
no ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
password cisco ← Console, auxiliary, and vty passwords are
login
transport input none

line aux 0
password cisco ← configured with the password cisco
login

line vty 0 4
password cisco
login
!
no scheduler allocate
end

```

6

**Figure 6-2** Output of the `show run` command (continued)

19. Check all commands and IP addresses, router RIP network numbers, and IP host addresses. RIP was configured automatically via the system configuration dialog in Lab 5-3. The network numbers listed for RIP should be the networks directly connected to your router. If there are no errors, proceed to Step 24.
20. If there is an error in the interface configurations, return to Steps 11 through 18 and reconfigure the interfaces. Then go to Step 24.

**530** Chapter 6 Router Startup and Configuration

21. If there is an error in the router RIP, type **conf t** and press **Enter** to enter global configuration mode. Then type **no router rip** and press **Enter** to remove the incorrect RIP information. Now type **router rip** to enter router configuration mode. Enter the correct numbers of the networks that are directly attached to your router, using this command as an example:  
**network 210.93.105.0**
22. Continue to use the network command until all networks attached to your router are listed. For example, the lab-a router will have three network command lines, because it is attached to three networks. Remember to use major network numbers, not interface addresses. When finished, press **Ctrl+Z** to return to enable mode.
23. If there is no error in the list of IP host names, go to Step 24. If there is an error in the list, type **conf t** and press **Enter**. Then type **no ip host** followed by the name of the router that has the error. Go to Steps 6 through 8, and reconfigure the IP to host name mappings. When you are sure they are correct, proceed to Step 24.
24. Type **copy run start** at the enable prompt, and press **Enter** to replace the startup configuration file. Press **Enter** again to accept the default destination filename.
25. Type **logout** to exit the router.

## Certification Objectives

Objectives for the CCNA exam:

- Access and utilize the router to set basic parameters (including CLI/SDM)
- Connect, configure, and verify operation status of a device interface
- Configure and verify a basic WAN serial connection

## Review Questions

1. What mode must you be in to configure IP addresses on a Cisco router?
2. What is the purpose of a host name table?
3. What is the command to point to another router or server for host name resolution?
4. What is the **clock rate** command used for?
5. What does the **no shutdown** command do?

## Lab 6.2 Install, Configure, and Use a TFTP Server

### Objectives

The objective of this lab is to show you the benefit of having a TFTP server on your network to configure the routers in the event they lose their IOS or configuration information. If you completed the labs in Chapter 5 and Lab 6.1 properly, your routers are configured to match the internetworking lab setup shown in Figure 6-1. It is now appropriate to back up these configurations to a TFTP server.

In this lab you will copy the five router configuration files as well as a single copy of the IOS to the TFTP server.

After completing this lab, you will be able to:

- Copy router configurations to the TFTP server
- Copy the Cisco IOS from the router to the TFTP server

6

### Materials Required

This lab requires the following:

- Completion of all labs in Chapter 5
- Completion of Lab 6.1
- A Windows computer configured with TFTP server software and with the IP address 210.93.105.3 /24 and the gateway configured as 210.93.105.1. The TFTP server should be connected with a UTP patch cable to the hub between the lab-d and lab-e routers, as shown in Figure 6-1.

### Activity

Estimated completion time: **45 minutes**

1. Open the TFTP program on the TFTP server by clicking Start, pointing to All Programs, and then clicking the name of the TFTP program; you can also double-click a desktop shortcut if one exists.
2. Move to a router terminal, and boot the computer into Windows if necessary.
3. Begin the HyperTerminal session with a router.
4. Turn on the router and hubs if necessary. Press Enter to start, and then type **cisco** for the user EXEC mode password.
5. Type **enable** and press Enter to access privileged EXEC mode.
6. Type **class** and press Enter when prompted for the enable secret password.
7. What command will you type to look at the active configuration?

Use the command you recorded in Step 7, and check to make sure it has been configured correctly, per Figure 6-1.

8. Ping the TFTP server to make sure you have connectivity to it. Type **ping** followed by 210.93.105.3, which is the IP address you configured on the TFTP server. Press Enter.

**532** Chapter 6 Router Startup and Configuration

If your ping fails, use the **show interfaces** command to make sure all of your configured interfaces are up/up. Perhaps your team members are having problems that may be affecting your ping. Also, make sure you check all physical connections and the TCP/IP configuration on the TFTP server. When you can ping the TFTP server successfully, proceed to the next step.

9. Type **copy run tftp** and press **Enter** to begin the process of backing up the running configuration to the TFTP server. This command will eventually fail if the TFTP server software is not running.
10. Next you are prompted for the IP address of the TFTP server. Type **210.93.105.3** and press **Enter**.
11. You are prompted for the name of the configuration file. Press **Enter** to accept the default name, which is **lab-c-config** for the lab-c router. Look at the screen on the TFTP server for an indication of success.
12. Type **show flash** and press **Enter**. What is the name of the IOS image of the router? Look at the name carefully. Depending on the font style being used in HyperTerminal, it can be difficult to tell the difference between a lowercase L and the number 1.

---

13. Backing up the configuration files is typically fast, as these files are small. Conversely, the IOS file is relatively large and takes more time to back up. Because the same IOS file is probably running on all the routers in the lab, only the person configuring the lab-e router should back up the IOS, which begins in the next step. The other team members should observe the process.
14. If you are configuring the lab-e router, type **copy flash tftp** and press **Enter** to begin backing up the router operating system (IOS) on the TFTP server.
15. You are prompted for the source filename. Type the name of the file you recorded in Step 12 and press **Enter**.
16. Next, you are prompted for the IP address of the remote host, which is the TFTP server. Type **210.93.105.3**, and press **Enter**.
17. Finally, you are prompted for the destination filename. The default (indicated in square brackets) is the same name you typed for the source filename in Step 15. Press **Enter** to accept the default.
18. A series of exclamation marks on your screen indicates the IOS is copying to the TFTP server. Notice that the transfer process appears as a series of hash marks on the TFTP server. The backup process will take a minute or so.
19. When the process is finished, go to the TFTP server and search for the backed-up files on the hard drive. When the router lab is completely backed up, you should have five configuration files and one IOS file on the TFTP server.
20. Log out of the router.

## Certification Objectives

Objectives for the CCNA exam:

- Access and utilize the router to set basic parameters (including CLI/SDM)
- Manage IOS configuration files (including save, edit, upgrade, restore)
- Manage Cisco IOS

## Review Questions

1. What is the purpose of a TFTP server?
  2. What is the purpose of a default gateway?
  3. What prompt and command are used to copy the active configuration to a TFTP server?
  4. What prompt and command are used to copy the IOS to a TFTP server?
5. List two show commands that display the IOS image filename.

6

---

## Lab 6.3 Configure a Message and Interface Description

### Objectives

The objective of this lab is to show you how to customize your router further by configuring a message of the day and by assigning descriptions to interfaces. In this lab, you will use the banner motd command and the description command to customize your router.

After completing this lab, you will be able to:

- Use the banner motd command to provide a message for anyone accessing the router
- Use the description command to add a description to a configured interface

### Materials Required

This lab requires the following:

- Completion of all labs in Chapter 5, as well as Lab 6.1

### Activity

|                                              |
|----------------------------------------------|
| Estimated completion time: <b>20 minutes</b> |
|----------------------------------------------|

1. Boot the computer into Windows, and begin a HyperTerminal session with the router.
2. Turn on the router and hubs if necessary. Press **Enter** to start, and type the password **cisco** to get to the user EXEC mode prompt.
3. Type **enable** and press **Enter** to access privileged EXEC mode.
4. Type **class** and press **Enter** when prompted for the enable secret password.
5. Type **conf t** and press **Enter** to enter global configuration mode.

**534** Chapter 6 Router Startup and Configuration

6. Type **banner motd #** and press Enter. What message appears?

---
7. Type **Welcome to the Cisco 2600 series router.**
8. Type **#** and press Enter to signal the end of your message. Press **Ctrl+Z** to exit global configuration mode.
9. Type **exit** and press Enter to log out of the router.
10. When prompted by the router, press **Enter** to start. You should see the message of the day.
11. Enter the password **cisco** to get to the user EXEC mode prompt.
12. Type **enable** and press Enter to access enable mode.
13. Type **class** and press Enter when prompted for the enable secret password.
14. Type **conf t** and press Enter to enter global configuration mode.
15. Type **no banner motd** and press Enter. This removes the message of the day.
16. From the global configuration mode prompt, type **int f0/0** and press Enter to enter interface configuration mode.
17. Type **description Attached to Ethernet LAN lab-e** (substitute the name of your router if necessary) and press Enter.
18. Press **Ctrl+Z** to return to the enable prompt.
19. Type **show int f0/0**. Does the description configured for f0/0 appear?

---
20. Copy the running configuration to the startup configuration.
21. Type **logout** to exit the router.

## Certification Objectives

Objectives for the CCNA exam:

- Access and utilize the router to set basic parameters (including CLI/SDM)

## Review Questions

1. What is the purpose of the banner command?
2. What does MOTD stand for?
3. What is the purpose of the description command?

4. What mode must you be in to configure a banner?
5. What mode must you be in to configure a description?

---

## Lab 6.4 Use the CDP, Ping, Trace, and Telnet Commands

### Objectives

The Cisco Discovery Protocol (CDP) shares configuration information between locally connected Cisco devices. The various show CDP commands tell you about routers and switches that are directly connected to your router. The ping and trace commands provide connectivity information at the Network layer of the OSI reference model and are used primarily for troubleshooting. Extended mode ping is a more sophisticated type of ping that you will also investigate. The telnet application provides Application layer connectivity information and lets you access remote routers.

6

The objective of this lab is to familiarize you with the displayed output of the various show cdp commands and other configured CDP commands. In addition, you will become familiar with the following troubleshooting commands: ping, extended mode ping, trace, and telnet.

After completing this lab, you will:

- Be familiar with the output generated by the various CDP commands
- Understand how to test for Network layer connectivity using the ping and trace commands
- Understand the difference between ping and extended mode ping
- Know how to use the telnet application to remotely access routers

### Materials Required

This lab requires the following:

- Completion of all labs in Chapter 5, as well as Lab 6.1

### Activity

Estimated completion time: **30 minutes**

1. Start the computer into Windows, and begin the HyperTerminal session with the router.
2. Turn on the router and hubs if necessary. Press **Enter** to start, and type the password **cisco** to get to the user EXEC mode prompt.
3. Type **enable** and press **Enter** to access enable mode.
4. Type **class** and press **Enter** when prompted for the enable secret password.

**536** Chapter 6 Router Startup and Configuration

5. Type **show cdp neighbors** and press Enter to get information regarding your directly connected neighbors. If you are unable to see your neighbors, use the **show interfaces** command and make sure the status of each of your interfaces is up/up. What is one of your neighbors?

---

What local interface is the neighbor on?

---

What kind of device is it (capability)?

---

What other information does this show command provide?

---

---

6. Press the **up arrow** until you get to the **show cdp neighbors** command. Press the **spacebar** once, then type **detail** and press **Enter**. What additional information do you get when you add “**detail**” to the **show cdp neighbor** command?

---

---

7. Type **show cdp interface** and press **Enter**. What is the default broadcast interval for CDP?

---

8. Type **conf t** and press **Enter** to enter global configuration mode.
9. Type **cdp timer 90** and press **Enter**. Exit to enable mode, and enter the **show cdp interface** command once again. Were you successful in changing the broadcast interval to 90 seconds?

---

10. Enter global configuration mode. Type **int f0/0** and press **Enter**.

11. Type **no cdp enable** and press **Enter**. What does this command do?

12. Press **Ctrl+Z** to return to enable mode, and enter the **show cdp interface** command. Has CDP been disabled on f0/0?

---

How do you know?

---

13. Reenable CDP on the interface using the **cdp enable** command in interface configuration mode.

## Lab 6.4 Use the CDP, Ping, Trace, and Telnet Commands

537

14. Press **Ctrl+Z** to return to enable mode. Can you confirm that CDP has been reenabled on the f0/0 interface?

---

15. Type **ping** and then type an IP address of a remote router interface. For example, if you are on the lab-b router and want to check for connectivity to the lab-d, S0/1 interface, you would type **ping 204.204.7.2** and press **Enter**.
16. Was the ping successful?

---

If not, attempt to ping several other interfaces. What symbol indicates a successful ping?

---

If your ping succeeded, what were the minimum, average, and maximum round trip times?



17. Type **ping** and press **Enter**. How does the extended mode ping command respond?

---

18. Press **Enter** to accept the default protocol. Enter any remote IP address. Change the repeat count to 20. Change the datagram size to 1500. Continue to press **Enter** to accept the defaults for the remaining prompts. How does this output differ from the output from the ping command you issued in Step 15?

---

---

19. Type **trace** and then type the IP address of an interface on the farthest remote router from your location. For example, if you are on the lab-b router and want to check for connectivity to the f0/0 interface on the lab-e router, type **trace 210.93.105.2** and press **Enter**.



If locked into an unsuccessful trace, break out by pressing **Ctrl+Shift+6**.

NOTE

20. Was the trace successful?

---

What information is obtained from the **trace** command?

---

What is the advantage of using the **trace** command instead of the **ping** command?

---

21. At which layer of the OSI reference model do ping and trace operate?

**538** Chapter 6 Router Startup and Configuration

22. At which layer of the TCP/IP reference model do Ping and Trace operate?

---

23. What underlying protocol controls the messages from Ping and Trace and also manages the work of IP in general?

---

24. Type **telnet** and then type the IP address of an interface on a remote router. For example, if you are on the lab-b router and want to telnet to the lab-e router, type **telnet 210.93.105.2** and press **Enter**.

Alternatively, you could just use the name of the router to which you want to connect. For example, you could type **lab-e** and press **Enter**.

What makes it possible to use names instead of IP addresses when telnetting? (*Hint:* See Lab 6.1.)

---

Did the telnet succeed?

---

25. If the telnet failed, try telnetting to a different router until you can telnet successfully. Ask your instructor for help if necessary.

26. You should be prompted for a password when you telnet successfully. Type **cisco** and press **Enter**. Is this the same kind of password you are prompted for when you log on to a router locally?

---

Exactly what kind of password is this?

---

27. Type **enable** and press **Enter** to access enable mode.

28. Type **class** and press **Enter** when prompted for the enable secret password.

29. Type **show run** and press **Enter**. Exactly what is displayed?

---

30. Type **show cdp neigh det** and press **Enter**. What is the advantage of using the telnet application in conjunction with the **show cdp neighbor** command?

---

31. At which layer of the OSI reference model is telnet operating?

---

32. At which layer of the TCP/IP reference model is telnet operating?

---

33. As a troubleshooting tool, what advantages does telnet have over ping and trace?

---

34. Type **logout** and press **Enter** to terminate your telnet session.

35. Type **logout** and press **Enter** to exit your router.

## Certification Objectives

Objectives for the CCNA exam:

- Connect, configure, and verify operation status of a device interface
- Verify device configuration and network connectivity using ping, traceroute, telnet, SSH, or other utilities
- Troubleshoot WAN implementation issues

## Review Questions

1. What is the purpose of the CDP protocol?
2. Is CDP enabled by default on all Cisco routers?
3. What is the difference between ping and extended mode ping?
4. What mode and command are used to disable CDP on an interface?
5. What mode and command are used to disable CDP on the entire router?

6

---

## Lab 6.5 Use Boot System Commands and the Configuration Register

### Objectives

When the router starts, it goes through a specified procedure outlined in Chapter 6 of your text. The IOS can be loaded from flash memory, ROM, or a TFTP server. By default, the configuration register is set to look to the startup configuration in NVRAM for boot instruction commands. If there are none, the IOS is loaded from flash by default. You can also affect the boot procedure by changing the configuration register.

The objective of this lab is to learn how to examine the configuration register and enter boot system commands into the router's configuration to force the router to boot from a TFTP server or to ROM. You will also learn how to change the configuration register and force the router to boot the IOS from ROM.

After completing this lab you will:

- Be familiar with the configuration register and its various settings
- Understand the various boot system commands and how to force the router to boot the IOS from a TFTP server or from ROM

## Materials Required

This lab requires the following:

- Completion of all labs in Chapter 5, as well as Labs 6.1 and 6.2

## Activity

Estimated completion time: **45 minutes**

1. Boot the computer into Windows, and begin the HyperTerminal session with the router.
2. Turn on the router and hubs if necessary. Press **Enter** to start, and type the password **cisco** to get to the user EXEC mode prompt.
3. Type **enable** and press **Enter** to access enable mode.
4. Type **class** and press **Enter** when prompted for the enable secret password.
5. Type **ping 210.93.105.3** to make sure you have connectivity to the TFTP server. If you do not have connectivity, check the status of your interfaces by typing **show interfaces**. You can also trace to the TFTP server to pinpoint where the problem is.
6. Check to make sure the TFTP server software is running on the TFTP server.
7. Type **show version** and press **Enter**. Scroll to the bottom of the command output. What is the name of the IOS image file?

---

What is the configuration register setting?

---

From where does this register setting indicate the IOS will be loaded?

---

8. Type **conf t** and press **Enter** to enter global configuration mode. Only the person configuring the lab-e router will perform Steps 9 through 19, which configure the lab-e router to boot from the TFTP server using the IOS that was previously copied to the server. The other team members should observe this process.
  9. Type **boot system tftp [filename]**, where filename is the name of the IOS image file you recorded in Step 7.
  10. Exit to enable mode.
  11. Type **copy run start** and press **Enter**. Press **Enter** again to confirm.
  12. Type **reload** and press **Enter**. Press **Enter** again to confirm.
  13. When the router reloads, it will look to NVRAM for boot system commands. What tells it to do this?
- 
14. If your boot system command was correctly configured, your router will load the IOS from the TFTP server. It will take a few minutes and you will see a series of exclamation

marks while it is loading. If it does not load correctly, you probably made a mistake when entering the filename. Make sure you recorded the filename correctly. Repeat Steps 8 through 12 if necessary.

15. Eventually you should be prompted to press **Return** to get started. Type the password **cisco** to get to the user EXEC mode prompt.

16. Type **enable** and press **Enter** to access enable mode.

17. Type **class** and press **Enter** when prompted for the enable secret password.

18. Type **conf t** and press **Enter** to enter global configuration mode.

19. Type **no boot system tftp [filename]**, where filename is the name of the IOS image file you recorded in Step 7.

20. All team members should configure their own routers, beginning with this step. Type **config-register 0x2100** and press **Enter**. Exit to enable mode.

21. Enter the **copy run start** command and confirm to save it as the default name.

22. Type **reload** and press **Enter**. Confirm if necessary.

23. When the router reloads, it will look to NVRAM for boot system commands. When it sees none, it will look at the configuration register. From where does the current configuration register tell the router to boot the IOS?

---

24. What does the ROM Monitor mode prompt look like?

---

---

25. The commands in ROM Monitor mode are generally not the same as the commands from the command EXEC you have been using thus far in the labs. At this point, you must change the configuration register back to the value you recorded in Step 7 so that the IOS will once again be loaded from flash memory. Type **confreg 0x2102**. If your configuration register setting in Step 7 is not 0x2102, substitute the register setting you recorded. Press **Enter**.

26. Type **reset** and press **Enter**.

27. At this point, the router should reload and the bootup procedure should appear as it has in previous labs. Enter the appropriate passwords to enter enable mode, then type **show version** and press **Enter**. Has the configuration register been reset to the default?

---

28. Log out of the router.

## Certification Objectives

Objectives for the CCNA exam:

- Access and utilize the router to set basic parameters (including CLI/SDM)
- Manage Cisco IOS

## Review Questions

1. What are two ways to control the boot procedure for loading the IOS?
2. What would happen during bootup if the configuration register were set to 0x2101?
3. Why might you want to use a series of boot system commands in your configuration?

---

## Lab 6.6 Investigate the Security Device Manager (SDM) Interface

### Objectives

Cisco's SDM is a Web-based tool designed to help network administrators configure the most complex tasks on a Cisco router. In order to become familiar with this new tool, you will download it from the Cisco website and install it on your computer. You will then install the SDM demo and become comfortable with the interface as well as basic functionality. You do not need connectivity to a router in order to learn about the SDM.

The objective of this lab is to become familiar with Cisco's Security Device Manager. You will download and install SDM, identify router interfaces and their status, change an interface IP address, observe the SDM reconfiguring the router in response to your IP address change, and test and monitor the Fast Ethernet interfaces.

After completing this lab you will:

- Be familiar with Cisco's SDM interface
- Understand the strengths and weaknesses of SDM

### Materials Required

This lab requires the following:

- A Windows computer with Internet access

### Activity

Estimated completion time: **60 minutes**

1. Boot the computer into Windows, and open a Web browser.
2. Although the SDM tools used in this lab are free, you will have to create a Cisco Connection Online (CCO) account to download them. If you already have a CCO account, skip to Step #3. Navigate to [www.cisco.com](http://www.cisco.com) in your browser and click on Register at the top right of the Web page. Fill in the form to create an account. Make sure you use a legitimate e-mail address because your new account must be activated from a link that will be sent to the address given. Click on the e-mail link to activate your account.

Lab 6.6 Investigate the Security Device Manager (SDM) Interface **543**

3. To install SDM on your computer, navigate to [www.cisco.com/pcgi-bin/tablebuild.pl/sdm](http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm). If this link has changed, search the Cisco webpage for SDM. Find the SDM-V232.zip file and click to download it. Note that this is not the latest version. As of the time of this writing, the latest version of SDM does not work with the demo software so make sure you get release version 2.3.2.
4. Click **Next** to verify the download, and then click **Accept** to accept the license agreement.
5. You will be prompted for credentials. You should use the username and password you just created, in other words, your CCO login information.
6. Save the file to the Desktop.
7. Double-click the file on the Desktop to open it. In the pane on the right, double-click **Setup** to install the SDM software. Click **Run** if you get a security warning, and accept all defaults to install SDM on your computer. Finish the installation wizard without launching SDM. Close the open window.
8. You will now download the SDM demo software. Navigate to [www.cisco.com/pcgi-bin/tablebuild.pl/sdm-tool-demo](http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm-tool-demo). If this link has expired, search the Cisco Web pages for “SDM demo.” At the time of this writing, the filename was SDM\_demo\_tool.zip and the release version was 2.3.2. Click on the file to download it.
9. Click **Next** to verify, then click **Accept** to accept the agreement, and begin the download. You may be asked again for your credentials. Use your new CCO username and password.
10. Save the file to the Desktop. Once the download is complete, double-click **SDM\_demo\_tool** to open it.
11. In the right pane, double-click the **PC\_setup\_instruction** file and read it. It should instruct you to copy dataFile.zip to the C:\ drive or whatever your main drive is designated. Close the instructions and copy the file now.
12. Return to your browser and disable all pop-ups. You will also need to enable ActiveX (content). You can enable active content or have the computer prompt you. Your settings may already be set to “prompt.”
13. Double-click the **Cisco SDM shortcut** on your Desktop to launch the software. Enter **127.0.0.1** as the device IP address and check the box to enable **HTTPS**. Click **Launch**.
14. Check the box to allow blocked content if necessary. Click **Run** if you get a security warning. Click **OK** when the Information window displays.
15. The demo should open. Notice the demo provides a fictional Cisco 2801 router with the hostname **2801Router** running version **12.4(6)T** of the IOS.
16. Click the double down arrows on the Interfaces and Connections pane to expand it. How many configured LAN interfaces are there? \_\_\_\_\_ What are the interface designations, their associated IP addresses, and corresponding subnet masks?  
\_\_\_\_\_
17. Click the **Configure** button at the top of the window. Notice the “How do I” area at the bottom of the window. Click **Go** to find out how to configure an unsupported WAN interface. Does the SDM support every possible interface on a Cisco router? \_\_\_\_\_ Close the Help window.

**544 Chapter 6 Router Startup and Configuration**

18. Click the **Edit Interface/Connection** tab and double-click the **FastEthernet0/0** interface to display the interface properties. Change the IP address to **10.77.158.80** and click **OK**. Notice the SDM warning window asking if you want the parameters affected by your IP address change to be modified also. Click **Yes**. Then click **OK** to close the Commands Delivery Status window.
19. With **FastEthernet0/0** still selected, click the **Test Connection** button in the upper-right corner and then click **Start**. An information window opens, telling you the connection has failed. Click **OK** to close the information window. What was the failure reason? \_\_\_\_\_ What is the recommended action?

---

Close the test connection window.

20. Click **FastEthernet0/1** to select it and click the **Test Connection** button. Click **Start**.
  21. Click **OK** to close the test failed information window. What are the failure reasons given?
- 

---

Close the test window.

22. Click the **Monitor** button. Are all of the Fast Ethernet interfaces up? \_\_\_\_\_ If not, which ones are down?

---

23. Close out your SDM session by closing all SDM associated windows.

## Certification Objectives

Objectives for the CCNA exam:

- Access and utilize the router to set basic parameters (including CLI/SDM)
- Connect, configure, and verify operation status of a device interface

## Review Questions

1. Can Cisco's SDM be used to configure everything on a router?
2. What did the SDM do in response to your changing an IP address, and why is this important?
3. The **show interfaces** CLI command will notify you if an interface is down. What additional information will the SDM give you regarding the down interface?

## C H A P T E R S E V E N

# ROUTING PROTOCOLS

## Labs included in this chapter

- Lab 7.1 Understand Terms and Concepts Related to Routing
- Lab 7.2 Configure Static Routes
- Lab 7.3 Configure RIP

## CCNA Exam Objectives

| Objective                                                                                                        | Lab      |
|------------------------------------------------------------------------------------------------------------------|----------|
| Describe basic routing concepts                                                                                  | 7.1      |
| Perform and verify routing configuration tasks for a static or default route given specific routing requirements | 7.2,     |
| Verify router hardware and software operation using <code>show</code> and <code>debug</code> commands            | 7.2, 7.3 |

## Lab 7.1 Understand Terms and Concepts Related to Routing

### Objectives

Your router needs a routing table to route packets correctly and efficiently. Routing is an extremely important topic, and an entire Cisco CCNP exam is devoted to it. At your current level, however, you only need to understand the basic concepts, terminology, and initial configuration commands involved with routing. Learning the concepts and terminology are the objectives of this lab. You will match the bulleted routing terms in the activity with the definitions in Table 7-1.

After completing this lab you will:

- Understand the terms and concepts related to routing

### Materials Required

This lab requires the following:

- Pencil or pen

### Activity

Estimated completion time: **45 minutes**

1. Relate the following bulleted terms to the descriptions in Table 7-1 by placing the terms in the correct cell in the second column. There may be more than one correct term or phrase for each description. Each term is used at least once.

- |                    |                           |                   |                     |
|--------------------|---------------------------|-------------------|---------------------|
| • Link-state       | • Split horizon           | • Distance-vector | • IPX               |
| • Metric           | • RIP                     | • Convergence     | • EIGRP             |
| • EGP              | • Direct connection       | • OSPF            | • Autonomous system |
| • Hold-down timers | • IGP                     | • IGRP            |                     |
| • BGP              | • Administrative distance | • NetBEUI         | • IP                |
| • Static route     |                           |                   |                     |

| Routing Concept Description                                                                                                                     | Matching Term |
|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Protocols that cannot be routed                                                                                                                 |               |
| Protocols that broadcast their entire routing tables periodically                                                                               |               |
| A type of route used in a stub situation or as a backup                                                                                         |               |
| The method a router uses to rank the reliability of routing information                                                                         |               |
| A group of routers that will share routing information and are under the control of one administrator                                           |               |
| Protocols that can be routed                                                                                                                    |               |
| Used to combat the count-to-infinity problem                                                                                                    |               |
| Protocols that, after the initial flooding of routing information, update neighbors at triggered intervals and consume relatively low bandwidth |               |
| A method of determining the suitability of a route                                                                                              |               |
| Routing protocols used within an autonomous system or private internetwork                                                                      |               |
| A state where all routers in the internetwork have a common view of the topology                                                                |               |
| Administrative distance of 100 or less                                                                                                          |               |
| Nonproprietary and commonly used routing protocol with a 15-hop limitation                                                                      |               |
| Routing protocols that can be used only between Cisco routers                                                                                   |               |
| Routing protocols used between autonomous systems or private internetworks                                                                      |               |

**Table 7-1** Routing concepts and terminology



7

## Certification Objectives

Objectives for the CCNA exam:

- Describe basic routing concepts

## Review Questions

1. A default route is a type of static route. What is it used for?
2. Rank IGRP, EIGRP, RIP, OSPF, static route, and direct connection in terms of administrative distance from lowest to highest. Record the administrative distance for each.
3. What is the difference between split horizon and split horizon with poison reverse?

## Lab 7.2 Configure Static Routes

### Objectives

The objective of this lab is to configure a static route on the router. To configure a router, you need to configure the interfaces and provide some way to find routes to other routers. The two methods for finding routes are (1) to let the routers update one another through dynamic routing protocols, and (2) to statically configure the routes using the `ip route` command. Static routes are often configured as a backup to dynamic routing. They are also used when the router is the last one in a chain of routers, in other words, a stub router. In a stub situation, there is no point using up bandwidth to advertise routes when there is only one way for packets to go.

In this lab you will configure the router for a static route to a remote network. In the process of configuring the router, you will also learn about the `show` commands that are useful for monitoring network routes.

After completing this lab you will:

- Understand the command syntax for configuring static routing
- Know how to check the router for routing table information
- Be familiar with the output from the `show ip route` command

### Materials Required

This lab requires the following:

- The internetworking lab setup shown in Figure 7-1
- The successful completion of the labs in Chapter 5

### Activity

Estimated completion time: **45 minutes**

1. Start the Windows computer and begin a HyperTerminal session with the router.
2. Turn on the router and hubs, if necessary. Press `Enter`, type the password `cisco` to get to the user EXEC mode prompt, type `enable`, and then press `Enter` to access privileged EXEC mode.
3. Type `class`, and then press `Enter` when prompted for the enable secret password.
4. Enter the `show interfaces` command and make sure the status of all the participating interfaces is up/up.
5. Type `show ip route`, and then press `Enter` to see the routing table information on the router. Which networks are directly connected to your router?

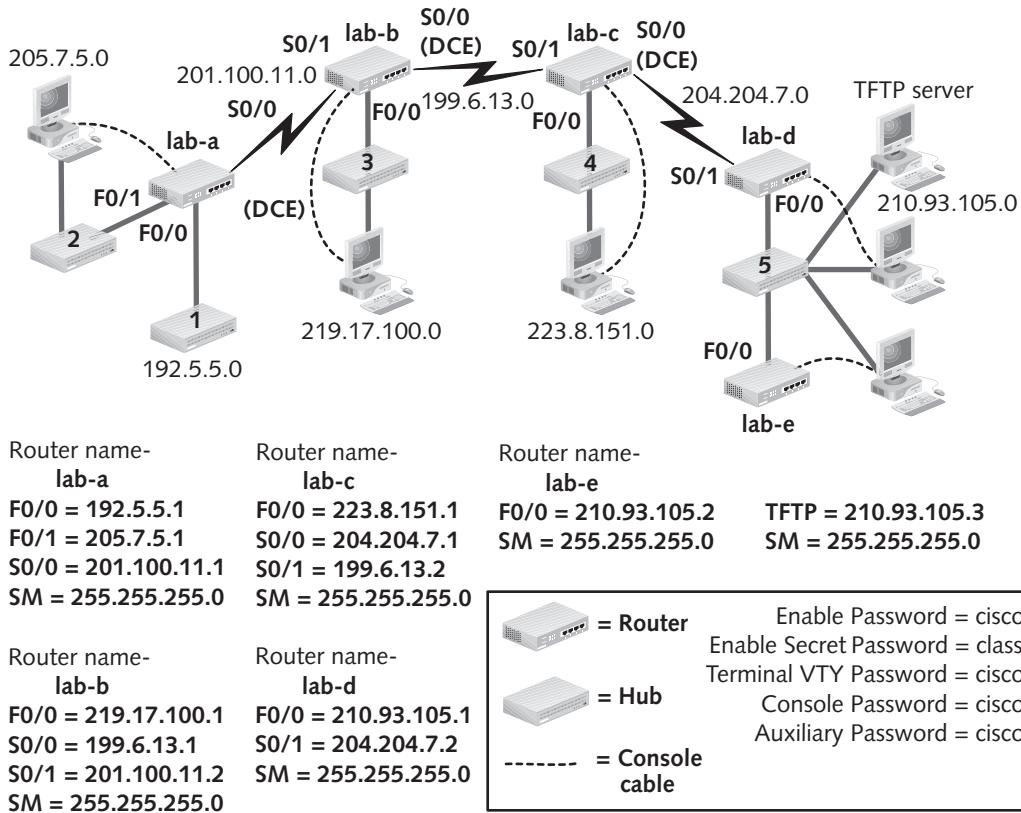
---

How do you know whether a network is directly connected?

---

Has your router discovered any networks through the RIP routing protocol?

---

**Figure 7-1** Connection information

How do you know whether your router has discovered a network through RIP?

6. To configure a static route on a router, you must know the destination network number, the subnet mask, and the IP address of the next router interface (hop) in the path to the destination network. Review the syntax for the `ip route` command, which is shown here:

```
ip route [remote network] [subnet mask] [IP address of interface on
next hop in the path] [administrative distance (optional)]
```

7. Examine the network in Figure 7-1 and the example command below. This command would configure a static route to network 205.7.5.0 from the lab-e router:

```
ip route 205.7.5.0 255.255.255.0 210.93.105.1 255
```

8. The last IP address in the command in Step 7 is the f0/0 interface on the lab-d router. It corresponds to the next hop on the path to the destination network. The 255 at the end of the command is the optional administrative distance. If you do not put an administrative distance in the command, what is the default?

9. Type `conf t`, and then press `Enter` to enter global configuration mode.

**550** Chapter 7 Routing Protocols

10. Use the **ip route** command to configure a static route on your router. Use an administrative distance of 255. Do not configure a static route to a network to which you are directly connected. Which router are you configuring?

---

For which network are you configuring a static route?

---

Which command did you enter?

---

11. Use the **ip route** command to configure another static route on your router to a different remote network. Use an administrative distance of 255.

For which network are you configuring a static route?

---

Which command did you enter?

---

12. Press **Ctrl+Z** to return to the enable prompt, and then press **Enter** to clear the message.

13. Type **show ip route**, and then press **Enter** to see the routing table information on the router. Do you see your static routes? Why not?
- 

14. Return to global configuration mode, and use the up arrow to find your static route commands. For each command, remove the administrative distance, but leave the remainder intact. Execute each of the commands again.

15. Press **Ctrl+Z** to return to the enable prompt, and then press **Enter** to clear the message.

16. Type **show ip route**, and then press **Enter** to see the routing table information on the router.

You should see your static routes. What is the symbol that lets you know these are static routes?

---

Why did removing the administrative distance of 255 from the static route commands change the routing table in this way?

---

17. Do not save the configuration. Type **logout**, and then press **Enter** to exit the router.

## Certification Objectives

Objectives for the CCNA exam:

- Perform and verify routing configuration tasks for a static or default route given specific routing requirements
- Verify router hardware and software operation using **show** and **debug** commands

## Review Questions

1. What is a stub router?
2. Why do you think the default administrative distance of a static route is only 1?
3. What is the purpose of changing the default administrative distance of a static route?
4. What is the only type of routing table entry that would have a default administrative distance less than the default administrative distance of a static route?

7

---

## Lab 7.3 Configure RIP

### Objectives

The objective of this lab is to demonstrate how to configure the router for RIP. RIP is the most common dynamic routing protocol in use on smaller internetworks because it is so easy to configure. In addition to configuring RIP, you will change the timer information, including the update interval. You will also use the show commands and a debug command for monitoring network routes.

After completing this lab you will:

- Understand the difference between dynamic routing and static routing
- Understand the command syntax for configuring RIP routing
- Be familiar with the output from the `show ip protocol`, `show ip route`, and `debug ip rip` commands

### Materials Required

This lab requires the following:

- The successful completion of the labs in Chapter 5
- The internetworking lab setup shown in Figure 7-1

### Activity

Estimated completion time: **45 minutes**

1. Start the computer with Windows and begin a HyperTerminal session with the router.
2. Turn on the router, if necessary. Press `Enter`, type the password `cisco` to get to the user EXEC mode prompt, type `enable`, and then press `Enter` to access privileged EXEC mode.

**552** Chapter 7 Routing Protocols

3. Type **class**, and then press **Enter** when prompted for the enable secret password.
  4. Enter global configuration mode.
  5. Remove RIP from the router using the **no router rip** command.
  6. Press **Ctrl+Z** to return to enable mode.
  7. Wait a few minutes for the RIP routes to be flushed from the router, or enter the **clear ip route** command to clear the routing table.
  8. Type **show ip route**, and then press **Enter**. Are all of your routes either directly connected or statically configured?
- 
- 

If the answer is “no” and RIP routes are still active, wait a few more seconds and try the **show ip route** command again. You should proceed to Step 9 only when you have confirmed that no RIP routes are active.

9. Enter global configuration mode.
  10. Type **router rip** to enter router configuration mode.
  11. Enter the networks to which your router is directly connected. Refer back to Figure 7-1, and use the **network** command to indicate which networks are directly connected to your router. For example, if you are configuring the lab-d router, you are directly connected to networks 204.204.7.0 and 210.93.105.0. In this case, you would type network 204.204.7.0 [Enter] and network 210.93.105.0 [Enter].
  12. Press **Ctrl+Z** to return to the enable prompt, press **Enter** to clear the message, and then wait a minute to give the router a chance to update its routing table.
  13. Type **show ip route**, and then press **Enter**. Has your router obtained any route information via RIP?
- 
14. Type **show ip protocol**, and then press **Enter**. What is the RIP update interval?
- 

What is the invalid interval?

---

What is the hold-down timer interval?

---

What is the flush interval?

---

15. Enter global configuration mode, then type **router rip** and press **Enter** to enter router configuration mode.
16. The **timers basic** command allows you to change the default timers you recorded in Step 14. Review the format of the following command:

```
timers basic [update interval] [invalid interval] [hold-down timer]
[flush interval]
```

17. Type **timers basic 60 500 360 440** and press Enter.
  18. Press Ctrl+Z to return to enable mode.
  19. Type **show ip protocol** and review the timer information. Have the timers been reconfigured, as shown by the commands in Step 17?
- 
20. Type **debug ip rip**, and then press Enter. Watch the screen for a minute or so to see the displayed information. What useful information can you obtain from this command?
- 
21. Press Enter if necessary to get to the prompt, and then type **no debug all** and press Enter to disable all debugging.
  22. Do not save the configuration. Type **logout**, and then press Enter to exit the router.

## Certification Objectives

Objectives for the CCNA exam:

7

- Verify router hardware and software operation using show and debug commands

## Review Questions

1. What is an advantage of increasing the update interval?
2. What is the purpose of the hold-down timer?
3. List three commands to turn off the debugging you configured using the **debug ip rip** command.
4. What is the purpose of the flush interval?



## C H A P T E R E I G H T

# ADVANCED ROUTING PROTOCOLS

## Labs included in this chapter

- Lab 8.1 Identify the Characteristics of Various Routing Protocols
- Lab 8.2 Configure RIPv2
- Lab 8.3 Configure EIGRP
- Lab 8.4 Configure OSPF in a Single Area

## CCNA Exam Objectives

| Objective                                                                   | Lab           |
|-----------------------------------------------------------------------------|---------------|
| Compare and contrast methods of routing and routing protocols               | 8.1           |
| Configure, verify, and troubleshoot RIPv2                                   | 8.2           |
| Troubleshoot routing issues                                                 | 8.2, 8.3, 8.4 |
| Verify router hardware and software operation using show and debug commands | 8.2, 8.3, 8.4 |
| Configure, verify, and troubleshoot EIGRP                                   | 8.3           |
| Configure, verify, and troubleshoot OSPF                                    | 8.4           |

## Lab 8.1 Identify the Characteristics of Various Routing Protocols

### Objectives

A CCNA must understand RIP, RIPv2, EIGRP, and OSPF. The objective of this lab is to help you learn how to identify the characteristics of RIP, RIPv2, EIGRP, and OSPF.

After completing this lab, you will be able to:

- Identify basic characteristics of RIP, RIPv2, EIGRP, and OSPF

### Materials Required

This lab requires the following:

- A pen or pencil

### Activity

Estimated completion time: **20 minutes**

- Fill in the Routing Protocol column of Table 8-1 with the protocol(s) being described. Possible answers are RIP, RIPv2, EIGRP, and OSPF. Note that more than one routing protocol might be appropriate for a characteristic.

| Characteristic                              | Routing Protocol |
|---------------------------------------------|------------------|
| Broadcasts periodically                     |                  |
| Uses multicasting                           |                  |
| Uses multicast address 224.0.0.10           |                  |
| Uses multicast address 224.0.0.9            |                  |
| Uses multicast address 224.0.0.5            |                  |
| May elect a DR                              |                  |
| Uses LSAs                                   |                  |
| Is actually a hybrid routing protocol       |                  |
| Limited to 15 hops                          |                  |
| Cisco proprietary                           |                  |
| Auto-summarizes at major network boundaries |                  |
| Calculates a feasible successor             |                  |
| Uses the Dijkstra algorithm                 |                  |
| Uses the DUAL algorithm                     |                  |

**Table 8-1** Routing protocol characteristics (*Continued*)

| Characteristic                                                    | Routing Protocol |
|-------------------------------------------------------------------|------------------|
| Classful                                                          |                  |
| Classless                                                         |                  |
| Has the ability to authenticate                                   |                  |
| Uses PDMs to support multiple protocols such as IPX and AppleTalk |                  |
| Uses Hello packets to establish adjacencies                       |                  |
| Open standard                                                     |                  |
| Uses cost as its only metric                                      |                  |

## Certification Objectives

Objectives for the CCNA exam:

- Compare and contrast methods of routing and routing protocols


 8

## Review Questions

1. What can classless routing protocols do that classful routing protocols cannot?
2. What is an advantage of OSPF over EIGRP?
3. What is an advantage of EIGRP over OSPF?
4. Why might you have to turn off the auto-summarization feature?
5. Why is multicasting rather than broadcasting generally preferred for routing updates?

---

## Lab 8.2 Configure RIPv2

### Objectives

RIPv2 is a classless routing protocol, which means it can carry subnet masking information in its routing updates. RIPv2 configuration is only slightly more complicated than configuring basic RIP. The objective of this lab is to configure RIPv2 and compare it with the RIP you configured in Chapter 7. In addition, you will configure a router interface to

**558** Chapter 8 Advanced Routing Protocols

be passive. Passive interfaces listen for updates from other routers but do not send routing updates.

After completing this lab, you will be able to:

- Configure RIPv2
- Configure passive interfaces
- Monitor RIPv2

## Materials Required

This lab requires the following:

- The internetworking lab setup used in the labs in Chapters 5, 6, and 7
- The successful completion of the labs in Chapter 5 as well as Lab 6.1

## Activity

Estimated completion time: **30 minutes**

1. If necessary, turn on the workstations.
2. Open the HyperTerminal program on each workstation that will connect to the routers.
3. If necessary, turn on the routers and hubs.
4. Press **Enter** on the workstations if you need to initiate a response from the router.
5. Enter enable mode using **cisco** as the console password and **class** as the enable password.
6. Enter global configuration mode.
7. Type **router rip**, and then press **Enter**.
8. Type **version 2** to change from basic RIP to RIPv2, and then press **Enter**.
9. Enter the networks to which your router is directly connected. Refer to Figure 8-1 and use the **network** command to indicate which networks are directly connected to your router. For example, if you are configuring the lab-d router, you are directly connected to networks 204.204.7.0 and 210.93.105.0. In this case, you would type:  

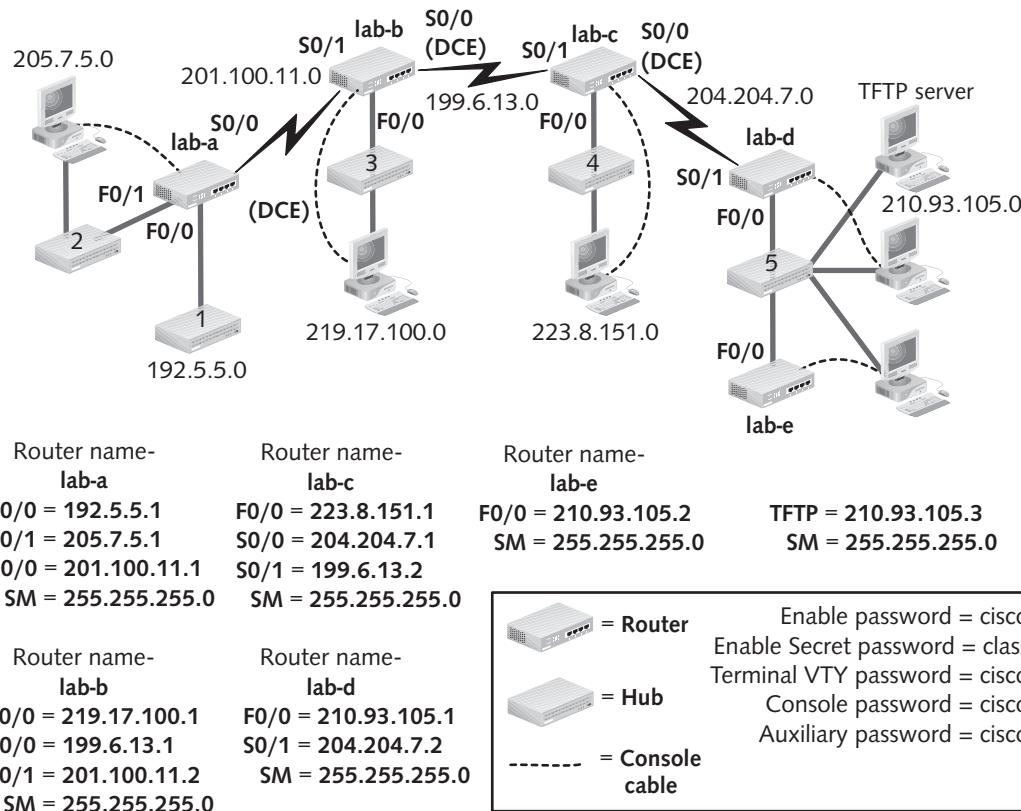
```
network 204.204.7.0 [Enter]
network 210.93.105.0 [Enter]
```
10. Press **Ctrl+Z** to return to enable mode.
11. Enter the **show ip protocols** command. Which routing protocol is listed?

Which version of RIP updates is being sent and received?

---

What is the update interval?

---

**Figure 8-1** Connection information

What is the invalid interval?

---

What is the hold-down timer interval?

---

What is the flush interval?

---

Are these default intervals the same or different from the ones recorded for RIP version 1 in Lab 7.3, Step 14?

---

12. Type **show ip route** and press Enter. Can you tell by this command output which RIP version is running?

---

13. What is the administrative distance of RIPv2?

---

**560** Chapter 8 Advanced Routing Protocols

14. Type **debug ip rip** and press **Enter**. Wait for the output to display. Is RIPv2 sending and receiving updates to routers on all active interfaces?

---

If not, make sure RIPv2 is correctly configured on the routers.

15. Type **undebbug all** and press **Enter**.
16. Enter global configuration mode.
17. Type **router rip** and press **Enter** to enter router configuration mode.
18. Type **passive-interface s[#]**, where [#] is an active serial interface on your router. The lab-e router has no active serial interfaces and should use f0/0. Which interface have you made active?

- 
19. Press **Ctrl+Z** to exit to enable mode.
  20. Type **debug ip rip** and press **Enter**. Are you sending updates out of the passive interface you listed in Step 18?

If you are, you have incorrectly configured the passive interface.

21. Type **undebbug all** and press **Enter** to disable all debugging.
22. Enter global configuration mode.
23. Type **router rip** and press **Enter**.
24. Use the **no passive-interface** command with the correct interface to reestablish normal routing updates in and out of all active router interfaces.
25. Log out of the router without saving your configuration.

## Certification Objectives

Objectives for the CCNA exam:

- Configure, verify, and troubleshoot RIPv2
- Verify router hardware and software operation using show and debug commands
- Troubleshoot routing issues

## Review Questions

1. What command tells the router to listen for and advertise RIPv2 instead of RIPv1?
2. What is the advantage of RIPv2 over RIPv1?
3. What is the disadvantage of RIPv2?

4. What command tells an interface on a router to listen for but not send routing updates?
5. RIPv1 and RIPv2 default timers are identical. True or False?

---

## Lab 8.3 Configure EIGRP

### Objectives

EIGRP is based on distance-vector technology but is really a hybrid routing protocol because it also includes elements of link-state routing. Like most distance-vector routing protocols, EIGRP only needs to know about directly connected routers; in other words, neighbors. EIGRP uses the DUAL algorithm to calculate the best route to a destination. The objective of this lab is to configure and monitor EIGRP. In addition, you will disrupt the topology and watch as EIGRP runs DUAL in an attempt to find alternative routes.

After completing this lab, you will be able to:

- Configure EIGRP
- Monitor EIGRP



### Materials Required

This lab requires the following:

- The internetworking lab setup used in the labs in Chapters 5, 6, and 7
- The successful completion of the labs in Chapter 5 and Lab 6.1

### Activity

Estimated completion time: **30 minutes**

1. If necessary, turn on the workstations.
2. Open the HyperTerminal program on each workstation that will connect to the routers.
3. If necessary, turn on the routers and hubs.
4. Press **Enter** on the workstations if you need to initiate a response from the router.
5. Enter enable mode using **cisco** as the console password and **class** as the enable password.
6. Enter global configuration mode.
7. Type **router eigrp 65000** and press **Enter**.
8. Enter the networks to which your router is directly connected. Refer to Figure 8-1 and use the **network** command to indicate which networks are directly connected to your router. For example, if you are configuring the lab-d router, you are directly connected to networks 204.204.7.0 and 210.93.105.0. In this case, you would type:

**network 204.204.7.0 [Enter]**

**network 210.93.105.0 [Enter]**

**562** Chapter 8 Advanced Routing Protocols

9. Press **Ctrl+Z** to exit to enable mode.
10. Type **show ip route**. What is the letter code for EIGRP routes?

---

What is the administrative distance of EIGRP?

---

11. Type **show ip protocols** and press **Enter**. Does EIGRP auto-summarize by default?

12. Type **show ip eigrp topology** and press **Enter**. What does this output display?

---

How many entries are there in the table?

---

13. Type **debug ip eigrp** and press **Enter**. Nothing will display if the network is stable. Now you will make the network unstable by shutting down an interface.
14. Type **conf t** and press **Enter** to change to global configuration mode.
15. Type **int s[#]**, where [#] is an active interface on your router that is connected to another active router interface. If you are configuring the lab-e router, you will need to use f0/0 as your interface. Press **Enter**.
16. Type **shutdown** and press **Enter**. Debug output is immediately displayed on all connected routers as they attempt to find alternate paths.
17. Press **Ctrl+Z** to return to enable mode.
18. Type **show ip eigrp topology** and press **Enter**. How many successors are now in the table?

---

Compare this with your answer recorded in Step 12.

---

19. Enter global configuration mode.
20. Type **int s[#]** (or **int f0/0** if you are configuring the lab-e router) and press **Enter**.
21. Type **no shutdown** and press **Enter**.
22. Press **Ctrl+Z** and press **Enter**.
23. Type **show ip eigrp topology** and press **Enter**. You should have the same number of entries in the table now as you did in Step 12.
24. Type **show ip route** and press **Enter**. All successors should be in your routing table.
25. Type **undebbug all** and press **Enter** to disable all debugging.
26. Type **logout** and press **Enter**. Do not copy this configuration to NVRAM.

## Certification Objectives

Objectives for the CCNA exam:

- Configure, verify, and troubleshoot EIGRP
- Troubleshoot routing issues
- Verify router hardware and software operation using show and debug commands

## Review Questions

1. Why did you not need the no auto-summary command in this lab?
2. What is in the EIGRP topology table?
3. EIGRP is a hybrid routing protocol based on link-state technology. True or False?

8

---

## Lab 8.4 Configure OSPF in a Single Area

### Objectives

OSPF is a link-state routing protocol that is more complicated to configure than the routing protocols you have previously worked with in the labs. The CCNA exam requires you to know the basics about configuring OSPF in a single area. The objective of this lab is to configure and monitor OSPF for a broadcast multiaccess network. In addition, you will learn how to force a particular OSPF router to become the designated router. Finally, you will configure the OSPF routers for MD5 authentication.

After completing this lab, you will be able to:

- Configure OSPF
- Monitor OSPF
- Understand the DR/BDR process
- Know how to configure MD5 authentication on OSPF routers

### Materials Required

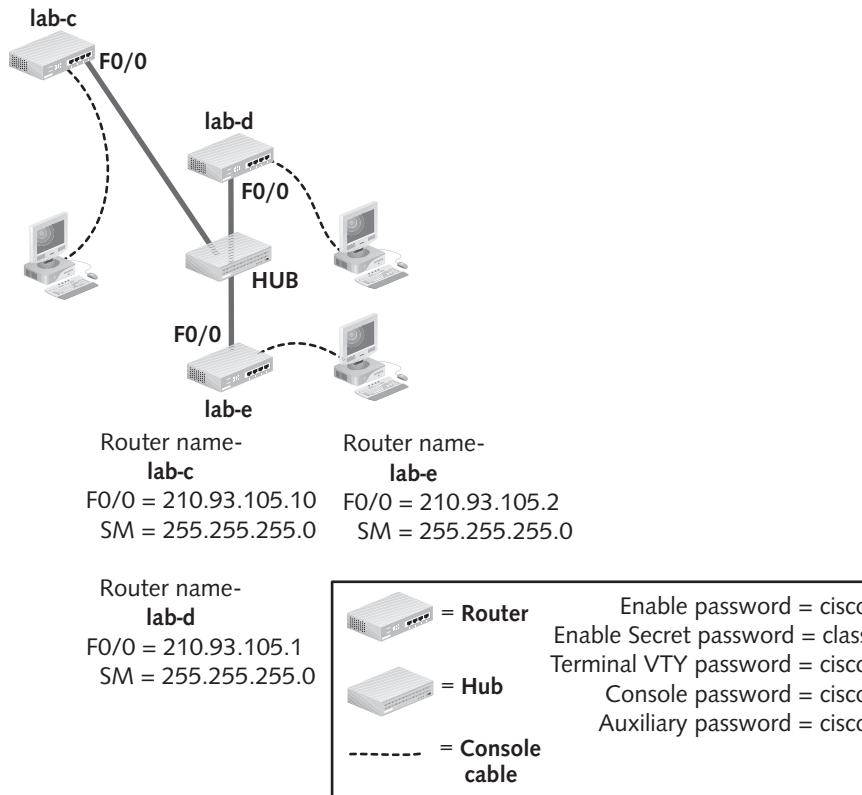
This lab requires the following:

- The internetworking lab setup used in the labs in Chapters 5, 6, and 7
- The successful completion of the labs in Chapter 5 and Lab 6.1

## Activity

Estimated completion time: **45 minutes**

1. Turn off all routers and hubs.
2. Using Figure 8-1 for reference, disconnect the serial cable between the lab-b and lab-c routers. Using Figure 8-2 for reference, disconnect the serial cable between the lab-c and lab-d routers.



**Figure 8-2** OSPF lab setup

3. Move the UTP cable from the lab-c router's hub to the hub shared by the lab-d and lab-e routers.
4. Turn on the lab-c, lab-d, and lab-e routers and the hub they share. Leave the rest of the lab equipment turned off.
5. Begin a HyperTerminal session with the routers.
6. Press **Enter** on the workstations if you need to initiate a response from the router.
7. Enter enable mode using **cisco** as the console password and **class** as the enable password.

8. On the lab-c router only, you need to change the IP address on the Fast Ethernet interface. Using Figure 8-2 as a reference, change the IP address on the f0/0 interface of the lab-c router to 210.93.105.10.
9. Make sure the routers can ping each other before continuing. The following steps apply to all routers unless otherwise mentioned.
10. Enter global configuration mode.
11. Type **router ospf 1** and press Enter.
12. Type **network 210.93.105.0 0.0.0.255 area 0** and press Enter. Return to enable mode using **Ctrl+Z**.
13. Type **show ip ospf** and press Enter. What is your router ID?

---

How many times has the SPF algorithm run?

---

14. Type **show ip ospf database** and press Enter. All three participating OSPF interfaces should be listed under Router Link States.
15. Type **show ip ospf interface** and press Enter. What is the cost associated with this interface?



8

---

Which router is the designated router (DR)?

---

---

Which router is the backup designated router (BDR)?

---

---

What is the default priority?

---

16. Type **debug ip ospf events** and press Enter. No output will be produced other than hello packet processing if the network is stable. You will now destabilize the network and watch the SPF algorithm in action.
17. On the lab-c router only, disconnect the UTP from the Fast Ethernet interface. Watch and wait as the debug output displays OSPF adjusting to the new network topology. Eventually, you should see a new DR/BDR election take place. Which router is the new DR?

---

Which router is the new BDR?

---

18. Plug the UTP cable back into the Fast Ethernet interface on the lab-c router and watch the debug output. Do you think this process will restore lab-c as the DR and lab-e as the BDR?
19. On all routers, type **undebbug all** and press Enter to disable all debugging.

**566** Chapter 8 Advanced Routing Protocols

20. Enter the **show ip ospf int** command.

Which router is the DR?

---

Which router is the BDR?

---

21. Enter the following commands on the lab-d router only:

```
conf t  
int f0/0  
ip ospf priority 100
```

Press Ctrl+Z

22. Turn on debugging on all three routers using the **debug ip ospf events** command.

23. Unplug all UTP from the hub and wait for 30 seconds before plugging the cables back in. This should force a flooding and a new election. Watch the election process.

24. Turn debugging off of all routers.

25. Enter the **show ip ospf int** command.

Which router is the DR?

---

Which router is the BDR?

---

Why did the router with the lowest IP become the DR?

---

26. OSPF routers support plain text authentication as well as MD5 authentication. If you choose to use authentication, you must configure an entire area with the same authentication. Authentication is configured in interface configuration mode and also in router configuration mode. Enter the following commands on all three routers to configure MD5 authentication:

```
conf t  
int f0/0  
ip ospf message-digest-key 1 md5 cannonball  
exit  
router ospf 1  
area 0 authentication message-digest
```

Press Ctrl+Z

27. Enter the **show ip ospf int** command to verify that MD5 authentication has been configured on the router.

28. Enter the **debug ip ospf adj** command to watch the authentication process. Notice that a key must be sent with the hello packets when MD5 authentication is configured.

29. Enter the **undebbug all** command to turn off all debugging.
30. Log out out of the routers. Do not save the configuration in NVRAM.

## Certification Objectives

Objectives for the CCNA exam:

- Troubleshoot routing issues
- Verify router hardware and software operation using show and debug commands
- Configure, verify, and troubleshoot OSPF

## Review Questions

1. What extra parameters are necessary in the **network** command when using OSPF, as compared with RIP, RIPv2, and EIGRP?
2. What is the purpose of areas in OSPF?
3. What is the purpose of the DR?
4. What determines which router will be the DR?
5. What are the two steps involved when configuring OSPF authentication?



## C H A P T E R N I N E

# NETWORK SERVICES

## Labs included in this chapter

- Lab 9.1 Configure NAT
- Lab 9.2 Configure DHCP
- Lab 9.3 Use SDM to configure NAT, DHCP, and DNS

## CCNA Exam Objectives

| Objective                                                              | Lab      |
|------------------------------------------------------------------------|----------|
| Explain the basic operation of NAT                                     | 9.1      |
| Configure NAT for given network requirements                           | 9.1, 9.3 |
| Explain the operation and benefits of using DHCP and DNS               | 9.2      |
| Configure, verify, and troubleshoot DHCP and DNS operation on a router | 9.2, 9.3 |

## Lab 9.1 Configure NAT

### Objectives

The objective of this lab is to configure the router for Network Address Translation (NAT). NAT was developed by Cisco and is useful for conserving IP address space as well as managing and hiding your internal IP scheme. NAT is available in many formats. In this lab, you will learn how to configure static NAT, dynamic NAT, and Port Address Translation (PAT). Static NAT is a mapping of one inside IP address to one outside IP address. It does not conserve IP address space. Dynamic NAT also maps one inside address to one outside address but the outside addresses come from a pool, so the router does not track which outside address is assigned to a particular inside address. PAT maps multiple inside IP addresses to a single outside address; it also keeps track of the different IP addresses using random port numbers so that no computer has the same socket as any other. In this lab, you will configure the router for the three flavors of NAT described above. You will also use the `show ip nat statistics` command used to monitor NAT on routers.

After completing this lab you will:

- Understand the difference between static NAT, dynamic NAT, and PAT
- Understand the command syntax for configuring static NAT, dynamic NAT, and PAT
- Know how to check the router for NAT

### Materials Required

This lab requires the following:

- The successful completion of the labs in Chapter 5

### Activity

Estimated completion time: **45 minutes**

1. Start the Windows computer and begin a HyperTerminal session with the router.
2. Press **Enter** and type the password **cisco** to get to the user EXEC mode prompt, type **enable**, and then press **Enter** to access privileged EXEC mode.
3. Type **class**, and then press **Enter** when prompted for the enable secret password.
4. Enter global configuration mode.
5. To configure static NAT on the router you must define the mapping of an inside address to an outside address. Type **ip nat inside source static 192.168.100.1 200.200.200.1**, and then press **Enter**. What specifically does this command tell the router to do?
6. Next you must define the inside and the outside. Type **int f0/0**, and then press **Enter** to enter interface configuration mode.
7. Type **ip nat inside** and press **Enter**. What specifically did the commands in Steps 6 and 7 tell the router?

8. On your own, enter the two commands to configure the s0/0 interface as the outside. What two commands did you enter?

---

9. Press **Ctrl+Z**, then type **show run** and press **Enter**. The running configuration should indicate that static NAT has been configured on the router.

10. Type **reload** and press **Enter**. Do not save your configuration. Confirm the reload and wait for the router to reboot without static NAT configured.

11. To configure dynamic NAT on the router, you must begin by configuring an access list to define a group of inside addresses. Access lists are covered in detail in Chapter 10. Enter the following command at the global configuration mode prompt:

```
access-list 1 permit 192.168.100.0 0.0.0.255
```

This command tells the router to allow all IP addresses on the 192.168.100.0 network to be associated with access list number 1.

12. Next, enter the following two commands to define the outside pool of addresses named cannon and link the cannon pool to the access list you created in Step 11.

```
ip nat pool cannon 200.200.200.1 200.200.200.100 netmask  
255.255.255.0
```

```
ip nat inside source list 1 pool cannon
```

9

13. On your own, enter the four commands to define the inside and outside. *Hint:* See Steps 6, 7, and 8.

14. Press **Ctrl+Z**, then enter the **show run** command to see if you have configured dynamic NAT on the router.

15. Enter the **show ip nat statistics** command. What type of information does this command display?

---

16. Type **reload** and press **Enter**. Do not save your configuration. Confirm the reload and wait for the router to reboot without dynamic NAT configured.

17. To configure PAT you begin as you did with dynamic NAT by creating an access list to define the inside addresses. Type the following command at the global configuration mode prompt:

```
access-list 1 permit 192.168.100.0 0.0.0.255
```

18. Next, you must tell the router to take every inside address defined by the access list and map it to a single address, specifically the address associated with the serial interface. To do this, enter the following command:

```
ip nat inside source list 1 interface s0/0 overload
```

19. On your own, enter the four commands to define the inside and outside.

20. Press **Ctrl+Z**, then enter the **show run** command to see if you have configured PAT on the router.

21. Turn off the router without saving the configuration.

## Certification Objectives

Objectives for the CCNA exam:

- Configure NAT for given network requirements
- Explain the basic operation of NAT

## Review Questions

1. Does static NAT conserve IP addresses? Why or why not?
2. Does PAT conserve IP addresses? Why or why not?
3. Why do dynamic NAT and PAT require configuration of an access list?
4. What is the purpose of the address pool in dynamic NAT?
5. Give three reasons for using NAT.

---

## Lab 9.2 Configure DHCP

### Objectives

Very often a Dynamic Host Configuration Protocol (DHCP) server provides the IP configuration information to the clients when they bootup. However, other devices, such as routers, can be configured to provide DHCP functionality also. The benefit of using a router rather than a computer as a DHCP server is that one router can provide configuration information for multiple subnets. The objective of this lab is to configure a router to be a DHCP server. This will allow hosts to obtain their IP configuration automatically from the router. In this lab, you will learn how to configure DHCP on a Cisco router using the command-line interface. Your configuration will allow the router to provide an IP configuration to the computer connected to the hub or switch off of the F0/0 interface. Finally, you will verify your configuration using various show commands associated with DHCP.

After completing this lab you will:

- Understand how to configure your router to be a DHCP server
- Know how to check the router for successful DHCP functionality

### Materials Required

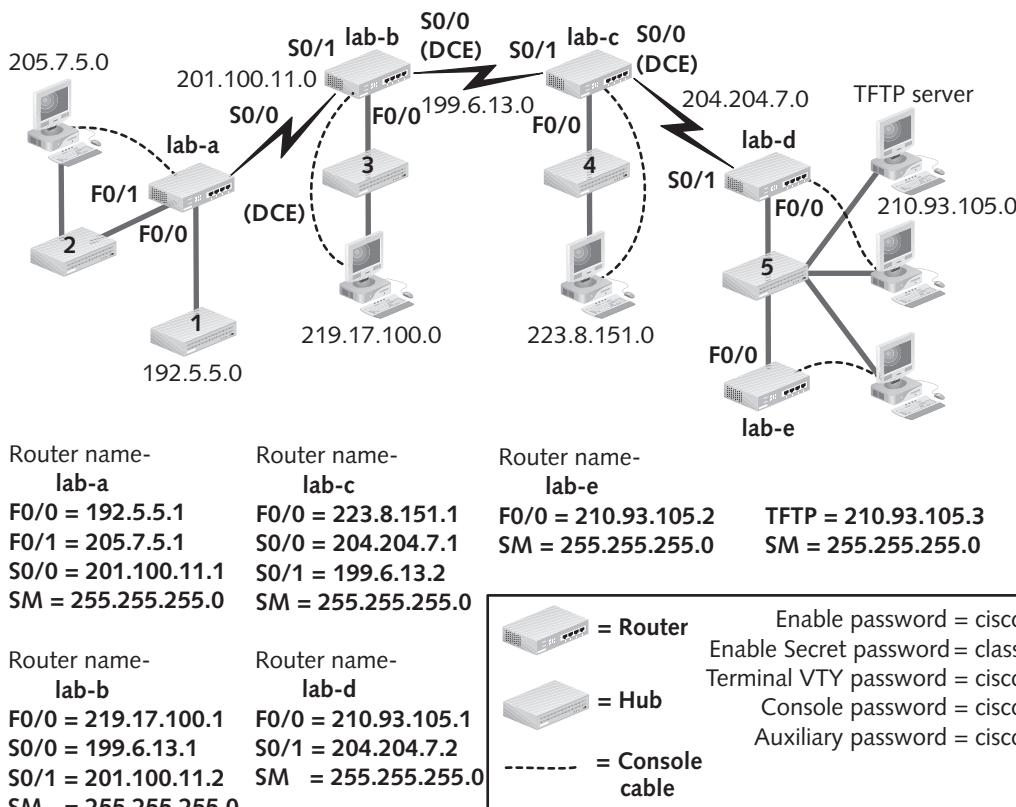
This lab requires the following:

- The successful completion of the labs in Chapters 5 and 6
- Five patch cables

## Activity

Estimated completion time: **30 minutes**

1. Start the Windows computer and begin a HyperTerminal session with the router.
2. Press **Enter** and type the password **cisco** to get to the user EXEC mode prompt, type **enable**, and then press **Enter** to access privileged EXEC mode.
3. Type **class**, and then press **Enter** when prompted for the enable secret password.
4. Enter global configuration mode. Refer to Figure 9-1 before continuing with the lab. Your commands will be specific to the router you are configuring. Note that the lab-d and lab-e router are on the same network, so the lab-e router should not be configured for DHCP.



**Figure 9-1** Connection information

5. Enter the **ip dhcp pool [routername]** command on the router. Substitute the correct name of your router for the routername. For example, if you are configuring the lab-a router, the command would be **ip dhcp pool lab-a**. What does this command do?

How did the prompt change? \_\_\_\_\_

**574 Chapter 9 Network Services**

6. Enter the **network [network number] [subnet mask]** command using the network defined by your router's F0/0 interface. For example, if you are configuring the lab-a router, the command would be **network 192.5.5.0 255.255.255.0**. Refer to Figure 9-1 for this information. What does this command do?

---

7. Enter the **default-router [F0/0 interface IP address]** command substituting the IP address on the F0/0 interface on the router you are configuring. For example, the command on the lab-a router would be **default-router 192.5.5.1**. What important information will this provide to the client computers on this network?

---

8. Enter the **domain-name cannon** command.
9. Enter the **dns-server 210.93.105.3** command. What will this command do?

---

10. Enter the **netbios-name-server 210.93.105.3** command. What will this command do?

---

11. Enter the **ip dhcp excluded-address [F0/0 interface IP address] 210.93.105.3** command substituting the IP address on the F0/0 interface on the router you are configuring. Why should you exclude these two addresses from the DHCP pool?

---

12. Press **Ctrl+Z** to return to the privileged EXEC mode prompt.
13. Make sure your computer is configured to obtain its IP configuration information automatically. Do this by checking the properties of the connection. In Windows Vista, click the **Start** button, right-click **Network** and then click **Properties**. In the left pane, click **Manage network connections**. Right-click your **Local Area Connection** and click **Properties**. Double-click **Internet Protocol Version 4**. Select **Obtain an IP address automatically** if it is not already selected. Click **OK** twice, then close the open windows. If you are using Windows XP, these steps will be slightly different.
14. Connect a patch cable from your computer to the hub or switch connected to your router's F0/0 interface.
15. Click the **Start** button on your computer, enter the **cmd** command, and press **Enter** to reach the command line interface on the computer. Enter the **ipconfig /release** command to drop any IP configuration information. Enter the **ipconfig /renew** command to broadcast a request for IP configuration information from a DHCP server. You could also reboot the computer to obtain new IP configuration information.
16. At the computer's command-line interface, enter the **ipconfig /all** command. What is the IP address, subnet mask, and default gateway assigned to the Ethernet adapter?

---

17. What is the DNS and WINS server address?

---

18. When does the DHCP lease expire? \_\_\_\_\_

19. Return to the HyperTerminal connection on the router.
20. Enter the `show ip dhcp binding` command. If you configured DHCP correctly, your computer's new IP address and associated MAC address should display in the table.
21. Enter the `show ip dhcp pool` command. How many total addresses are available in the pool? \_\_\_\_\_ . How many addresses have been leased?  
\_\_\_\_\_
22. Turn off the router without saving the configuration.

## Certification Objectives

Objectives for the CCNA exam:

- Explain the operation and benefits of using DHCP and DNS
- Configure, verify, and troubleshoot DHCP and DNS operation on a router

## Review Questions

1. What is the benefit of using DHCP?
2. What is the benefit of configuring a router to be the DHCP server rather than a computer? **9**
3. DHCP functionality requires that both the server and the client be configured for DHCP.  
True or False?
4. List three addresses you would typically exclude from a DHCP pool.

---

## Lab 9.3 Use SDM to Configure NAT, DHCP, and DNS

### Objectives

Cisco's Security Device Manager (SDM) is a Web-based tool used for advanced configuration of Cisco routers. As you learned in Chapter 9, SDM can also be used to configure NAT, DHCP, and DNS, although this is typically only done when SDM is already being used to configure other more difficult parameters. The purpose of this lab is to further familiarize you with the SDM interface and to configure NAT, DHCP, and DNS using SDM. You do not need to install SDM on your routers. You will complete this lab using the SDM simulator you installed in Lab 6.6.

After completing this lab you will:

- Be familiar with Cisco's SDM interface
- Understand how to configure NAT, DHCP, and DNS on a router using the Cisco SDM

## Materials Required

This lab requires the following:

- Completion of Lab 6.6

## Activity

Estimated completion time: **45 minutes**

1. Boot the computer into Windows.
2. Double-click the **Cisco SDM shortcut** on your Desktop to launch the software. Enter **127.0.0.1** as the device IP address and click to enable **HTTPS**. Click **Launch**.
3. Click to allow blocked content if necessary. Click **Run** if you get a security warning. Click **OK** when the Information window displays.
4. The demo should open. Notice the demo provides a fictional Cisco 2801 router with the hostname **2801Router** running version **12.4(6)T** of the IOS.
5. Click the **Configure** button and then click the **NAT** button in the left pane.
6. Make sure the Basic NAT radio button is selected.
7. Click the **Edit NAT Configuration** tab, then click the **Delete** button to delete the current NAT configuration. Click **OK** and then click **OK** again to save the changes.
8. Click **Add** to begin creating a new NAT configuration. Make sure the **Static** radio button is selected. The **Direction** text box should indicate **From inside to outside**. This is the default. Enter this IP address: **192.168.100.1**. Leave the **Network Mask (Optional)**: text box blank.
9. Enter this outside IP address: **200.200.200.1**. Click **OK**, click **Yes** on the warning dialog box, and then click **OK** to save the changes. You should see your original address, the translated address, and the word **static** as the **Rule Type**. If so, you have created a static NAT mapping.
10. You will now create a dynamic NAT configuration. Click **Add** to open the Add Address Translation Rule dialog box. Select **Dynamic**. The **Direction** text box should indicate **From inside to outside**.
11. Click the button beside the **ACL Rule** text box and select **Create a new rule (ACL)** and select from the dropdown list box.
12. Enter **10** in the **Name/Number** text box and select **Standard Rule** as the **Type**.
13. In the **Description** text box enter **Inside addresses for translation**. Click **Add**.
14. Select **Permit** as the **Action** and select **A Network** as the **Type**.
15. Enter **192.168.100.0** in the **IP Address** text box and select **0.0.0.255** in the **Wildcard Mask** dropdown list box.
16. Click **OK**, then click **OK** again to save the ACL rule.
17. The **ACL Rule** text box should indicate number **10**. Change the **Type** to **Address Pool**.
18. Click the button beside the **Address Pool** text box and click **Create a new NAT Pool and Select**.
19. Type **RouterA** in the **Pool Name** text box. The **PAT** check box should be unchecked.
20. Define the outside pool of addresses by typing **200.200.200.1** in the first **IP address** text box and **200.200.200.100** in the second **IP address** text box. Enter this mask: **255.255.255.0**. Click **OK**, then click **OK** in the **Add Address Translation Rule** box, click **No**, and then

click **OK** to save the pool configuration. The address pool as well as the translation address pool should display along with the word Dynamic to indicate the NAT type.

21. Configuring PAT is very similar to configuring Dynamic NAT. The only difference is that the inside pool of addresses defined by the ACL rule all map to a single outside address. To change your dynamic NAT configuration to PAT, select it and click **Edit**.
22. Change the Type from Address Pool to Interface.
23. Change the Interface to **FastEthernet0/1** and click **OK**, click **Yes**, then click **OK** to save the configuration.
24. To configure the router to be a DHCP server using SDM, click the **Additional Tasks** button in the left pane of the SDM simulator.
25. Click the plus sign to the left of **DHCP**, then click **DHCP Pools**.
26. Click **Add** to begin configuring DHCP.
27. Enter **RouterA** in the DHCP Pool Name text box.
28. Enter **192.168.100.0** as the DHCP Pool Network and **255.255.255.0** as the subnet mask.
29. Enter **192.168.100.4** in the Starting IP text box and **192.168.100.254** in the Ending IP text box.
30. Configure the DNS Server1 and WINS Server1 with the IP address **192.168.100.2**.
31. Configure the DNS Server2 and WINS Server2 with the IP address **192.168.100.3**.
32. Enter the Domain Name as **cannon.com** and configure the Default Router as **192.168.100.1**. Click **OK**, then click **OK** again to save the configuration. Your DHCP configuration should display.
33. Close all SDM windows to end your session with the SDM simulator.

9

## Certification Objectives

Objectives for the CCNA exam:

- Configure NAT for given network requirements
- Configure, verify, and troubleshoot DHCP and DNS operation on a router

## Review Questions

1. When might you decide to use SDM to configure NAT, DHCP, and DNS?
2. What is the only difference between configuring dynamic NAT and configuring PAT?
3. What is your opinion regarding using the SDM for configuring NAT?
4. What is your opinion regarding using the SDM for configuring DHCP?



## C H A P T E R T E N

# ACCESS LISTS

## Labs included in this chapter

- Lab 10.1 Create and Apply a Standard IP Access List on the Lab-d Router
- Lab 10.2 Create and Apply an Extended IP Access List on the Lab-b Router
- Lab 10.3 Create and Apply a Named Access List on the Lab-c Router

## CCNA Exam Objectives

| Objective                                                        | Lab              |
|------------------------------------------------------------------|------------------|
| Describe the purpose and types of ACLs                           | 10.1, 10.2, 10.3 |
| Configure and apply ACLs based on network filtering requirements | 10.1, 10.2, 10.3 |
| Verify and monitor ACLs in a network environment                 | 10.1, 10.2, 10.3 |

## Lab 10.1 Create and Apply a Standard IP Access List on the Lab-d Router

### Objectives

The objective of this lab is to configure a standard IP access list, which filters traffic based on source IP addresses. This process is carried out in two steps. First, the list is created using a text editor and configured in global configuration mode. Second, the list is applied to the appropriate interface as either an inbound list or an outbound list in interface configuration mode.

In this lab, you will create a standard IP access list that will deny access to network 210.93.105.0 from any host on network 205.7.5.0. You then will apply it to the appropriate interface on the lab-d router in the internetworking lab. Finally, you will monitor and test your list.

Note that you must complete the first six questions of this lab before attempting to configure the router. This will save time because designing the list is the most time-consuming part of access list configuration, and can be done in advance.

After completing this lab, you will be able to:

- Create a standard IP access list using Notepad
- Configure the standard IP access list and apply it to the appropriate interface
- Use the correct show commands to monitor the standard IP access list
- Test the standard IP access list

### Materials Required

This lab requires the following:

- The internetworking lab setup used in the labs from Chapters 5 and 6
- The successful completion of the labs in Chapters 5 and 6

### Activity

Estimated completion time: **45 minutes**

Before beginning, make sure the lab equipment is set up and configured as shown in Figure 10-1. Pay particular attention to the wiring and IP configuration changes that were made to the lab during previous labs. Do not skip the first six questions in this lab. Doing so will only slow down the configuration process.

1. Examine Figure 10-1. The access list to deny access to network 210.93.105.0 from any host on network 205.7.5.0 should be created and applied on the lab-d router. Why?

---

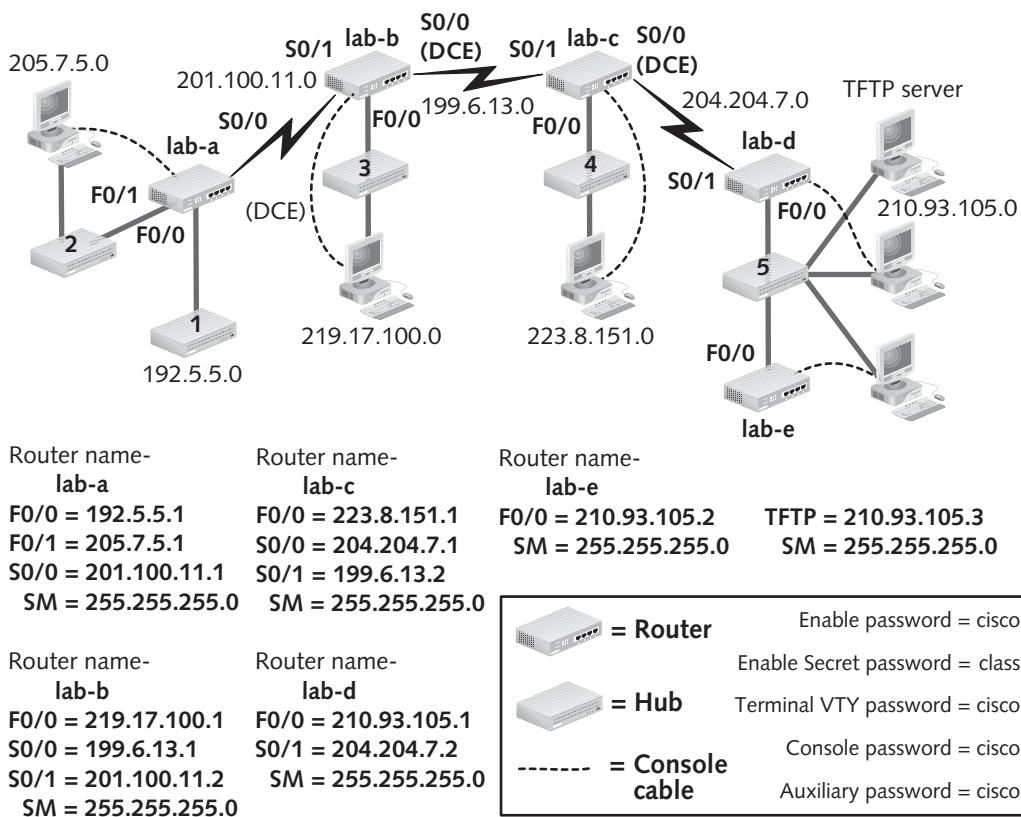
2. Write the access list to deny any traffic from network 205.7.5.0 from reaching any host on network 210.93.105.0. Do not forget the permit statement. Use Figure 10-1 for reference.

---

---

## Lab 10.1 Create and Apply a Standard IP Access List on the Lab-d Router

581

**Figure 10-1** Connection information

3. Why is the permit statement necessary?

---



---

4. Which list number did you use in the list?

---



---

What is the acceptable range for a standard IP list?

---



---

Correct your list number in Step 2, if necessary.

5. On which interface and in which direction will you apply the list you created in Step 2?

---



---

Why?

---



---

6. Which command will you use to apply the access list?

---



---

**582** Chapter 10 Access Lists

7. Turn on the Windows computers, routers, and hubs, if necessary. Attach a UTP patch cable between the NIC in the lab-a Windows computer and the hub connected to the F0/1 interface of the lab-a router. Make sure the NIC light on the computer and the corresponding port light on the hub are on.
  8. Make sure the IP address and gateway configured on the lab-a Windows computer are 205.7.5.2 and 205.7.5.1, respectively. You may have to restart the computer if you make any IP configuration changes to the workstation.
  9. Return to the lab-d computer, if necessary. Log in to the lab-d router using **cisco** as the console password. Enter enable mode using the password **class**.
  10. Enter global configuration mode.
  11. Click the Windows Start button, point to All Programs, point to Accessories, and then click Notepad to open the Notepad program.
  12. Type **no access-list [#]**, where # is the list number that you recorded in Step 4. Press Enter. Why should this statement be the first line in your text editor access list?
- 

13. Type the access list commands created in Step 2 on separate lines under the no access-list command.
14. Highlight your list and copy it to the Clipboard.
15. Minimize Notepad, right-click beside the **lab-d(config)#** prompt, and then click Paste to Host. Your list should be entered into the router's running configuration. If it did not work, try the copy-and-paste operation again.
16. When will the access list take effect?

---
17. Enter interface configuration mode for the interface you specified in Step 5.
18. Apply the list using the command you specified in Step 6.
19. Press **Ctrl+Z** to return to enable mode.
20. Use the **show access-lists** command to see the access list defined on the lab-d router. What information is provided by this command?

---
21. In this case, which other command will give you identical information?

---
22. Type **show ip interface**, and then press Enter. What kind of information do you get regarding the access list?

---
23. Move to the computer attached to the lab-a router, or ask your teammate configuring the lab-a router to do the next three steps for you. Make sure that it is turned on, and then close any open programs, if necessary.
24. Open a Windows command prompt window.

25. Type **ping 210.93.105.2**, and then press **Enter**.

26. What was the response?

---

What does the response mean?

---

27. If you were able to ping successfully, your access list is incorrect or is applied incorrectly. Make any necessary corrections to your access list in Notepad, copy and paste to the host again, and then retest.
28. Close the command prompt window on the workstation connected to the lab-a router.
29. Return to the lab-d router, if necessary.
30. Enter global configuration mode and then interface configuration mode for the interface on which the list is applied.
31. Use the **no ip access-group [#] [direction]** command, where # is the list number and *direction* is either in or out, to remove the list from the interface.
32. Type **exit** to return to global configuration mode.
33. Type **no access-list [#]**, where # is the list number, to remove the list from the router.
34. Exit to enable mode and use the **show access-lists** command to verify that the list has been removed.
35. Log out of the lab-d router.

10

## Certification Objectives

Objectives for the CCNA exam:

- Describe the purpose and types of ACLs
- Verify and monitor ACLs in a network environment
- Configure and apply ACLs based on network filtering requirements

## Review Questions

1. How does using Notepad facilitate creating access lists in the router?
2. Why must standard IP access lists be applied as close to the destination as possible?
3. What is the wildcard mask that filters any host on a class B network?
4. What is the wildcard mask that filters any host on a class A network?

## Lab 10.2 Create and Apply an Extended IP Access List on the Lab-b Router

### Objectives

The objective of this lab is to configure an extended IP access list. This process is the same as that for a standard IP access list. First, the list is created using a text editor and configured in global configuration mode. Second, it is applied to the appropriate interface as either an inbound list or an outbound list in interface configuration mode.

In this lab you will create an extended IP access list to deny the host with the IP address 219.17.100.2 from pinging the host with IP address 205.7.5.2. You will then apply the list to the appropriate interface on the lab-b router in the internetworking lab. Finally, you will monitor and test your list.

Note that you must complete the first six questions of this lab before attempting to configure the router. This will save time because designing the list is the most time-consuming part of access list configuration, and can be done in advance.

After completing this lab, you will be able to:

- Create an extended IP access list using Notepad
- Configure the extended IP access list and apply it to the appropriate interface
- Use the correct show commands to monitor the extended IP access list
- Test the extended IP access list

### Materials Required

This lab requires the following:

- The internetworking lab setup used in the labs from Chapters 5 and 6
- The successful completion of the labs in Chapters 5 and 6
- Two extra UTP patch cables

### Activity

Estimated completion time: **45 minutes**

Do not skip the first six questions in this lab. Doing so will only slow down the configuration process.

1. Examine Figure 10-1 again. The access list to deny the host with the IP address 219.17.100.2 from pinging the host with IP address 205.7.5.2 should be created and applied on the lab-b router. Why?

- 
2. Write the access list to deny ping traffic from node 219.17.100.2 from reaching host 205.7.5.2. Do not forget the permit statement. Use Figure 10-1 for reference.
- 
-

## Lab 10.2 Create and Apply an Extended IP Access List on the Lab-b Router

**585**

3. Why is the **permit** statement necessary?

---

---

4. Which list number did you use in the list?

---

---

Correct your list number in Step 2, if necessary.

5. On which interface and in which direction will you apply the list you created in Step 2?

---

---

Why?

---

---

6. Which command will you use to apply the access list?

---

---

7. Turn on the Windows computers, routers, and hubs, if necessary. Make sure a UTP patch cable is between the NIC in the lab-a Windows computer and the hub connected to the F0/1 interface of the lab-a router. Make sure the NIC light on the computer and the corresponding port light on the hub are on. The lab-b computer should be attached via UTP to the hub connected to the F0/0 interface on the lab-b router. Again, check lights to make sure you have Physical layer connectivity.

8. Make sure the IP address and gateway configured on the lab-a Windows computer are 205.7.5.2 and 205.7.5.1, respectively. You may have to restart the computer if you changed the IP configuration of the workstation.

9. Make sure the IP address and gateway configured on the lab-b Windows computer are 219.17.100.2 and 219.17.100.1, respectively. You may have to restart the computer if you changed the IP configuration of the workstation.

10. Return to the lab-b computer if necessary. Open a Windows command prompt window.

11. Type **ping 205.7.5.2**, and then press **Enter**.

What was the response?

---

---

What does the response mean?

---

---

12. If you were unable to ping successfully, start troubleshooting with the help of your instructor. Make sure all of the interfaces between the lab-b router and the lab-a router have an up/up status. After you can ping successfully, continue with the next step.

13. Close the command prompt window on the workstation connected to the lab-b router.

**10**

**586** Chapter 10 Access Lists

14. Log in to the lab-b router using **cisco** as the console password. Enter enable mode using the password **class**.
  15. Enter global configuration mode.
  16. Click the Windows Start button, point to All Programs, point to Accessories, and then click Notepad to open the Notepad program.
  17. Type **no access-list [#]**, where # is the list number that you recorded in Step 4, and then press **Enter**. Why should this statement be the first line in your text editor access list?
- 
- 

18. Type the **access list** commands created in Step 2 on separate lines under the **no access-list** command.
  19. Highlight your list and copy it to the Clipboard.
  20. Minimize Notepad, right-click beside the **lab-b(config)#** prompt, and then click **Paste to Host**. Your list should be entered into the router's running configuration.
  21. When will the access list take effect?
- 
- 

22. Enter interface configuration mode for the interface you specified in Step 5.
23. Apply the list using the command you specified in Step 6.
24. Press **Ctrl+Z** to return to enable mode.
25. Open a Windows command prompt window.
26. Type **ping 205.7.5.2**, and then press **Enter**.
27. What was the response?

---

What does the response mean?

---

---

28. If you were able to ping successfully, your access list is incorrect or applied incorrectly. Make any necessary corrections to your access list in Notepad, copy and paste to the host again, and then retest.
  29. Close the command prompt window on the workstation connected to the lab-b router.
  30. Use the **show access-lists** command to see the access list defined on the lab-b router. What information is provided by this command?
-

Lab 10.2 Create and Apply an Extended IP Access List on the Lab-b Router **587**

31. Compared to using this command with a standard IP list, what additional information do you receive for an extended IP list? (*Hint:* matches)
- 

32. Type **clear access-list counters [#]**, where # is the list number, and then press **Enter**. What do you think this command does?
- 

33. Use the **show access-lists** command again. Were the counters (matches) cleared?
- 

34. Enter global configuration mode and then interface configuration mode for the interface on which the list is applied.

35. Use the **no ip access-group [#] [direction]** command, where # is the list number and *direction* is either in or out, to remove the list from the interface.

36. Type **exit** to return to global configuration mode.

37. Type **no access-list [#]**, where # is the list number, to remove the list from the router.

38. Exit to enable mode and use the **show access-lists** command to verify that the list has been removed.

39. Log out of the lab-b router.

**10**

## Certification Objectives

Objectives for the CCNA exam:

- Describe the purpose and types of ACLs
- Verify and monitor ACLs in a network environment
- Configure and apply ACLs based on network filtering requirements

## Review Questions

1. What does the **host** keyword represent?
2. What does the **any** keyword represent?
3. With standard IP lists, the 0.0.0.0 wildcard mask is assumed. Is it also assumed with extended IP lists?

## Lab 10.3 Create and Apply a Named Access List on the Lab-c Router

### Objectives

In Cisco IOS versions 11.2 and above, you can use names instead of numbers to identify lists. The objective of this lab is to create an extended named list on the lab-c router that denies any Web or ICMP traffic to host 223.8.151.2.

After completing this lab, you will be able to:

- Create an extended named access list
- Apply the list to the appropriate interface
- Test the list
- Use the correct show commands to monitor the list

### Materials Required

This lab requires the following:

- The internetworking lab setup used in the labs from Chapters 5 and 6
- The successful completion of the labs in Chapters 5 and 6
- One extra UTP patch cable

### Activity

Estimated completion time: **25 minutes**

1. Turn on the Windows computers, routers, and hubs, if necessary. Attach a UTP patch cable between the NIC in the lab-c Windows computer and the hub connected to the F0/0 interface of the lab-c router. Make sure the NIC light on the computer and the corresponding port light on the hub are on.
  2. Make sure the IP address and gateway configured on the lab-c Windows computer are 223.8.151.2 and 223.8.151.1, respectively. You may have to restart the computer if you changed the IP configuration of the workstation.
  3. Log in to the lab-c router using the HyperTerminal program. The console password is **cisco**. Enter enable mode using the password **class**.
  4. Enter the **show interface** command and make sure that all of the active interfaces on the router are up. If any of the interfaces are administratively down, enter interface configuration mode for that interface and enter the **no shutdown** command.
  5. Enter global configuration mode. Type **ip access-list extended cannon** and press **Enter**. To what does the prompt change?
- 
6. Type **deny tcp any host 223.8.151.2 eq www** and press **Enter**. What does this access list line do?

Lab 10.3 Create and Apply a Named Access List on the Lab-c Router 589

7. Type **deny icmp any host 223.8.151.2** and press Enter. What does this access list line do?

---

8. Type **permit ip any any** and press Enter.

9. Now apply the list. Type **int f0/0** and press Enter.

10. Type **ip access-group cannon out** and press Enter.

11. Press **Ctrl+Z** to return to enable mode.

12. Use the **show access-lists** command to see if your named list appears.

13. Use the **show ip interface** command to see if your named list was applied correctly. If your list has been configured and applied correctly, proceed to the next step. If it has not been configured or applied correctly, use the **no ip access-list extended cannon** command and the **no ip access-group cannon out** command to remove the list and then try again.

14. Now test the list. Move to the lab-b or lab-d computer and access the corresponding router. Type **ping 223.8.151.2** and press Enter. Alternatively, you could ask your teammate on the lab-b or lab-d router to ping the address. What was the response and what does it mean?

---

15. Enter global configuration mode on the lab-c router.

16. Use the up arrow key on your keyboard to find the **ip access-list extended cannon** command you entered earlier.

17. Press **Ctrl+A** to move the cursor to the beginning of the line.

18. Type **no**, press the **spacebar** once, and then press **Enter** to remove the named access list.

19. Type **int f0/0** and press **Enter**.

20. Use the up arrow key on your keyboard to find the **ip access-group cannon out** command you entered earlier.

21. Press **Ctrl+A** to move the cursor to the beginning of the line.

22. Type **no**, press the **spacebar** once, and then press **Enter** to remove the application of the named access list.

23. Press **Ctrl+Z** to return to enable mode.

24. Use the **show access-lists** command to verify that the list has been removed.

25. Again attempt to ping 223.8.151.2 from the lab-b or lab-d router. This time the ping should be successful.

26. Log out of the lab-c router.

10

## Certification Objectives

Objectives for the CCNA exam:

- Describe the purpose and types of ACLs
- Verify and monitor ACLs in a network environment
- Configure and apply ACLs based on network filtering requirements

## Review Questions

1. What is an advantage of using named lists?
2. What is the advantage of using extended lists over standard lists?
3. Which Cisco IOS version allows you to use named lists?

## C H A P T E R E L E V E N

# PPP AND FRAME RELAY

## Labs included in this chapter

- Lab 11.1 Configure PPP with CHAP and PAP
- Lab 11.2 Set Up a Test Frame Relay Network
- Lab 11.3 Configure the Lab-c Router to Simulate a Frame Relay Switch
- Lab 11.4 Configure the Lab-b and Lab-d Routers for Frame Relay

## CCNA Exam Objectives

| Objective                                                   | Lab              |
|-------------------------------------------------------------|------------------|
| Configure and verify a PPP connection between Cisco routers | 11.1             |
| Configure and verify Frame Relay on Cisco routers           | 11.2, 11.3, 11.4 |

## Lab 11.1 Configure PPP with CHAP and PAP

### Objectives

The objective of this lab is to configure a serial interface on the router for Point-to-Point Protocol (PPP) with Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication. Although the default encapsulation on serial interfaces is High-level Data Link Control (HDLC), PPP is preferred in many cases because of its superior Network layer and authentication functionality.

In this lab you will configure each end of a WAN link for PPP with CHAP and PAP. *This means you must configure a router that has an active serial interface.* You will check the status of the newly configured serial interfaces using the `show interface` command. Finally, you will confirm Network layer connectivity between the WAN links.

After completing this lab, you will be able to:

- Configure PPP with CHAP and PAP on a WAN link
- Understand why a WAN link is working or not
- Interpret the status line of the `show interface` command output

### Materials Required

This lab requires the following:

- The internetworking lab setup used in the labs from Chapters 5 and 6
- Completion of the labs in Chapters 5 and 6

### Activity

Estimated completion time: **30 minutes**



This lab cannot be done on the lab-e router because the router has no active serial interfaces.

NOTE

- Start the Windows computer, and begin the HyperTerminal session with the router.
  - Turn on the routers and hubs, if necessary. Press `Enter` to get started, and then type the password `cisco` to reach the user EXEC mode prompt. Type `enable`, and then press `Enter` to access privileged EXEC mode.
  - Type `class`, and then press `Enter` when prompted for the enable secret password.
  - Enter global configuration mode.
  - Enter the command to configure an active serial interface on your router. Which command did you enter?
- 
- Type `encap ppp`, and then press `Enter`. What does the `encap` abbreviation stand for?  
\_\_\_\_\_

What does the **encap ppp** command do?

---

What was the encapsulation before you changed it to **ppp**?

7. Type **ppp authentication chap pap**, and then press **Enter**.

---

What does this command do?

8. Type **exit**, and then press **Enter** to return to global configuration mode.
9. Next, configure the username and password for the link. The command syntax is **username [remote router host name] password [password]**. Use **cannon** as the password. Which command did you enter?

- 
10. Press **Ctrl+Z**.

11. Enter the **show interfaces** command for the interface that you just configured. What is the status of this interface?

- 
12. If the line protocol is down, what is your explanation for it being down? (*Hint:* Is the other end of the WAN link configured for PPP?)



11

- 
13. Move to the remote router that you specified in Step 9. This router is on the other end of the WAN link that you just configured. To which router did you move?

- 
14. Enter global configuration mode, and then enter the command to configure the serial interface connected to the serial interface you have already configured. Which command did you enter?

- 
15. Type **encap ppp**, and then press **Enter**.

16. Type **ppp authentication chap pap**, and then press **Enter**.

17. Press **Ctrl+Z**.

18. Enter the **show interfaces** command for the interface that you just configured. What is the status of this interface?

---

---

**594** Chapter 11 PPP and Frame Relay

19. If the line protocol is down, what is your explanation for it being down? (*Hint:* password)

---

---

---

20. Enter global configuration mode.

21. Configure the username and password for the link, as you did in Step 9. You must use the remote router's host name but the same password, which should be **cannon**. Which command did you enter?

---

22. Press **Ctrl+Z**.

23. Enter the **show interfaces** command again for the interface that you just configured. What is the status of this interface?

---

---

24. If the line protocol is up, what is your explanation?

---

---

25. Ping the other end of the WAN link to confirm connectivity. Which command did you use?

---

---

26. Enter the **show ip interface** command for the interface that you configured for PPP. Notice the words "peer address" with the IP address of the remote serial interface in the output. What is the meaning of "peer" in this context?

---

---

27. Enter global configuration mode, and then interface configuration mode for the serial interface on which the PPP encapsulation has been configured. Remove the PPP encapsulation from the serial interface. Which command did you use?

---

---

28. Exit to global configuration mode, and then use the keyboard and editing shortcuts to retrieve the username command and negate it.

29. Repeat Steps 27 and 28 for the first router that you configured for PPP. Exit to enable mode.

30. Use the **show interfaces** command to examine the default encapsulation on Cisco WAN interfaces. What is it?

---

---

31. Type **logout**, and then press **Enter** to exit the router.

## Certification Objectives

Objectives for the CCNA exam:

- Configure and verify a PPP connection between Cisco routers

## Review Questions

- Why is PAP considered a two-way handshake?
- Why is CHAP considered a three-way handshake?
- When is Cisco's HDLC used on WAN interfaces?
- What are the advantages of PPP compared with its predecessor SLIP?

---

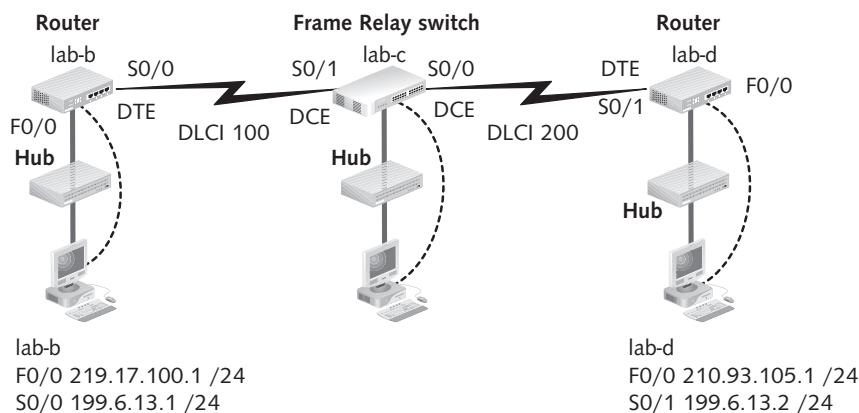
## Lab 11.2 Set Up a Test Frame Relay Network

### Objectives

The objective of this lab is to configure a test Frame Relay network using a router to simulate the Frame Relay switch. As you may know, a Cisco router can be configured to act as a Frame Relay switch. Because a Frame Relay switch acts as a channel service unit/data service unit (CSU/DSU), the router simulating the switch must be configured as the data communications equipment (DCE) on both serial interfaces.

11

In this lab you will make the physical connections necessary to set up a test Frame Relay network. The lab-c router will act as the switch, and the lab-b and lab-d routers connected to the lab-c router will be configured for Frame Relay, as shown in Figure 11-1. You will also test the DCE.



**Figure 11-1** Frame Relay configuration

**596** Chapter 11 PPP and Frame Relay

After completing this lab, you will be able to:

- Set up a test Frame Relay network
- Understand the relationship between the DCE and the data terminal equipment (DTE), and the equipment that comprises each
- Test the DCE connection using the show controller serial command
- Erase the startup configuration on the routers

## Materials Required

This lab requires the following:

- The internetworking lab setup used in the labs from Chapters 5 and 6
- Completion of the labs in Chapters 5 and 6

## Activity

Estimated completion time: **30 minutes**

1. Make sure that all routers are off. Refer to Figure 11-1 as you work through this lab.
  2. Remove the serial cable between the lab-b and lab-c routers.
  3. Plug the DCE end into the S0/1 interface of the lab-c router.
  4. Plug the DTE end into the S0/0 interface of the lab-b router. Why is reversing the serial cable ends necessary in this lab?
- 
- 

5. Turn on the lab-b, lab-c, and lab-d routers and the hubs that are connected to them.
  6. Turn on the computers connected via the console port to the three routers, if necessary.
  7. Open a session in HyperTerminal to connect to the three routers.
  8. Move to the lab-c router terminal, which will be the one simulating the Frame Relay switch.
  9. Press **Enter** to get started, if necessary, and type the password **cisco** to reach the user EXEC mode prompt. Type **enable**, and then press **Enter** to access privileged EXEC mode.
  10. Type **class**, and then press **Enter** when prompted for the enable secret password.
  11. Type **show controller serial 0/0**, and then press **Enter**. Does the command output indicate that it is a DCE port?
- 

If the answer is no, something is wrong with the way the cable is connected to the S0/0 interface, and you must begin troubleshooting. Make sure the correct end of the cable is securely attached to the router interface. If the answer is yes, proceed to Step 12.

12. Type **show controller serial 0/1**, and then press **Enter**. Does the command output indicate that it is a DCE port?
- 

If the answer is no, something is wrong with the way that the cable is connected to the S0/1 interface, and you must begin troubleshooting. Make sure the correct end of the cable is securely attached to the router interface. If the answer is yes, proceed to Step 13.

13. Type **erase start**, and then press **Enter** to erase the startup configuration. Confirm the erase, if necessary. Where is the startup configuration stored?

---

14. Type **reload**, and then press **Enter** to restart the router with the empty configuration. If you are prompted to save, type **N** for no. Confirm the reload.
15. Because the startup configuration has been erased, you will be prompted to enter an initial configuration using the system configuration dialog. Type **N** for no and press **Enter**. You may also be prompted to terminate autoinstall. Type **Y** for yes and press **Enter**.
16. Move to the lab-b router terminal.
17. Press **Enter** to get started, if necessary, and then type the password **cisco** to reach the user EXEC mode prompt. Type **enable**, and then press **Enter** to access privileged EXEC mode.
18. Type **class**, and then press **Enter** when prompted for the enable secret password.
19. Type **show controller serial 0/0**, and then press **Enter**. Does the command output indicate that it is a DTE port?

If the answer is no, something is wrong with the way the cable is connected to the S0/0 interface, and you must begin troubleshooting. If the answer is yes, proceed to Step 20.

20. Type **erase start**, and then press **Enter** to erase the startup configuration. Confirm the erase, if necessary.
21. Type **reload**, and then press **Enter** to restart the router with the empty configuration. If you are prompted to save, type **N** for no. Confirm the reload.
22. Because the startup configuration has been erased, you will be prompted to enter an initial configuration using the system configuration dialog. Type **N** for no and press **Enter**. You may also be prompted to terminate autoinstall. Type **Y** for yes and press **Enter**.
23. Move to the lab-d router terminal.
24. Press **Enter** to get started, if necessary, and type the password **cisco** to reach the user EXEC mode prompt. Type **enable**, and then press **Enter** to access privileged EXEC mode.
25. Type **class**, and then press **Enter** when prompted for the enable secret password.
26. Type **show controller serial 0/1**, and then press **Enter**. Does the command output indicate that it is a DTE port?

11

If the answer is no, something is wrong with the way that the cable is connected to the S0/1 interface, and you must begin troubleshooting. If the answer is yes, proceed to Step 27.

27. Type **erase start**, and then press **Enter** to erase the startup configuration. Confirm the erase, if necessary.
28. Type **reload**, and then press **Enter** to restart the router with the empty configuration. If you are prompted to save, type **N** for no. Confirm the reload.
29. Because the startup configuration has been erased, you will be prompted to enter an initial configuration using the system configuration dialog. Type **N** for no and press **Enter**. You may also be prompted to terminate autoinstall. Type **Y** for yes and press **Enter**.

**598** Chapter 11 PPP and Frame Relay

30. In Frame Relay networks, what is the DCE?

---

---

In Frame Relay networks, what is the DTE?

---

---

You have made and tested the physical connections necessary to make the lab-c router simulate a Frame Relay switch. In the next lab, you will configure the lab-c router with the correct Frame Relay commands.

### Certification Objectives

Objectives for the CCNA exam:

- Configure and verify Frame Relay on Cisco routers

### Review Questions

1. What is the function of a DTE?
2. What is the function of a DCE?
3. In the case of Frame Relay, are the DTE and DCE both customer premises equipment (CPE)?

---

## Lab 11.3 Configure the Lab-c Router to Simulate a Frame Relay Switch

### Objectives

If you made the physical connections outlined in Lab 11.2, you are ready to configure the lab-c router to simulate a Frame Relay switch, which is the objective of this lab. This lab involves some commands that, although not normally seen on a router, give you insight into the structure of a Frame Relay network.

In this lab you will configure the lab-c router to simulate a Frame Relay switch that connects the lab-b and lab-d routers.

After completing this lab, you will be able to:

- Configure a router to simulate a Frame Relay switch
- Understand how a Frame Relay switch operates

## Materials Required

This lab requires the following:

- The internetworking lab setup used in the labs from Chapters 5 and 6
- Completion of the labs in Chapters 5 and 6 and Lab 11.2

## Activity

Estimated completion time: **30 minutes**

1. Move to the lab-c router terminal, if necessary. Press **Enter** to get started, and then enter global configuration mode.
2. Type **frame-relay switching**, and then press **Enter**. This command must be entered before the router can perform as a Frame Relay switch.
3. Type **int s0/1**, and then press **Enter** to begin configuration of the serial port leading to the lab-b router, as shown in Figure 11-1.
4. Type **encap frame-relay**, and then press **Enter**. What does this command do?

---

5. Type **no ip address**, and then press **Enter**. Why is there no IP address on this router interface?

---

6. Type **clockrate 1000000**, and then press **Enter**. What is the speed of this link? (Include units in your speed statement.)

---

Why is the clockrate command necessary on this interface?

---

7. Type **frame-relay intf-type dce**, and then press **Enter**. This command sets up the interface as a DCE device on a Frame Relay network. The default is DTE, so you will not normally use this command on a router.
8. Type **frame-relay route 100 int s0/0 200**, and then press **Enter**. This command configures a static route from the lab-b router to the lab-d router through the switch using the DLCIs.
9. Type **no shutdown** and then press **Enter**.
10. Enter interface configuration mode for the S0/0 interface, and configure it as you configured the S0/1 interface using the commands in Steps 4 through 9. The static route command in Step 8 will be slightly different, reflecting a route from the lab-d router to the lab-b router. Which static route command will you use?
11. Press **Ctrl+Z** to exit to enable mode. In the next lab, you will configure the lab-b and lab-d routers to operate on the simulated Frame Relay network.

## Certification Objectives

Objectives for the CCNA exam:

- Configure and verify Frame Relay on Cisco routers

## Review Questions

- Which WAN encapsulation was on the serial interface on the lab-c router before you configured it for Frame Relay?
- Why don't you typically use the `frame-relay switching` command on a router?
- What does the Data Link Connection Identifier (DLCI) do?
- What is the most important parameter to negotiate in a Frame Relay contract with a service provider?

---

## Lab 11.4 Configure the Lab-b and Lab-d Routers for Frame Relay

### Objectives

If you made the physical connections outlined in Lab 11.2, and configured the lab-c router to simulate a Frame Relay switch, as outlined in Lab 11.3, you are ready to configure the lab-b and lab-d routers for Frame Relay, which is the objective of this lab.

In this lab you will configure the lab-b and lab-d routers for Frame Relay with the default Cisco encapsulation for Local Management Interface (LMI) and Inverse ARP enabled. You will then test your configuration using the Frame Relay show commands.

After completing this lab, you will be able to:

- Configure a router for Frame Relay
- Understand the output of the various Frame Relay show commands

### Materials Required

This lab requires the following:

- The internetworking lab setup used in the labs from Chapters 5 and 6
- Completion of the labs in Chapters 5 and 6 and Labs 11.2 and 11.3

## Activity

Estimated completion time: **30 minutes**

1. Move to the lab-b router terminal, if necessary, and then press **Enter** to get started and enter global configuration mode.
2. Configure the IP address on the F0/0 interface of the lab-b router, per Figure 11-1. Which command did you enter?
3. Type **no shutdown** and press **Enter**.
4. Configure the IP address on the S0/0 interface of the lab-b router, per Figure 11-1. Include the **no shutdown** command. Which commands did you enter?

- 
5. Type **encap frame-relay** and then press **Enter**. What does this command do?

---

- 
6. Exit to global configuration mode.
  7. Enter the commands to configure the router for the RIPv2 routing protocol. Which two commands did you enter?
  8. Enter the **network** commands to complete the RIPv2 configuration. Use Figure 11-1 as a reference. Which two network commands did you enter?

**11**

Notice that when the lab-c router operates as a Frame Relay switch, the serial interfaces on the lab-b and lab-d routers reside on the same network.

9. Press **Ctrl+Z** to return to enable mode.
10. Move to the lab-d router terminal and enter global configuration mode.
11. Using Steps 2 through 9 and Figure 11-1 as a reference, configure the lab-d router for Frame Relay.
12. From the lab-d router, ping the FastEthernet port of the lab-b router. Was the ping operation successful?

---

If the answer is no, check your configurations on all three routers and get help from your teammates or instructor if necessary. Make sure that the interfaces are not shut down. In addition, check your routing table. There should be three entries in the routing table of the lab-d and lab-b routers: the two networks to which the router is directly connected and a network that the router learned about via RIPv2. Repeat Step 12 from the lab-b router and ping the lab-d router. When the ping operations are successful, proceed to Step 13.

**602** Chapter 11 PPP and Frame Relay

13. Type **show frame-relay pvc** on the lab-b or lab-d router, and then press **Enter**. Are these routers acting as DCEs or DTEs? How do you know?

---

---

What is the local DLCI?

14. Type **show frame-relay map** on the lab-b or lab-d router, and then press **Enter**. To which IP address is the local DLCI mapped?

15. Type **show interfaces** on the lab-b or lab-d router. Can you verify that the Frame Relay encapsulation is on the appropriate serial interface?

16. Move to the lab-c router console terminal.

17. Type **show frame-relay route**, and then press **Enter** to look at the Frame Relay switching table. What information is contained in a Frame Relay switch table?

---

---

18. Type **show frame-relay pvc**, and then press **Enter** on the lab-c router terminal. Is this router acting as a DCE or DTE? How do you know?

---

---

19. Log out of all three routers. Turn off the three routers.

20. Switch the ends of the serial cable between the lab-b and lab-c router.

## Certification Objectives

Objectives for the CCNA exam:

- Configure and verify Frame Relay on Cisco routers

## Review Questions

- Which show command displays statistics regarding the PVC circuit?
- How exactly did the Frame Relay map table get built in this lab?
- Why did you not have to use the **frame-relay lmi-type** command in this lab?

## C H A P T E R T W E L V E

# BASIC SWITCHING AND SWITCH CONFIGURATION

## Labs included in this chapter

- Lab 12.1 Configure a Cisco 2950 Switch Using the CLI
- Lab 12.2 Evaluate Hub Performance
- Lab 12.3 Evaluate Switch Performance

## CCNA Exam Objectives

| Objective                                                                                                                                   | Lab              |
|---------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts                          | 12.1, 12.2, 12.3 |
| Verify network status and switch operation using basic utilities                                                                            | 12.1             |
| Perform and verify initial switch configuration tasks including remote access management                                                    | 12.1             |
| Identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures | 12.1             |
| Implement basic switch security                                                                                                             | 12.1             |
| Explain basic switching concepts and the operation of Cisco switches                                                                        | 12.1, 12.3       |
| Explain the technology and media access control method for Ethernet networks                                                                | 12.2, 12.3       |
| Explain network segmentation and basic traffic management concepts                                                                          | 12.2, 12.3       |

## Lab 12.1 Configure a Cisco 2950 Switch Using the CLI

### Objectives

The objective of this lab is to configure a Cisco 2950 series switch using the command-line interface. The focus of this lab will be the basic switch commands you learned in Chapter 12 of the text, as well as some router commands introduced in earlier chapters which can also be configured on a switch. The commands include hostname, IP address, gateway, domain name, description, banner message, passwords, and port security. You will also monitor, test, and back up your configuration. Finally, you will reset the switch to the factory default settings. These switch commands are part of the CCNA exam.

After completing this lab, you will be able to:

- Identify the status of switch ports
- Configure basic switching commands including port security
- Monitor and test your switch configuration
- Copy the switch configuration to a TFTP server
- Reset the switch configuration to factory defaults

### Materials Required

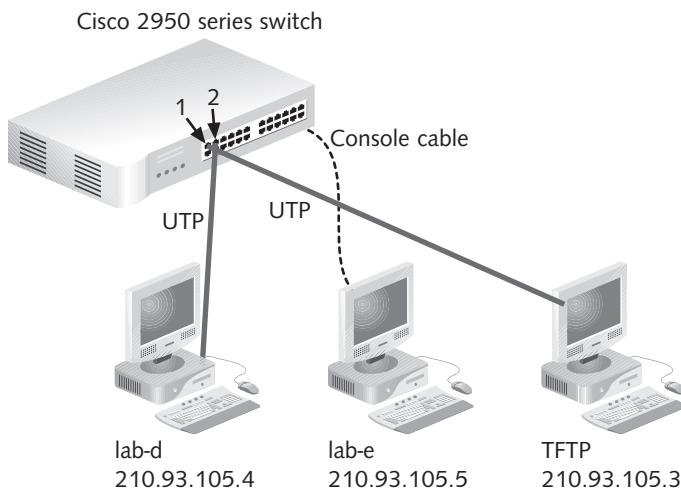
This lab requires the following:

- One Cisco 2950 series switch
- A console cable for the switch
- RJ-45-to-DB-9 adapter
- Three Windows workstations with NICs installed and with HyperTerminal installed (it is easiest to use the lab-d, lab-e, and TFTP server computers)
- One computer running TFTP software and configured with IP address 210.93.105.3
- The lab-d computer configured for IP address 210.93.105.4
- The lab-e computer configured for IP address 210.93.105.5
- Two patch cables
- One power cord for the switch

### Activity

Estimated completion time: **45 minutes**

1. Review Figure 12-1. Plug the console cable into the Cisco 2950 switch console port.
2. Plug the other end of the console cable into an RJ-45-to-DB-9 adapter and connect the adapter to a COM port on the lab-e computer.
3. Connect the TFTP server with IP address 210.93.105.3 to **port 1** of the switch with a UTP patch cable.
4. Connect the lab-d computer with IP address 210.93.105.4 to **port 2** of the switch with a UTP patch cable.



**Figure 12-1** Lab 12.1 configuration

5. Turn on the TFTP server and log in, if necessary.
6. Turn on the lab-d computer and log in, if necessary.
7. Plug in the switch.
8. The port lights on the switch should turn green, and all lights should initially be on and not blinking. After a minute or so, port lights without connections should go off. Ports 1 and 2 should turn first to orange and then to green, which indicates readiness. If the port lights with the computer connections are orange and do not turn green, there is a problem, possibly with the cable. Start troubleshooting and ask your instructor for help.
9. On the lab-d computer, open a Windows command prompt window.
10. Type **ping 210.93.105.3** and press **Enter**.
11. Were you able to ping the TFTP server successfully?

12

---

If you were not able to ping successfully, start troubleshooting with the help of your instructor.

12. On the TFTP server, open a Windows command prompt window.
13. Type **ping 210.93.105.4** and press **Enter**.
14. Were you able to ping the lab-d computer successfully?

---

If you were not able to ping successfully, start troubleshooting with the help of your instructor.

15. Turn on the lab-e computer and log in, if necessary.
16. Start a HyperTerminal session with the switch on the lab-e computer.
17. Press **Enter** to generate output from the switch, if necessary.
18. What is the default hostname for the switch? \_\_\_\_\_

**606** Chapter 12 Basic Switching and Switch Configuration

19. Now you will configure parameters on the switch using almost exactly the same commands you used on a router in previous labs. Enter the following commands:

```
enable  
conf t  
hostname malabar  
enable secret florida  
line con 0  
password cisco  
login  
exit  
line vty 0 15  
password cisco  
login  
exit
```

Which command in this list of commands is not typical for a Cisco router?

- 
20. Enter the **banner motd #** command. In response to the prompt, type **Unauthorized entry is a security violation.#** then press Enter.
21. Type **exit** and press Enter.
22. Type **copy run start** and press Enter, then press Enter again to confirm.
23. Enter the **show run** command. Look for the hostname and enable secret password, which will be at the top of the configuration list. Notice the enable secret password is encrypted. Press the spacebar to scroll through the output. Towards the end of the output, you should see the console and telnet password configurations. Notice they are in clear text.
24. Now you will setup the switch's IP configuration. Typically, the address goes on interface vlan 1. Vlan 1 is considered the management vlan and represents all ports on the switch unless they are moved out of vlan 1. You will learn more about vlans in Chapter 13. Setting up an IP configuration on a switch is not necessary but is helpful if you want to configure and monitor your switch remotely. Type the appropriate commands to enter global configuration mode.
25. Enter the following IP configuration commands:

```
int vlan 1  
ip address 210.93.105.10 255.255.255.0  
description engineering department switch  
no shutdown  
exit  
ip default-gateway 210.93.105.1  
ip domain-name cannonball.com
```

Why is the IP address configured on vlan 1 instead of a port such as f0/0?

- 
26. Next you will configure security on ports 1 and 2. Enter the following commands:

```
int range f0/1 - 2  
switchport port-security mac-address sticky  
switchport port-security maximum 1  
switchport port-security violation shutdown  
Ctrl+Z  
copy run start
```

Explain how the three security measures you have configured on these ports should work.

---

---

- 
27. Finally, you will monitor, test, and back up your configuration. Enter the **show mac-address-table** command. Notice that several static MAC addresses you did not configure are in the table. These are base MAC addresses that are assigned to the CPU and are not relevant to your configuration. Ports 1 and 2 should each indicate a MAC address that was learned dynamically.

28. On the lab-d computer, open a Command Prompt window if necessary and enter the **ipconfig /all** command. Look for the MAC address (physical address). Is it the MAC address reported by the switch for port 2? \_\_\_\_\_

29. Perform Step 28 on the TFTP computer. Is the MAC address of TFTP recorded correctly in the switch table? \_\_\_\_\_

30. To test your port security configuration, unplug the patch cable end from the lab-d computer and connect it to the NIC on the lab-e computer. Leave the other end of the patch cable connected to the switch. What happened to the light on switch port 2? \_\_\_\_\_ Why do you think this happened?
- 

**12**

31. Open a Command Prompt window on the lab-e computer and attempt to ping the TFTP server at 210.93.105.3. Make sure you are not pinging from the HyperTerminal window. Was your ping successful? \_\_\_\_\_ Why or why not?
- 

32. Move the patch cable end from the NIC on the lab-e computer back to the NIC on the lab-d computer. Attempt to ping the TFTP server at 210.93.105.3 from the lab-d computer. Did it work? \_\_\_\_\_ If it did not work, the port is still shut down because it has not “seen” the MAC address of the lab-d computer yet. Return to the HyperTerminal window on the lab-e computer. At some point the f0/2 interface should indicate that it is up. If it does not come up on its own, you will have to enter the **no shutdown** command on the f0/2 interface. Once the interface is up, attempt once again to ping from the lab-d computer to the TFTP server. Once your ping is successful, continue to Step 33.

**608** Chapter 12 Basic Switching and Switch Configuration

33. Now you will test the telnet password. On the lab-d computer, enter **telnet 210.93.105.10** at the command prompt. If your telnet configuration is correct on the switch, you should be prompted for the vty line password. Enter **cisco** and press Enter.
34. Continuing on the lab-d computer, type **enable** and press Enter, then type **florida** and press Enter to reach the enable mode prompt.
35. Next, enter the **show run** command and scroll through the output. Enter the **exit** command to quit your telnet session with the switch.
36. Now that you know your switch configuration is working, return to HyperTerminal on the lab-e computer and enter the **copy run start** command at the enable mode prompt. Press Enter to confirm.
37. Finally, you will back up your configuration to the TFTP server. Open the TFTP server program on the TFTP server, if necessary.
38. On the lab-e computer, type **copy start tftp** and press Enter. You will be prompted for the ip address of the remote host, which is the TFTP server.
39. Type **210.93.105.3** and press Enter. Press Enter again to accept the default destination filename. The copy will be quick since configuration files are relatively small. Did the TFTP server report a successful copy? \_\_\_\_\_  
If you answered no, try again with the help of your instructor.
40. To reset the switch to the factory defaults, you use the same command as is used on a router. Type **erase start** and press Enter. Press Enter again to confirm.
41. Turn off the switch.
42. Close all windows on the computers and log off.

## Certification Objectives

Objectives for the CCNA exam:

- Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
- Verify network status and switch operation using basic utilities
- Perform and verify initial switch configuration tasks including remote access management
- Explain basic switching concepts and the operation of Cisco switches
- Implement basic switch security
- Identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures

## Review Questions

1. Many of the configuration commands on a Cisco 2950 series switch are identical to the commands used on a Cisco 2600 series router. True or False?
2. Why might you want to configure an IP number on your switch?

3. Why might there be more MAC addresses in a switching table reported by the show mac-address-table command than connected devices?
4. What is the purpose of the interface range command?
5. What is the only thing you need to know to back up a configuration file to a TFTP server?

---

## Lab 12.2 Evaluate Hub Performance

### Objectives

The objective of this lab is to illustrate how hubs operate given two different scenarios. The first scenario involves generating data traffic on two ports. The second scenario involves generating data traffic on six ports. In this lab, you will connect the six computers used in the internetworking lab to a common hub. Next, you will time the transfer of a large file between two of the computers. Finally, you will measure the time it takes to move the file back to its original location while generating traffic on six of the ports. The workstations used in this lab are the same ones used to connect to routers lab-a through lab-e. As such, the workstations are referred to as the lab-a workstation, lab-b workstation, the lab-c workstation, and so on. The TFTP server workstation is also used.

After completing this lab, you will be able to:

- Describe how hubs perform when transferring data between two computers
- Describe how hubs perform when transferring data between many computers

**12**

### Materials Required

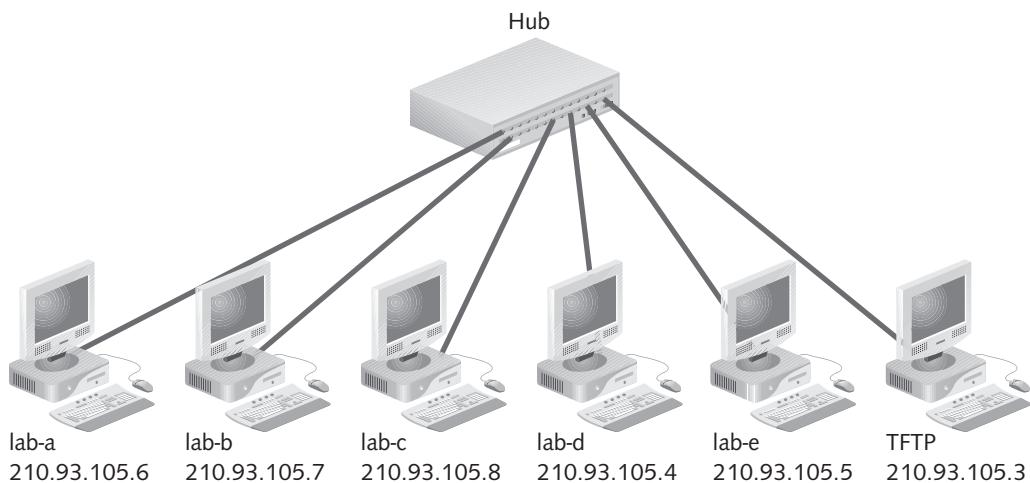
This lab requires the following:

- The internetworking lab computers: lab-a, lab-b, lab-c, lab-d, lab-e, and the TFTP server
- Lab workstations with IP addresses configured for the 210.93.105.0 network and with all workstations in the same workgroup, as shown in Figure 12-2.
- One hub
- Six UTP patch cables
- A shared desktop on all computers with full access
- A file named SWITCHTEST equal to at least 500 MB on the desktops of the lab-b, lab-d, and lab-e computers
- A stopwatch

## Activity

Estimated completion time: **45 minutes**

1. Turn on the six lab workstations and log in, if necessary.
2. Review Figure 12-2. Connect all six workstations via UTP from their NICs to a single hub. Use ports 5 and 6 for the lab-e and TFTP server, respectively. Make sure that you do not use the uplink port on the hub. Plug in the hub and make sure that the hub lights on all connected ports are on.



**Figure 12-2** Lab 12.2 configuration

3. On all six computers, click **Start** then click **Network**. It is important that you are able to see all of the workstations on the network. Sometimes it takes a while for the computers to see each other. Use the F5 key to refresh your screen as necessary until all computers are recognized. Remember, the IP addresses must all be on the same network (210.93.105.0) and the workgroup name must be the same on all computers. Do not continue until all computers can see all other computers. If every workstation is not visible in the Network window, contact your instructor. *Note:* If your computers are using Windows XP, this step will be somewhat different.
4. On the TFTP server, double-click the **lab-e** icon in the **Network** window, and then double-click the **Desktop** folder.
5. Right-click and drag the **SWITCHTEST** file from the desktop of the lab-e computer to the desktop of the TFTP server. *When the shortcut menu appears, stop. This is the operation that you will time using the stopwatch.*
6. Using the stopwatch, calculate the time that it takes to **MOVE** (not copy) the **SWITCHTEST** file from the lab-e computer to the TFTP server.
7. Observe the hub during the move. If there is a collision light, how active is it?

8. Observe the hub ports. Is there any appreciable activity on the ports of the lab-a, lab-b, lab-c, and lab-d workstations? \_\_\_\_\_
  9. How long (in minutes and seconds) did it take to move the SWITCHTEST file from the lab-e computer to the TFTP server? \_\_\_\_\_
  10. Prepare to move the SWITCHTEST file simultaneously from the TFTP server back to the lab-e computer, from the lab-b computer to the lab-a computer, and from the lab-d computer to the lab-c computer.
  11. Move to the lab-c computer, open the **Network** window if necessary, and double-click the **lab-d** icon. Double-click the **Desktop** folder. You should see the SWITCHTEST file.
  12. Right-click and drag the **SWITCHTEST** file from the desktop of the lab-d computer to the desktop of the lab-c computer. When the shortcut menu appears, *stop*.
  13. Move to the lab-a computer and repeat Steps 11 and 12 in preparation for moving the SWITCHTEST file from the lab-b desktop to the desktop of the lab-a computer.
  14. Move to the lab-e computer and repeat Steps 11 and 12 in preparation for moving the SWITCHTEST file from the TFTP desktop to the desktop of the lab-e computer. *This is the only operation that you will time using the stopwatch.*
  15. As close to simultaneously as possible, have your team begin moving (not copying) the SWITCHTEST file from the lab-d computer to the lab-c computer, from the lab-b computer to the lab-a computer, and from the TFTP server to the lab-e computer. *Remember that one of the team members must time the move from the TFTP server to the lab-e computer.*
  16. Observe the hub during the move. If there is a collision light, how active is it compared with the generated activity on only two ports?
- 
17. Approximately how long did it take (in minutes and seconds) to move the SWITCHTEST file from the TFTP server back to the lab-e computer? \_\_\_\_\_
  18. Compare your answer in Step 17 with your answer in Step 9. If there is a difference, how do you account for it?
- 
19. Disconnect the workstations from the hub and unplug the hub.

**12**

## Certification Objectives

Objectives for the CCNA exam:

- Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
- Explain network segmentation and basic traffic management concepts
- Explain the technology and media access control method for Ethernet networks

## Review Questions

1. How do regular half-duplex communications through a hub work?
2. Would a hub be used to solve network congestion problems in an Ethernet network? Why or why not?
3. Why did it take longer to transfer the files when there was traffic on all connected hub ports?

---

## Lab 12.3 Evaluate Switch Performance

### Objectives

The objective of this lab is to illustrate how switches operate in the two scenarios in which you worked in Lab 12.2. In this lab, you will connect the six computers in the internetworking lab to a Cisco 2950 series switch and time the transfer of a large file between two of the computers. You will then measure the time it takes to move the file back while generating other traffic on the rest of the network. Finally, a comparison will be made between the times recorded in this lab and the times recorded for the hub in Lab 12.2.

After completing this lab, you will be able to:

- Understand how switches perform when transferring data between two computers
- Understand how switches perform when transferring data between many computers

### Materials Required

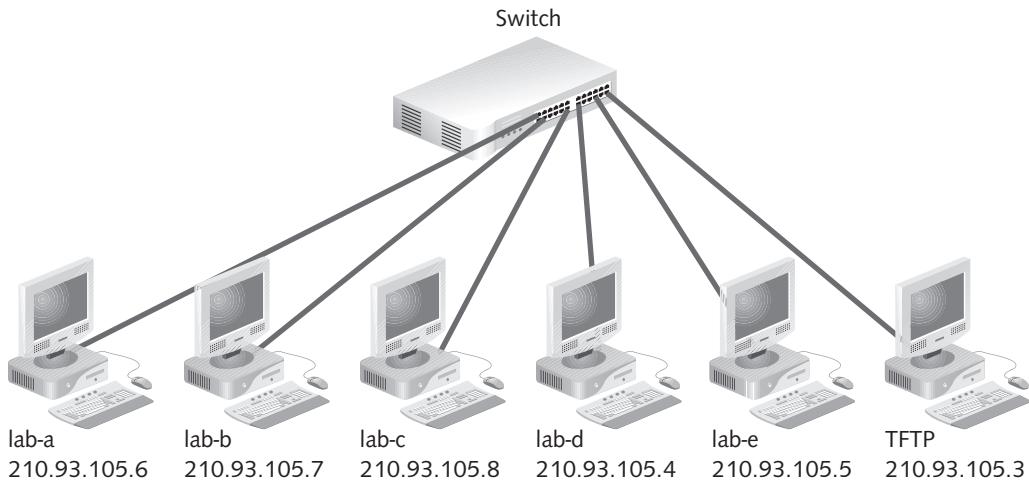
This lab requires the following:

- The internetworking lab computers: lab-a, lab-b, lab-c, lab-d, lab-e, and the TFTP server
- Lab workstations with IP addresses configured for the 210.93.105.0 network
- One Cisco 2950 series switch
- Six UTP patch cables
- A shared desktop on all computers with full access
- A file named SWITCHTEST containing enough files to equal at least 500 MB on the desktops of the lab-a, lab-c, and lab-e computers
- A stopwatch
- The completion of Lab 12.2

## Activity

Estimated completion time: **45 minutes**

1. Turn on the lab workstations and log in, if necessary.
2. Review Figure 12-3. Connect all six workstations via UTP from their NICs to a single switch. Use ports 5 and 6 for the lab-e computer and the TFTP server. Make sure that the switch is turned on and that the connected port lights on the switch have turned green.



**Figure 12-3** Lab 12.3 configuration

3. On all six computers, click **Start**, and then click **Network**. It is important that you are able to see all of the workstations on the network. Sometimes it takes a while for the computers to see each other. Use the F5 key to refresh your screen as necessary until all computers are recognized. Remember, the IP addresses must all be on the same network (210.93.105.0) and the workgroup name must be the same on all computers. Do not continue until all computers can see all other computers. If every workstation is not visible in the Network window, contact your instructor. *Note:* If your computers are using Windows XP, this step will be somewhat different.
4. On the TFTP server, double-click the **lab-e** icon, and then double-click the **Desktop** folder.
5. Right-click and drag the **SWITCHTEST** file from the desktop of the lab-e computer to the desktop of the TFTP server. When the shortcut menu appears, stop. *This is the operation that you will time using the stopwatch.*
6. Using the stopwatch, calculate the time it takes to move (not copy) the SWITCHTEST file from the lab-e computer to the TFTP server.
7. Observe the switch during the move. Is there equal activity on each connected port, or are ports 5 and 6 busier than the other connected ports?

**614** Chapter 12 Basic Switching and Switch Configuration

8. What are the connected ports not involved in the move doing?

---

9. How long (in minutes and seconds) did it take to move the SWITCHTEST file from the lab-e computer to the TFTP server? \_\_\_\_\_

---

10. Prepare to move the SWITCHTEST file simultaneously from the TFTP server to the lab-e computer, from the lab-a computer to the lab-b computer, and from the lab-c computer to the lab-d computer.

11. Move to the lab-b computer, double-click the lab-a icon in the Network window, and then double-click the Desktop folder. You should see the SWITCHTEST file.

12. Right-click and drag the SWITCHTEST file from the desktop of the lab-a computer to the desktop of the lab-b computer. When the shortcut menu appears, stop.

13. Move to the lab-d computer, and repeat Steps 11 and 12 in preparation for moving the SWITCHTEST file from the lab-c computer to the lab-d computer.

14. Move to the lab-e computer and repeat Steps 11 and 12 in preparation for moving the SWITCHTEST file from the TFTP server to the desktop of the lab-e computer. *This is the only operation that you will time using the stopwatch.*

15. As close to simultaneously as possible, have your team begin moving (not copying) the SWITCHTEST file from the lab-c computer to the lab-d computer, from the lab-a computer to the lab-b computer, and from the TFTP server to the lab-e computer. *Remember that one of the team members must time the move from the TFTP server to the lab-e computer.*

16. Observe the switch during the move. Is there equal activity on each connected port?

---

17. Approximately how long did it take (in minutes and seconds) to move the SWITCHTEST file from the TFTP server to the lab-e computer? \_\_\_\_\_

---

18. Record your timings from Lab 12.2 and Lab 12.3 in Table 12-1:

| Scenario                     | Transfer Time in Minutes and Seconds |
|------------------------------|--------------------------------------|
| Hub—activity on two ports    |                                      |
| Hub—activity on six ports    |                                      |
| Switch—activity on two ports |                                      |
| Switch—activity on six ports |                                      |

**Table 12-1** Hub and switch comparison

19. You should have recorded a time difference between the two hub experiments. How do you explain this?

---

20. You should have seen no appreciable time difference between the switch experiments. How do you explain this?
- 
- 

21. Disconnect the workstations from the switch and unplug the switch.

## Certification Objectives

Objectives for the CCNA exam:

- Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
- Explain basic switching concepts and the operation of Cisco switches
- Explain the technology and media access control method for Ethernet networks
- Explain network segmentation and basic traffic management concepts

## Review Questions

1. In terms of collisions and speed, what are the differences between hubs and switches?
2. How do switches solve network congestion problems on Ethernet networks?
3. What does the term “switched bandwidth” mean?



## C H A P T E R      T H I R T E E N

# ADVANCED SWITCHING CONCEPTS

## Labs included in this chapter

- Lab 13.1 Understand Switching and LAN Design Concepts and Terminology
- Lab 13.2 Configure “Router on a Stick”

## CCNA Exam Objectives

| Objective                                                                                                                                           | Lab  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|------|
| Explain the technology and media access control method for Ethernet networks                                                                        | 13.1 |
| Describe enhanced switching technologies (including VTP, RSTP, VLAN, PVST, 802.1Q)                                                                  | 13.1 |
| Describe how VLANs create logically separate networks and the need for routing between them                                                         | 13.1 |
| Verify network status and switch operation using basic utilities (including ping, traceroute, telnet, SSH, arp, ipconfig, show, and debug commands) | 13.2 |
| Identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures         | 13.2 |
| Configure, verify, and troubleshoot VLANs                                                                                                           | 13.2 |
| Configure, verify, and troubleshoot inter-VLAN routing                                                                                              | 13.2 |
| Configure, verify, and troubleshoot VTP                                                                                                             | 13.2 |
| Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network                                | 13.2 |
| Implement basic switch security                                                                                                                     | 13.2 |

## Lab 13.1 Understand Switching and LAN Design Concepts and Terminology

### Objectives

The objective of this lab is to make sure you have a good understanding of modern Ethernet LAN design and the associated terminology. In this lab, you match switching and LAN design terms with their correct definitions.

After completing this lab, you will be able to:

- Understand the terms and concepts related to switching and LAN design

### Materials Required

This lab requires the following:

- Pencil or pen

### Activity

Estimated completion time: **40 minutes**

- Review the following list of terms and then write them in the correct location in Table 13-1. Use each term only once.

- |               |                    |                      |                   |
|---------------|--------------------|----------------------|-------------------|
| • 10BaseT     | • ISL              | • Fast Ethernet      | • Full-duplex     |
| • Half-duplex | • Shared bandwidth | • Switched bandwidth | • CSMA/CD         |
| • Slot time   | • Collision domain | • Broadcast domain   | • VLAN            |
| • Latency     | • Broadcast storm  | • 100BaseT4          | • 100BaseTX       |
| • Auto        | • Half             | • Microsegmentation  | • STP             |
| • Cut-through | • Fragment-free    | • Store-and-forward  | • Management VLAN |
| • VTP         | • RSTP             | • PVST               | • 802.1Q          |

| Description                                                                                                                               | Matching Term |
|-------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| An amount of time that should be slightly longer than the time it takes to transmit a 64-byte frame on an Ethernet wire                   |               |
| Data Link layer protocol defined by IEEE specification 802.1d                                                                             |               |
| The total network bandwidth dedicated to each unicast transmission, even if multiple unicast transmissions are occurring at the same time |               |
| A logical broadcast domain on the LAN created by one or more switches                                                                     |               |
| A layer 2 messaging protocol that manages all the changes to the VLANs across networks                                                    |               |
| The process by which an entire transmitted frame is read into the switch's buffer before being forwarded by the switch                    |               |

**Table 13-1** Switching and LAN design concepts and terminology (*Continued*)

## Lab 13.1 Understand Switching and LAN Design Concepts and Terminology

**619**

| Description                                                                                                                                                                                                                                                                                                             | Matching Term |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Default setting for 10BaseT switch ports                                                                                                                                                                                                                                                                                |               |
| An evolution of STP defined by IEEE 802.1w that allows for more rapid convergence                                                                                                                                                                                                                                       |               |
| A situation in which all devices are in contention for the total bandwidth of the network                                                                                                                                                                                                                               |               |
| The practice of increasing the number of collision domains without increasing the number of subnets                                                                                                                                                                                                                     |               |
| The lag or delay that a device or part of the network media causes                                                                                                                                                                                                                                                      |               |
| Alternate one-way communications                                                                                                                                                                                                                                                                                        |               |
| A switching method in which a frame is forwarded immediately after the destination address is read                                                                                                                                                                                                                      |               |
| Fast Ethernet implementation that uses four pairs of either Category 3, 4, or 5 UTP cable                                                                                                                                                                                                                               |               |
| A topology in which an Ethernet station must first listen before transmitting on the network. Any station can transmit as long as there are no transmissions active on the network. If two stations transmit simultaneously, a collision will occur, and those stations must detect the collision and reset themselves. |               |
| An error condition in which broadcast traffic is above 126 packets per second and network communications are impeded                                                                                                                                                                                                    |               |
| Communication in two directions at once                                                                                                                                                                                                                                                                                 |               |
| A switching method in which a frame is forwarded after the first 64 bytes of the incoming frame are read                                                                                                                                                                                                                |               |
| VLAN 1, which cannot be deleted; also known as the default VLAN                                                                                                                                                                                                                                                         |               |
| An Ethernet flavor that allows frames to be transmitted in 90% less time than with standard Ethernet                                                                                                                                                                                                                    |               |
| A group of devices that will receive broadcast traffic from each other on the LAN                                                                                                                                                                                                                                       |               |
| Fast Ethernet implementation that uses two pairs of either Category 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP)                                                                                                                                                                                      |               |
| Open standard trunking protocol for VLANs                                                                                                                                                                                                                                                                               |               |
| A configuration setting in which a switch port is set to determine whether the connected device is full- or half-duplex, and it configures itself to match                                                                                                                                                              |               |
| Standard Ethernet using UTP cable configured in a physical star                                                                                                                                                                                                                                                         |               |
| Cisco proprietary protocol that maintains a spanning tree instance for each VLAN                                                                                                                                                                                                                                        |               |
| Cisco proprietary trunking protocol for VLANs                                                                                                                                                                                                                                                                           |               |
| A group of devices that are subject to the collisions of each other's traffic                                                                                                                                                                                                                                           |               |

**13**

## Certification Objectives

Objectives for the CCNA exam:

- Explain the technology and media access control method for Ethernet networks
- Describe enhanced switching technologies (including VTP, RSTP, VLAN, PVST, 802.1Q)
- Describe how VLANs create logically separate networks and the need for routing between them

## Review Questions

1. If you have a 10BaseT network with Category 5 UTP cable and are using Cisco 2950 series switches, what will you have to purchase to upgrade your network to full-duplex Fast Ethernet?
2. What are some ways you can limit broadcast traffic on your network?
3. What are ISL and 802.1Q and what is the difference between them?

---

## Lab 13.2 Configure “Router on a Stick”

### Objectives

Router on a stick (also known as ROAST) is an important CCNA exam topic. You must know how to configure and troubleshoot the router and the switch used in the ROAST implementation. Hosts on different VLANs require a layer 3 device to handle the routing between them. In the router-on-a-stick implementation, that device is typically a router.

Cisco uses the term router on a stick to describe a router that routes traffic between two or more subnets, across only one physical link. Each subnet on the switch is related to a separate VLAN, and each subnet requires that a subinterface be configured on the physical interface of the router. The router is connected to a switch via a Fast or Gigabit Ethernet port. You must specify a trunking protocol in order to trunk traffic from multiple VLANs across the single link between the router and the switch. You have two trunking protocol choices: the Cisco-proprietary ISL or the 802.1Q open standard. Not every Cisco switch or router supports both standards. In this project, you will be using the 802.1Q standard.

In addition to configuring ROAST in this project, you will also configure the router for port address translation (PAT). PAT is a form of network address translation (NAT) that maps every inside IP address on the LAN to the single IP address configured on the serial interface of the router. You will also configure the switch for the VLAN trunking protocol (VTP) as well as port-security. Port security on a switch can take multiple forms, but in this project you will restrict ports 2 and 3 on the switch to a single MAC address and configure the switch to learn the connected MAC addresses and keep the addresses in RAM for reference (sticky learn).

so that unauthorized devices cannot communicate. You will test your ROAST implementation by pinging successfully from a workstation on VLAN 1 to a workstation on VLAN 2 and vice-versa.

After completing this lab, you will be able to:

- Configure a 2600 series router for inter-VLAN routing using 802.1Q
- Configure a 2950 series switch for multiple VLANs and trunking
- Configure port address translation (PAT) on the router
- Configure VTP on the switch
- Configure port security on the switch

## Materials Required

This lab requires the following:

- One Cisco 2620 or 2621 series router that supports 802.1Q [minimum release 12.0(1)T with IP Plus]
- One Cisco 2950 series switch that supports 802.1Q [minimum release 12.0(5)WC(1)]
- Power cords for the switch and router
- Two Windows PCs with HyperTerminal or some other communications program used to configure the router and switch locally
- Two console (rollover) cables
- Two RJ-45-to-DB-9 adapters
- Three patch cables

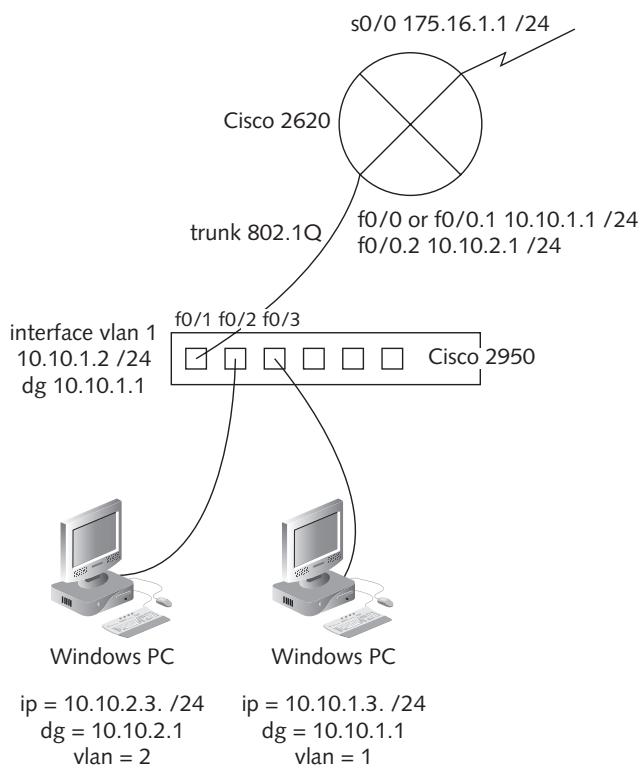
## Activity

Estimated completion time: **90 minutes**

**13**

1. Make sure all equipment is off. Refer to Figure 13-1 and connect the equipment accordingly. You do not need to connect a cable to the serial port on the router.
2. Turn on the equipment once it is cabled correctly.
3. Use a console cable and the HyperTerminal program to access the router and enter the **show version** command. What is the version of the IOS? \_\_\_\_\_ If the version is earlier than 12.3, the IP address that serves as the default gateway for VLAN 1 on the switch will be configured on f0/0 without the 802.1Q encapsulation specified. If the version is 12.3 or later, the IP address will be configured on the first subinterface (f0/0.1), as will the 802.1Q encapsulation, and there will be no IP address on f0/0.
4. Configure the enable password **class** on the router.
5. Configure the vty password **cisco** for all telnet sessions on the router.
6. Configure the name of the router as **c2620**.

## 622 Chapter 13 Advanced Switching Concepts

**Figure 13-1** Router on a stick

7. Configure the interfaces on the router as shown in Figure 13-1 and based on the router's IOS version.
8. Configure port address translation (PAT) on the router.
9. Save your router configuration.
10. Enter the **show run** command. The output should resemble Figure 13-2.
11. Console into the switch and configure the name of the switch as **c2950**.
12. Configure the enable password **cisco**.
13. Configure the vty password **cisco** for all telnet sessions on the switch.
14. Create **vlan 2** and name it **engineering**.
15. Define the first port on the switch as a trunk link.
16. Define the second and third ports on the switch as access links.
17. Use the **switchport trunk allowed vlan all** command on the first port to allow traffic from all VLANs across the trunk link.
18. Place the second port in vlan 2 using the **switchport access vlan 2** command.
19. Configure port security so that only one MAC address can be learned on the second and third ports.

```
Current configuration:  
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname c2620  
enable password class  
!  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
  
interface FastEthernet0/0 ←  
  ip address 10.10.1.1 255.255.255.0  
  no ip directed-broadcast  
  ip nat inside  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/0.1 ←  
  no ip directed-broadcast  
!  
interface FastEthernet0/0.2  
  encapsulation dot1Q 2  
  ip address 10.10.2.1 255.255.255.0  
  no ip directed-broadcast  
!  
interface Serial0/0  
  ip address 175.16.1.1 255.255.255.0  
  no ip directed-broadcast  
  ip nat outside  
  no ip mroute-cache  
!  
interface Serial0/1  
  no ip address  
  no ip directed-broadcast  
  shutdown  
!  
interface Serial0/2  
  no ip address  
  no ip directed-broadcast  
  shutdown
```

**NOTE:** For IOS versions 12.3 or newer, there will be no IP address on f0/0 if you are using 802.1Q. The IP address will be on f0/0.1 instead and include the **encapsulation dot1Q 1** command.

Figure 13-2 Output of the show run command for the Cisco 2620 router (continued)

**624** Chapter 13 Advanced Switching Concepts

(continued)

```

!
interface Serial0/3
  no ip address
  no ip directed-broadcast
  shutdown
!
ip nat inside source list 1 interface Serial0/0 overload
ip classless
no ip http server
!
access-list 1 permit 10.10.0.0 0.0.255.255
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password cisco
  login
!
end

```

20. Configure the **switchport port-security mac-address sticky** command on ports 2 and 3 so that the single MAC address learned will be made permanent in the switch's RAM.
21. Configure interface vlan1 for the ip address **10.10.1.2 255.255.255.0**.
22. Configure the default gateway for the switch as **10.10.1.1 255.255.255.0**.
23. Configure the VTP mode as transparent.
24. Enter the **show run** command. Your output should resemble the output in Figure 13-3.

```

Current configuration : 1250 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c2950
enable password class

```

**Figure 13-3** Output of the **show run** command on the Cisco 2950 switch (continued)

(continued)

```
!ip subnet-zero
!
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id

vlan 2
  name engineering
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 2
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
!
interface FastEthernet0/3
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
!
interface Vlan1
  ip address 10.10.1.2 255.255.255.0
  no ip route-cache
!
ip default-gateway 10.10.1.1
ip http server
!
line con 0
line vty 0 4
  password cisco
  login
line vty 5 15
  login
!
!
end
```

## 626 Chapter 13 Advanced Switching Concepts

25. Enter the **show vlan** command. Your output should resemble the output in Figure 13-4.

| VLAN Name               | Status    | Ports                                                                                                                                                                             |
|-------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 default               | active    | Fa0/3, Fa0/4, Fa0/5, Fa0/6<br>Fa0/7, Fa0/8, Fa0/9, Fa0/10<br>Fa0/11, Fa0/12, Fa0/13, Fa0/14<br>Fa0/15, Fa0/16, Fa0/17, Fa0/18<br>Fa0/19, Fa0/20, Fa0/21, Fa0/22<br>Fa0/23, Fa0/24 |
| 2 engineering           | active    | Fa0/2                                                                                                                                                                             |
| 1002 fddi-default       | act/unsup |                                                                                                                                                                                   |
| 1003 token-ring-default | act/unsup |                                                                                                                                                                                   |
| 1004 fddinet-default    | act/unsup |                                                                                                                                                                                   |
| 1005 trnet-default      | act/unsup |                                                                                                                                                                                   |

**Figure 13-4** Output of the **show vlan** command on the Cisco 2950 switch

26. Configure the IP addresses, subnet masks, and default gateways for the two workstations, as shown in Figure 13-1.
27. Test your ROAST by pinging from workstation to workstation. If you can ping both ways, you have successfully configured the equipment. If you cannot ping successfully, begin troubleshooting using step 28 as your guide.
28. Check the following:
  - The connected port lights on the router, switch, and workstations should be on. If they are not on, check the cables.
  - Make sure the active interfaces on the router and switch are up. You may need to bring them up with the **no shutdown** command.
  - Check all IP addresses, subnet masks, and default gateways.
  - If you are having a duplexing problem, use the **duplex auto** command on the router Fast Ethernet interface (f0/0).
29. When your configuration is working, demonstrate your ROAST implementation to your instructor.
30. Once your instructor has verified your ROAST implementation, erase the router configuration using the **erase start** command. Erase the switch configuration using the **erase start** command. In addition, enter the **delete flash:vlan.dat** command on the switch in order to erase the VLAN configuration. Finally, delete the IP configuration on the workstations by configuring them to get their IP information automatically.

## Certification Objectives

- Verify network status and switch operation using basic utilities (including ping, traceroute, telnet, SSH, arp, ipconfig, show, and debug commands)
- Identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures
- Configure, verify, and troubleshoot VLANs
- Configure, verify, and troubleshoot inter-VLAN routing
- Configure, verify, and troubleshoot VTP
- Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network
- Implement basic switch security

## Review Questions

1. A switch is LAN equipment. Why, then, is a router necessary to allow computers on VLANs to communicate?
2. What is the purpose of the `switchport port-security mac-address sticky` command?
3. What is the basis for the term “router on a stick”?
4. How are subinterfaces used in the router-on-a-stick configuration?
5. What is the difference between a trunk port and an access port?



## C H A P T E R F O U R T E E N

# NETWORK SECURITY

## Labs included in this chapter

- Lab 14.1 Using the SDM Security Audit Wizard
- Lab 14.2 Create a Router Firewall Using the SDM
- Lab 14.3 Creating VPNs with the SDM

## CCNA Exam Objectives

| Objective                                                                                               | Lab              |
|---------------------------------------------------------------------------------------------------------|------------------|
| Explain general methods to mitigate common security threats to network devices, hosts, and applications | 14.2, 14.3       |
| Describe recommended security practices including initial steps to secure network devices               | 14.1, 14.2, 14.3 |
| Describe VPN technology                                                                                 | 14.3             |

## Lab 14.1 Using the SDM Security Audit Wizard

### Objectives

In Chapter 6, you installed the demo version of Cisco's Security Device Manager (SDM). You learned that SDM is a free utility designed to help you configure a Cisco router without typing in commands using the CLI. You also learned that the primary purpose of SDM is for use in configuring complex security policies. An additional feature of SDM that you will explore in this lab is the Security Audit Wizard. Using this feature allows you to quickly determine the security status of your router. Then you can make necessary adjustments or use the one-step lockdown option, which will apply a list of predefined security settings to the router in one easy step. You will do this lab using the SDM simulator that you installed in Lab 6.6.

After completing this lab you will be able to:

- Use the Security Audit Wizard to gauge the status of the security on a Cisco router
- Secure your router using the Security Audit Wizard

### Materials Required

This lab requires the following:

- The successful completion of Lab 6.6

### Activity

Estimated completion time: **20 minutes**

1. Boot the computer into Windows.
2. Double-click the **Cisco SDM shortcut** on your Desktop to launch the software. Enter **127.0.0.1** as the device IP address and click the check box to **enable HTTPS**. Click the **Launch** button.
3. Click the warning bar in the browser if the content is blocked and then click **Allow Blocked Content** in the popup window to allow blocked content, if necessary. Click the **Yes** button if you get a security warning. You may have to do this step more than once. Click **OK** when the Information window displays.
4. The demo opens. Notice that it provides a fictional Cisco 2801 router with the hostname "2801Router" running version 12.4(6)T of the IOS.
5. Click the **Configure** button and then click the **Security Audit** button in the left pane. Read the Security Audit description and the One-step lockdown description. What is the difference between these two options?

- 
- 
- 
- 
6. Click **Perform security audit** to start the Security Audit Wizard. What four things will the audit do for you?
- 
- 
- 
-

7. Click **Next**. If necessary, click the check boxes to select **FastEthernet0/0** as the inside interface and **FastEthernet0/1** as the outside interface. Click **Next**.
8. Notice that the Security Audit dialog box lists typical security measures and indicates whether or not the router has passed that particular security measure. Click **Close**.
9. Now you are given the option of fixing the security problems listed in the Security Audit. Click the **Fix All** button to select all of the Fix it check boxes, then click **Next**.
10. Enter the password **cannonball**, then re-enter **cannonball** to confirm the new enable secret password. Click **Next** then click **Next** again. A summary of the security features that will be configured on the router is displayed.
11. Click **Finish** and then click **OK** to deliver the commands to the router.
12. Close the SDM.

## Certification Objectives

Objectives for the CCNA exam:

- Describe recommended security practices including initial steps to secure network devices
- Explain general methods to mitigate common security threats to network devices, hosts, and applications

## Review Questions

1. What is the purpose of the Security Audit Wizard?
2. What are the two ways the Security Audit Wizard allows you to fix security problems?
3. What is your opinion regarding using the Security Audit Wizard feature of the SDM?
4. List two appropriate situations in which to use the Security Audit Wizard.

**14**

---

# Lab 14.2 Configure a Router Firewall Using the SDM

## Objectives

In Chapter 9, you used the SDM to configure NAT, DHCP, and DNS. As discussed earlier, using the SDM to configure these items is not typically done, as the parameters are relatively easy to configure using the CLI. However, the SDM is quite helpful when configuring security such as Access Control Lists (ACLs), Virtual Private Networks (VPNs), and firewalls. As you know, the purpose of a firewall is to keep untrusted traffic off of your trusted network. You will see that configuring a firewall on a basic router without SDM requires advanced

**632** Chapter 14 Network Security

knowledge and hundreds of commands typed into the CLI. Conversely, the SDM allows you to create basic and advanced firewalls using the Firewall Policy Wizard with a few clicks of the mouse. You will do this lab using the SDM simulator that you installed in Lab 6.6.

After completing this lab you will be able to:

- Explain the purpose of a firewall
- Configure a basic and advanced firewall using the SDM

## Materials Required

This lab requires the following:

- The successful completion of Lab 6.6

## Activity

|                            |                   |
|----------------------------|-------------------|
| Estimated completion time: | <b>30 minutes</b> |
|----------------------------|-------------------|

1. Boot the computer into Windows.
2. Double-click the **Cisco SDM shortcut** on your Desktop to launch the software. Enter **127.0.0.1** as the device IP address and click the check box to **enable HTTPS**. Click the **Launch** button.
3. Click the warning bar in the browser if the content is blocked and then click **Allow Blocked Content** in the popup window to allow blocked content, if necessary. Click the **Yes** button if you get a security warning. You may have to do this step more than once. Click **OK** when the Information window displays.
4. The demo opens. Click the **Configure** button.
5. Click the **Firewall and ACL** button in the left pane. Basic Firewall should be selected.
6. Click the **Launch the selected task** button and then click **Next**.
7. The Outside (untrusted) interface text box should indicate **FastEthernet0/1**. If necessary, click to select **FastEthernet0/0** for the Inside (trusted) interface, and then click **Next**.
8. Click **Yes**, and then click **OK** to clear the warning dialog box.
9. The Basic Firewall Security Configuration has preconfigured security policies. Move the slider to compare the descriptions of the High Security and Low Security settings. What is the major difference between these settings?
10. Make sure **High Security** is selected and then click **Next**. Your configuration summary is displayed. Notice the number of commands necessary to create the firewall. Click **Finish** to complete the configuration.
11. Click **Merge** to add the existing Access Control List to your new firewall configuration. Click **OK** and then click **Finish** again. *Note:* You may have to click **Finish**, **Merge**, and **OK** more than once.
12. Finally, click **OK** to deliver the commands to the router. Click **OK** again. Your new firewall policy displays.

13. Next, you create an advanced firewall policy. Click the **Create Firewall** tab and select **Advanced Firewall**. Click the **Launch the selected task** button, and then click **Next**.
14. The Advanced Firewall Configuration Wizard launches. As before, the inside (trusted) interface should be FastEthernet0/0. Select **Dialer0** as the outside (untrusted) interface. Note that you could configure a DMZ interface. This option is not available via the Basic Firewall Configuration Wizard. Click **Next**.
15. Click **Yes**, then click **OK** to clear the warning dialog boxes.
16. Notice that the Advanced Firewall Configuration Wizard allows you to create a custom Application Security policy. This is another difference between the Basic and Advanced Firewall Configuration Wizards. Click **Next** to accept the preconfigured High Security setting.
17. Click **Finish** and then click **Merge** to add your new firewall to the security settings already established on the router. You may have to click **Finish**, **Merge**, and **OK** more than once.
18. Click **OK** and then click **OK** again. Your advanced firewall configuration is displayed. Notice that the firewall is composed of access list statements.
19. Close the SDM.

## Certification Objectives

Objectives for the CCNA exam:

- Describe recommended security practices including initial steps to secure network devices

## Review Questions

1. What are the two firewall options presented in the SDM?
2. What are the two differences between the basic and advanced configuration wizards?
3. How do you determine the untrusted interface?
4. How do you determine the trusted interface?
5. In terms of ease of configuration, how does using the SDM to configure a firewall compare to configuration using the CLI?

## Lab 14.3 Creating VPNs with the SDM

### Objectives

In Lab 14.2, you created a basic and an advanced firewall using SDM's Firewall Policy Wizard. Another often used security measure is the virtual private network (VPN). You can think of a VPN as a tunnel; it wraps your data in encryption so that the data can be transported without inspection across unsecured links such as the Internet. Many different types of VPNs are supported by the SDM. These include regular IPSec site-to-site, GRE over IPSec, Dynamic Multipoint VPN, Easy VPN, and WebVPN. In this lab, you will learn about these various types of VPNs and configure an IPSec site-to-site VPN. You will do this lab using the SDM simulator that you installed in Lab 6.6.

After completing this lab you will be able to:

- Explain the purpose of a VPN
- Explain the various types of VPNs
- Configure an IPSec site-to-site VPN using the SDM

### Materials Required

This lab requires the following:

- The successful completion of Lab 6.6

### Activity

Estimated completion time: **30 minutes**

1. Boot the computer into Windows.
2. Double-click the **Cisco SDM shortcut** on your Desktop to launch the software. Enter **127.0.0.1** as the device IP address and click the check box to **enable HTTPS**. Click the **Launch** button.
3. Click the warning bar in the browser if the content is blocked and then click **Allow Blocked Content** in the popup window to allow blocked content, if necessary. Click the **Yes** button if you get a security warning. You may have to do this step more than once. Click **OK** when the Information window displays.
4. The demo opens. Click the **Configure** button and then click the **VPN** button in the left pane.
5. Expand VPN if necessary by clicking on the plus sign next to VPN.
6. Click **Site-to-Site VPN** and observe the Use Case Scenario. Notice that you can create a Site-to-Site VPN or a GRE tunnel VPN. The GRE tunnel allows multicasting so that routing updates (such as those from EIGRP, which use multicasting) can pass across the VPN link.
7. Click **Easy VPN Remote** in the middle pane and observe the Use Case Scenario. This option configures the router to be a VPN client.

8. Click **Easy VPN Server** in the middle pane and observe the Use Case Scenario. This option configures the router to be a VPN server.
9. Click **Dynamic Multipoint VPN** in the middle pane and observe the Use Case Scenario. This option configures the router for VPN when it is part of a hub-and-spoke (star) topology. You can configure the router as a spoke (client) or as a hub (server).
10. Click **WebVPN** in the middle pane and observe the Use Case Scenario. WebVPNs allow access to a LAN using any SSL-enabled Web browser.
11. Now you will configure the router for an IPSec site-to-site VPN. Click **Site-to-Site VPN** in the middle pane. Select **Create a Site to Site VPN** if necessary. Click **Launch the selected task** to start the Site-to-Site VPN wizard.
12. Choose **Quick setup**, if necessary, and then click **Next**.
13. In the **Select the interface for this VPN connection** drop-down list box, choose **FastEthernet0/0**.
14. Select **Peer with a static IP address**, if necessary.
15. Enter **10.10.10.1** as the address of the remote peer.
16. Click the radio button to select Pre-shared keys and enter the key as **cannonball**. Re-enter **cannonball** to confirm the key.
17. Choose **FastEthernet0/0** as the source for encryption and enter the destination IP address as **10.10.10.2** and the subnet mask as **255.255.255.0**. Click **Next** and then click **Yes** to clear the warning dialog box.
18. A summary of the configuration is displayed. What hashing algorithm will be used?  
\_\_\_\_\_ What encryption algorithm will be used?  
\_\_\_\_\_
19. Click **Finish** and then click **OK** to deliver the commands to the router.
20. Click the **Test Tunnel** button and then click the **Start** button. Click **OK** when the test is completed. What important information does the VPN Troubleshooting dialog box display?
21. Click **Close** to close the dialog box, then close the SDM.

14

## Certification Objectives

Objectives for the CCNA exam:

- Explain general methods to mitigate common security threats to network devices, hosts, and applications
- Describe recommended security practices including initial steps to secure network devices
- Describe VPN technology

## Review Questions

1. When would you configure a GRE tunnel?
2. When would you configure a Dynamic Multipoint VPN?
3. What does WebVPN allow you to do that other VPN configurations do not?
4. What hashing algorithm and encryption algorithm does Cisco use for its site-to-site VPN implementation?



# A appendix

## CCNA Certification Objectives

This appendix maps the Cisco CCNA certification objectives with the book chapter in which these objectives are covered. Cisco has assigned the following eight categories of objectives:

- Describe how a network works
- Configure, verify, and troubleshoot a switch with VLANs and interswitch communications
- Implement an IP addressing scheme and IP services to meet network requirements in a medium-size enterprise branch office network
- Configure, verify, and troubleshoot basic router operation and routing on Cisco devices
- Explain and select the appropriate administrative tasks required for a WLAN
- Identify security threats to a network and describe general methods to mitigate those threats
- Implement, verify, and troubleshoot NAT and ACLs in a medium-size enterprise branch office network
- Implement and verify WAN links

**424** Appendix A CCNA Certification Objectives

The following tables, A-1 through A-8, map the objectives of each category to a specific chapter.

| Objective                                                                                            | Chapter      |
|------------------------------------------------------------------------------------------------------|--------------|
| Describe the purpose and functions of various network devices                                        | 2            |
| Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network  | 1, 3         |
| Describe the purpose and basic operation of the protocols in the OSI and TCP models                  | 1, 3         |
| Interpret network diagrams                                                                           | All chapters |
| Describe the components required for network and Internet communications                             | All chapters |
| Select the components required to meet a network specification                                       | All chapters |
| Describe common networked applications including Web applications                                    | 3            |
| Describe the impact of applications (Voice Over IP and Video Over IP) on a network                   | 3            |
| Determine the path between two hosts across a network                                                | 3, 7, 8      |
| Identify and correct common network problems at layers 1, 2, 3, and 7 using a layered model approach | 1, 2, 3      |

**Table A-1** Describe how a network works

| Objective                                                                                                                                        | Chapter   |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts                               | 2, 12, 13 |
| Explain network segmentation and basic traffic management concepts                                                                               | 2, 12     |
| Perform and verify initial switch configuration tasks including remote access management                                                         | 12        |
| Identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures      | 12, 13    |
| Describe how VLANs create logically separate networks and the need for routing between them                                                      | 12, 13    |
| Configure, verify, and troubleshoot trunking on Cisco switches                                                                                   | 13        |
| Configure, verify, and troubleshoot VTP                                                                                                          | 13        |
| Explain the technology and media access control method for Ethernet networks                                                                     | 2         |
| Explain basic switching concepts and the operation of Cisco switches                                                                             | 2, 12     |
| Verify network status and switch operation using basic utilities (including ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands | 12, 13    |
| Describe enhanced switching technologies (including VTP, RSTP, VLAN, PVSTP, 802.1q)                                                              | 13        |
| Configure, verify, and troubleshoot VLANs                                                                                                        | 12, 13    |
| Configure, verify, and troubleshoot interVLAN routing                                                                                            | 13        |
| Configure, verify, and troubleshoot RSTP operation                                                                                               | 13        |
| Implement basic switch security (including port security, trunk access, management vlan other than vlan1, etc.)                                  | 12, 13    |

**Table A-2** Configure, verify, and troubleshoot a switch with VLANs and interswitch communications

| Objective                                                                                                                                      | Chapter |
|------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Describe the operation and benefits of using private and public IP addressing                                                                  | 4       |
| Explain the operation and benefits of using DHCP and DNS                                                                                       | 9       |
| Configure, verify, and troubleshoot DHCP and DNS operation on a router (including CLI/SDM)                                                     | 9       |
| Implement static and dynamic addressing services for hosts in a LAN environment                                                                | 4       |
| Calculate and apply an addressing scheme including VLSM IP addressing design to a network                                                      | 4       |
| Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment | 4       |
| Describe the technological requirements for running IPv6 in conjunction with IPv4 (including protocols, dual stack, tunneling, etc)            | 4       |
| Describe IPv6 addresses                                                                                                                        | 4       |
| Identify and correct common problems associated with IP addressing and host configurations                                                     | 4       |

**Table A-3** Implement an IP addressing scheme and IP services to meet network requirements in a medium-size enterprise branch office network

| Objective                                                                                                         | Chapter      |
|-------------------------------------------------------------------------------------------------------------------|--------------|
| Describe basic routing concepts (including packet forwarding, router lookup process)                              | 5            |
| Describe the operation of Cisco routers (including router bootup process, POST, router components)                | 5, 6         |
| Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts | 5, 6         |
| Configure, verify, and troubleshoot RIPv2                                                                         | 8            |
| Access and utilize the router to set basic parameters (including CLI/SDM)                                         | 5, 6         |
| Connect, configure, and verify operation status of a device interface                                             | 5, 6         |
| Verify device configuration and network connectivity using ping, traceroute, telnet, SSH, or other utilities      | 5, 6         |
| Perform and verify routing configuration tasks for a static or default route given specific routing requirements  | 7            |
| Manage IOS configuration files (including save, edit, upgrade, restore)                                           | 5, 6         |
| Manage Cisco IOS                                                                                                  | 5, 6         |
| Compare and contrast methods of routing and routing protocols                                                     | 7, 8         |
| Configure, verify, and troubleshoot OSPF                                                                          | 8            |
| Configure, verify, and troubleshoot EIGRP                                                                         | 8            |
| Verify network connectivity (including using ping, traceroute, and telnet or SSH)                                 | 6, 7, 8      |
| Troubleshoot routing issues                                                                                       | 6, 7, 8      |
| Verify router hardware and software operation using SHOW & DEBUG commands                                         | 6, 7, 8      |
| Implement basic router security                                                                                   | 5, 6, 10, 14 |

**Table A-4** Configure, verify, and troubleshoot basic router operation and routing on Cisco devices

**426** Appendix A CCNA Certification Objectives

| Objective                                                                                                                   | Chapter |
|-----------------------------------------------------------------------------------------------------------------------------|---------|
| Describe standards associated with wireless media (including IEEE Wi-Fi Alliance, ITU/FCC)                                  | 2       |
| Identify and describe the purpose of the components in a small wireless network (including SSID, BSS, ESS)                  | 2       |
| Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point | 2       |
| Compare and contrast wireless security features and capabilities of WPA security (including open, WEP, WPA-1/2) 1           | 2       |
| Identify common issues with implementing wireless networks (including interface, misconfiguration)                          | 2       |

**Table A-5** Explain and select the appropriate administrative tasks required for a WLAN

| Objective                                                                                                                                      | Chapter |
|------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Describe today's increasing network security threats and explain the need to implement a comprehensive security policy to mitigate the threats | 14      |
| Explain general methods to mitigate common security threats to network devices, hosts, and applications                                        | 14      |
| Describe the functions of common security appliances and applications                                                                          | 14      |
| Describe security-recommended practices including initial steps to secure network devices                                                      | 14      |

**Table A-6** Identify security threats to a network and describe general methods to mitigate those threats

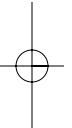
| Objective                                                                                          | Chapter |
|----------------------------------------------------------------------------------------------------|---------|
| Describe the purpose and types of ACLs                                                             | 10      |
| Configure and apply ACLs based on network filtering requirements.(including CLI/SDM)               | 10      |
| Configure and apply an ACLs to limit telnet and SSH access to the router using (including SDM/CLI) | 10      |
| Verify and monitor ACLs in a network environment                                                   | 10      |
| Troubleshoot ACL issues                                                                            | 10      |
| Explain the basic operation of NAT                                                                 | 9       |
| Configure NAT for given network requirements using (including CLI/SDM)                             | 9       |
| Troubleshoot NAT issues                                                                            | 9       |

**Table A-7** Implement, verify, and troubleshoot NAT and ACLs in a medium-size enterprise branch office network

| Objective                                                                          | Chapter |
|------------------------------------------------------------------------------------|---------|
| Describe different methods for connecting to a WAN                                 | 6, 11   |
| Configure and verify a basic WAN serial connection                                 | 6       |
| Configure and verify Frame Relay on Cisco routers                                  | 11      |
| Troubleshoot WAN implementation issues                                             | 6, 11   |
| Describe VPN technology (including importance, benefits, role, impact, components) | 14      |
| Configure and verify a PPP connection between Cisco routers                        | 11      |

**Table A-8** Implement and verify WAN links

A



appendix **B**

## Additional Resources

This appendix contains additional sources for information on subjects covered in this course.

## Internet Resources

Internet resources are invaluable for obtaining information on the latest network news, technology, and standards. The Internet and Web resources listed in this section are divided into the following categories:

- Standards organizations
- Technology reference
- Networking overviews and tutorials
- Technical forums
- Cisco routers
- Exam preparation resources

### Standards Organizations

The following organizations and Web sites provide networking standards discussed in this course:

- American National Standards Institute: [www.ansi.org](http://www.ansi.org)
- Electronic Industries Alliance: [www.eia.org](http://www.eia.org)
- Telecommunications Industry Association: [www.tiaonline.org](http://www.tiaonline.org)
- Institute of Electrical and Electronics Engineers (IEEE): [www.ieee.org](http://www.ieee.org)
- Internet Engineering Task Force (IETF): [www.ietf.org](http://www.ietf.org)
- International Telecommunication Union (ITU): [www.itu.int](http://www.itu.int)
- International Organization for Standardization (ISO): [www.iso.ch](http://www.iso.ch)
- International Electrotechnical Commission (IEC): [www.iec.ch](http://www.iec.ch)
- World Wide Web Consortium (W3C): [www.w3.org](http://www.w3.org)
- RFC Editor: [www.rfc-editor.org](http://www.rfc-editor.org)
- Computer and Communications Standards: [www.cmpcmm.com/cc/standards.html](http://www.cmpcmm.com/cc/standards.html)
- Underwriters Laboratories (UL): [www.ul.com](http://www.ul.com)

### Technology Reference

These Web sites have online definitions for computer and networking terminology:

- Babel: Glossary of Computer Oriented Abbreviations and Acronyms: [www.geocities.com/ikind\\_babel/babel/babel.html](http://www.geocities.com/ikind_babel/babel/babel.html)
- Webopedia: [www.webopedia.com](http://www.webopedia.com)
- Whatis.com: [www.whatis.com](http://www.whatis.com)

## Networking Overviews and Tutorials

An introduction to various networking concepts is provided on the following Web sites:

- Alliance Datacom's Frame Relay tutorial list: [www.alliancedatacom.com/frame-relay-tutorials.htm](http://www.alliancedatacom.com/frame-relay-tutorials.htm)
- Charles Spurgeon's Ethernet Web Site: [www.ethermanage.com/ethernet/ethernet.html](http://www.ethermanage.com/ethernet/ethernet.html)
- InterOperability Lab Tutorials: [www.iol.unh.edu/training](http://www.iol.unh.edu/training)
- WildPackets: [www.wildpackets.com](http://www.wildpackets.com)

## Technical Forums

The following sites contain technical information, discussions, and links to information covered in this course:

- Frame Relay Forum: [www.ipmplsforum.org](http://www.ipmplsforum.org)
- Open Group: [www.opengroup.org](http://www.opengroup.org)
- Protocols.com: [www.protocols.com](http://www.protocols.com)

## Cisco Routers

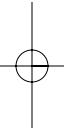
The following locations have information specific to Cisco routers:

- Cisco: [www.cisco.com](http://www.cisco.com)
- Cisco product documentation list: [www.cisco.com/univercd/cc/td/doc/product](http://www.cisco.com/univercd/cc/td/doc/product)
- Cisco command reference documents by subject: [www.cisco.com/univercd/cc/td/doc/product/software/ios100/rpcr/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios100/rpcr/index.htm)

## Exam Preparation Resources

The following Web sites contain information and technical papers concerning the CCNA exam:

- CCPrep.com: [www.ccprep.com](http://www.ccprep.com)
- Certnotes: [www.certnotes.com](http://www.certnotes.com)
- CramSession: [www.cramsession.com](http://www.cramsession.com)
- Transcender: [www.transcender.com](http://www.transcender.com)
- Boson Software: [www.boson.com](http://www.boson.com)





appendix

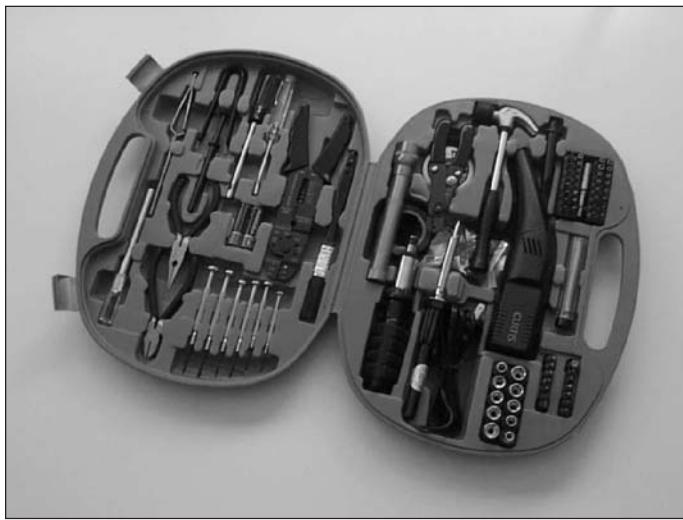
C

## A Networking Professional's Toolkit

This appendix provides pictures of networking tools that you may be using as a network administrator or I.T. team member.

**434** Appendix C A Networking Professional's Toolkit

Throughout this book, you have learned about the many tools you may use while implementing, analyzing, and troubleshooting a network. Although information on networking devices or software packages is readily available, it is not always easy to find details about the tools used by networking professionals. This appendix provides pictures of networking tools, some familiar and some probably unfamiliar, along with their proper names and uses. You can often find these tools together in toolkits with carrying cases. Toolkit providers include Aven Tools, Black Box, Curtis, Paladin, and Siemon.



**Figure C-1** A networking professional's toolkit

Many of the tools used by networking professionals are similar or identical to tools used by electricians. Tools pictured in the following figures fall into this category.



**Figure C-2** Soldering iron, solder, and solder wick; used for repairing connections



**Figure C-3** Pliers; used for bending cable or components or working in tight spaces



**Figure C-4** Screwdriver with several different head types; used for installing and uninstalling components

**436** Appendix C A Networking Professional's Toolkit

**Figure C-5** Hex keyset; used for removing computer covers or components



**Figure C-6** Pocket flashlights; used to illuminate the interior of devices



**Figure C-7** Wire cutters



**Figure C-8** Precision knife

C

**438** Appendix C A Networking Professional's Toolkit

Other tools used by networking professionals are unique to computer repair or telephony technicians. Tools pictured in the following figures fall into this category.



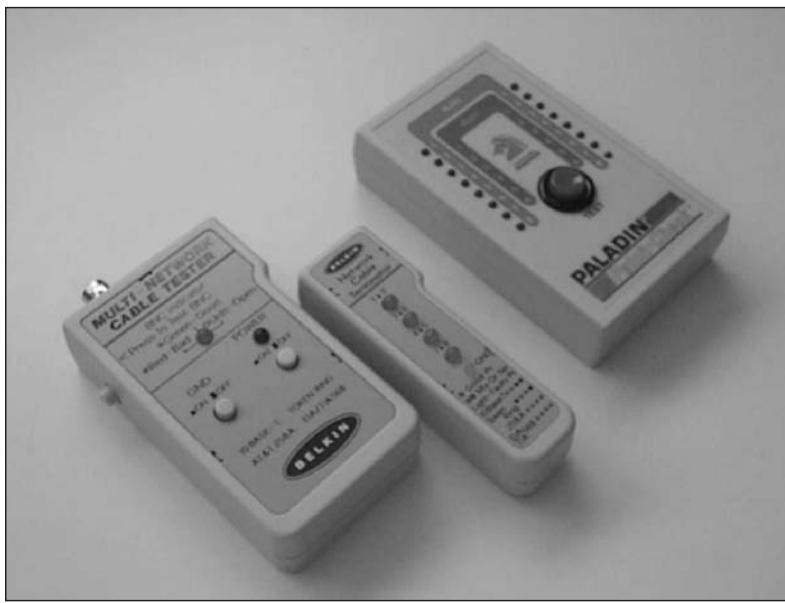
**Figure C-9** Cable preparation tool, including wire stripper and cutter; used for preparing cable for termination



**Figure C-10** Crimp tools; used for crimping wires into terminators



**Figure C-11** Punch-down block tool; used for crimping wires into punch-down blocks



**Figure C-12** Cable testing tools; used for verifying cable integrity

**440** Appendix C A Networking Professional's Toolkit



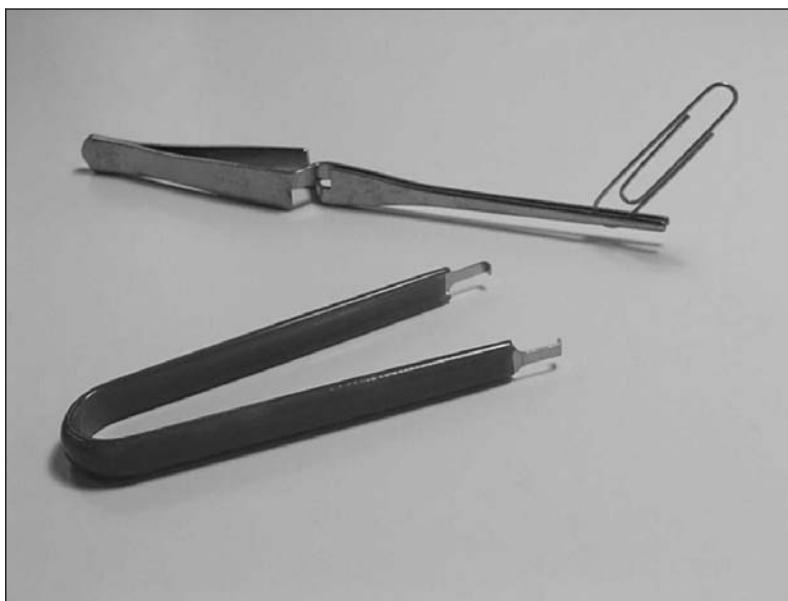
**Figure C-13** Cable ties; used for holding bundles of cables together



**Figure C-14** Magnetic extractor; used for retrieving small components



**Figure C-15** Extractors; used for retrieving small components



**Figure C-16** Tweezers; used for holding and maneuvering small components

**442** Appendix C A Networking Professional's Toolkit

**Figure C-17** Antistatic vacuum; used for cleaning electronic devices



appendix **D**

## Command Summary

This appendix lists the commands presented in this course. You should review these commands before you attempt the CCNA certification examination. The router commands in this appendix are organized into the following categories:

- Identification and navigation
- Passwords
- Router/switch general and startup configuration
- Examining the router and switch
- Interface configuration
- IP-related commands
- Access list configuration and status commands
- WAN configuration
- SWITCH/VLAN configuration

**444** Appendix D Command Summary

The tables in the following sections list the mode, command syntax, and a description of each command. The mode column is abbreviated so you can see the router/switch configuration mode that you must be in to properly execute the command. The following list illustrates the symbols used in the command tables:

- >: Symbolizes user mode, in which the command prompt looks like hostname>
- #: Symbolizes privileged mode, or enable mode, in which the command prompt looks like hostname#
- GC: Indicates global configuration mode, in which the command prompt looks like hostname(config)#
- IF: Indicates interface configuration mode, in which the command prompt looks like hostname(config-if)#
- CL: Indicates line configuration mode, in which the command prompt looks like hostname(config-line)#
- CR: Indicates router configuration mode, in which the command prompt looks like hostname(config-router)#
- CS: Indicates subinterface mode, in which the command prompt looks like hostname(config-subif)#
- CV: Indicates vlan configuration mode, in which the command prompt looks like hostname(vlan)#
- NA: Indicates that the mode is not significant for this command

If multiple symbols are listed in the mode field, the command will work with all modes listed.



**NOTE** This is not a comprehensive guide to all commands and options with which you can configure a router; such a guide would be too large for this appendix. This is an abridged guide that summarizes only the commands covered in this course. To see a larger list of Cisco commands, visit the Cisco Web site at [www.cisco.com/univercd/cc/td/doc/product/software/ios100/rpcr/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios100/rpcr/index.htm).

## Identification and Navigation

The commands shown in Table D-1 are basic navigation commands for the router. These commands allow you to change the router into different configuration modes and even set the identity and clock of the router.

| Mode | Command Syntax     | Description                                                                                                                          |
|------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| >    | enable             | Allows you to access privileged mode from user mode                                                                                  |
| #    | disable            | Returns prompt to user mode from privileged mode                                                                                     |
| #    | configure terminal | Allows you to access global configuration mode                                                                                       |
| GC   | line console 0     | Allows you to configure the console line that is used to access the router; often used to set a console line password; see Table D-2 |

**Table D-1** Identification and navigation commands (continued)

| Mode | Command Syntax                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GC   | line vty [#]                              | Allows you to access line configuration mode for virtual terminal lines; typing line vty 0 4 affects all five virtual terminal lines at the same time; typing a single number (0–4) allows configuration of the virtual terminal number that you entered                                                                                                                                                                                                      |
| GC   | interface [interface type and number]     | Allows you to access interface configuration mode; requires that you enter the type and number of the interface after the command; to configure the first FastEthernet interface on your router, type interface fastethernet 0/0                                                                                                                                                                                                                              |
| GC   | interface [subinterface type and number]  | Allows you to enter subinterface configuration mode; when creating an interface with Frame Relay with this command, add point-to-point or multipoint to the command                                                                                                                                                                                                                                                                                           |
| GC   | router [routing protocol or static]       | Allows you to enter router configuration mode; requires that you specify the name of a routing protocol or indicate static (to indicate a manually configured routing table); to enable RIP routing, for example, type router rip                                                                                                                                                                                                                             |
| GC   | hostname [name]                           | Allows you to set the host name for your router; requires that you enter the name after the hostname command; for example, to name your router "clyde", you would type hostname clyde                                                                                                                                                                                                                                                                         |
| GC   | banner motd [banner end character]        | Allows you to set the message of the day banner; to use this command, type banner motd followed by the single character that you want to end the message; for example, if you type banner motd @, the router prompt will move to the next line, and everything you type following that will be your banner message, until you enter the @ character, which indicates that you are finished typing your banner message; to see your message, reboot the router |
| NA   | Ctrl+Z                                    | Returns you to enable mode; do not press the plus key; press Ctrl+Z                                                                                                                                                                                                                                                                                                                                                                                           |
| #    | clock set [hh:mm:ss month day year]       | Used to set the time and date on the router                                                                                                                                                                                                                                                                                                                                                                                                                   |
| #    | reload [in hh:mm] [month day / day month] | Reboots the router; setting a time delay or month and day for the reboot is optional                                                                                                                                                                                                                                                                                                                                                                          |
| NA   | exit                                      | Logs you out from the > or # prompt; from other prompts, command takes you back one level; for example, typing exit at the router(config-if)# prompt takes you back to the router(config)# prompt                                                                                                                                                                                                                                                             |
| NA   | CTRL+^                                    | Allows you to abort a command in progress; executed by pressing Ctrl+Shift+6                                                                                                                                                                                                                                                                                                                                                                                  |
| > #  | quit                                      | Logs you out of the router                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Passwords

The commands shown in Table D-2 allow you to configure passwords for your router. Do not forget the passwords that you configure; you will need them when you want to access your router in the future.

| Mode | Command Syntax                                | Description                                                                                                                                                       |
|------|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GC   | enable password [password]                    | Allows you to set the privileged mode password, which is used to enter privileged mode                                                                            |
| GC   | enable secret [password]                      | Allows you to set the encrypted privileged mode password; overrides the enable password when configured                                                           |
| CL   | login [ <i>Enter</i> ] password<br>[password] | Allows you to set a line password; requires that you first type login, press the Return or Enter key, then type password followed by the password you want to set |

**Table D-2** Commands for configuring passwords

## Router/Switch General and Startup Configuration

The commands listed in this section are vital to configuring and managing the configuration of the router or switch. These commands cover saving, copying, and replacing the contents of the IOS and the device's configuration file.

| Mode | Command Syntax                                 | Description                                                                                                                                                                                   |
|------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| #    | hostname [host name]                           | Configures the host name of a router or switch                                                                                                                                                |
| #    | copy running-config startup-config             | Copies the running configuration to the NVRAM on the device; saves configuration changes you make while the device is running, so that they are implemented next time the device is restarted |
| #    | copy startup-config running-config             | Copies the device startup configuration from NVRAM to the running configuration. Does not replace the running configuration; instead, it merges the information.                              |
| #    | copy tftp flash                                | Copies a device IOS file from a TFTP server to flash memory                                                                                                                                   |
| #    | copy flash tftp                                | Copies a device IOS file from flash memory to a TFTP server                                                                                                                                   |
| #    | copy tftp startup-config                       | Copies the device configuration file from a TFTP server to the startup configuration in NVRAM on the device                                                                                   |
| #    | copy startup-config tftp                       | Copies the device startup configuration in NVRAM to a TFTP server                                                                                                                             |
| #    | erase flash                                    | Erases the flash memory on the device                                                                                                                                                         |
| #    | erase startup-config                           | Erases the device startup configuration from NVRAM                                                                                                                                            |
| GC   | mac-address-table permanent<br>[mac#] [slot/#] | Maps a permanent MAC address to a switch port                                                                                                                                                 |

**Table D-3** Startup and running configuration commands

## Examining the Router and Switch

The following list of commands allows you to examine router and switch configuration, components, resources, and other statistics. These commands are useful for checking the device's performance and troubleshooting configuration problems.

| Mode | Command Syntax                       | Description                                                                                                                                                                                        |
|------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| > #  | show clock                           | Displays the time and date                                                                                                                                                                         |
| > #  | show processes                       | Displays CPU utilization information                                                                                                                                                               |
| > #  | show interface fastethernet [slot/#] | Shows statistics and configuration information for the FastEthernet interface that is listed; requires that you enter the number of the interface after the command                                |
| > #  | show interface serial [slot/#]       | Shows statistics and configuration information for the serial interface that is listed; requires that you enter the number of the interface after the command                                      |
| > #  | show interfaces                      | Lists configuration and statistics for all interfaces configured on the device                                                                                                                     |
| > #  | show protocol                        | Shows the protocols configured on the system and indicates which interfaces are using them                                                                                                         |
| > #  | show history                         | Displays the last 10 commands executed                                                                                                                                                             |
| > #  | show flash                           | Shows the flash file(s), size, name, and the amount of flash memory used, total, and available                                                                                                     |
| > #  | show cdp neighbor                    | Shows a list of Cisco devices that are directly attached to this device                                                                                                                            |
| > #  | show cdp neighbor detail             | Adds IP address information to output obtained from show cdp neighbor command                                                                                                                      |
| #    | show running-config                  | Displays the currently running device configuration file                                                                                                                                           |
| #    | show startup-config                  | Displays the device startup configuration maintained in NVRAM                                                                                                                                      |
| > #  | show version                         | Displays version information for the router/switch. This includes the startup register setting, the router series number, how long the router has been up and running, and the IOS version number. |

**Table D-4** Commands for examining components and configuration

## Interface Configuration

Interfaces are an important part of the router, and Table D-5 lists commands that are specific to interface configuration. Table D-8 lists additional interface configuration commands related to WAN configuration.

**448** Appendix D Command Summary

| Mode | Command Syntax                                    | Description                                                                                                                                                                                                   |
|------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GC   | interface serial [slot/#]                         | Allows you to configure the specific serial interface that you identify                                                                                                                                       |
| GC   | interface fastethernet [slot/#]                   | Allows you to configure the specific FastEthernet interface on a router that you specify                                                                                                                      |
| IF   | encapsulation [encapsulation type]                | Allows you to set the encapsulation type for your interface                                                                                                                                                   |
| GC   | cdp run                                           | Allows you to enable the Cisco Discovery Protocol on a device                                                                                                                                                 |
| GC   | no cdp run                                        | Allows you to disable the Cisco Discovery Protocol on a device                                                                                                                                                |
| IF   | cdp enable                                        | Allows you to enable the Cisco Discovery Protocol on an interface                                                                                                                                             |
| IF   | no cdp enable                                     | Allows you to disable the Cisco Discovery Protocol on an interface                                                                                                                                            |
| IF   | description [description]                         | Allows you to configure a description for an interface                                                                                                                                                        |
| IF   | duplex [mode]                                     | Sets the duplex type on an interface (auto, full, full-flow-control, half)                                                                                                                                    |
| IF   | no shutdown                                       | Tells the router or switch not to shut down the interface; leave enabled                                                                                                                                      |
| IF   | loopback                                          | Allows you to configure the interface for loopback that is used for testing purposes; information transmitted out of the interface will be immediately returned on the receive circuit of that same interface |
| GC   | interface [interface slot #/.subinterface slot/#] | Creates and/or accesses a subinterface; for example, to create a subinterface #1 off S0/1, type interface s0/1.1                                                                                              |

**Table D-5** Interface configuration commands

---

## IP Commands

The commands in Table D-6 are related to the configuration, control, and troubleshooting of TCP/IP. They cover configuring an IP address and subnet mask, in addition to configuring routing protocols.

| Mode | Command Syntax                 | Description                                                          |
|------|--------------------------------|----------------------------------------------------------------------|
| IF   | ip address [ip address] [mask] | Sets the IP address and subnet mask for an interface on a router     |
| GC   | ip address [ip address] [mask] | Sets the IP address and the subnet mask for an interface on a switch |

**Table D-6** IP-related commands (*continued*)

| Mode  | Command Syntax                                 | Description                                                                                                                                                                                                     |
|-------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GC    | ip default-gateway [ip address]                | Sets the default gateway for an interface on a switch                                                                                                                                                           |
| IF CS | ip unnumbered [interface or logical interface] | Allows you to establish that the interface is to support the IP protocol, but not be assigned an IP address                                                                                                     |
| GC    | router rip                                     | Enables RIP routing and accesses router configuration mode                                                                                                                                                      |
| CR    | version 2                                      | Enables RIP version 2 when used after the <code>router rip</code> command                                                                                                                                       |
| CR    | network [major network number]                 | Used after <code>router rip</code> to indicate network number                                                                                                                                                   |
| GC    | router eigrp [autonomous system number]        | Enables EIGRP routing and accesses router configuration mode; requires that you enter an autonomous system number                                                                                               |
| CR    | network [major network number]                 | Used after <code>router eigrp</code> to indicate network number                                                                                                                                                 |
| GC    | router ospf [process id]                       | Enables OSPF routing and accesses router configuration mode; requires a process ID number that is only relevant on the local router                                                                             |
| CR    | network [ip address] [wildcard]                | Indicates the interface that participates in OSPF. The wildcard mask is a reversed subnet mask and is unique to identify interfaces for OSPF.                                                                   |
| GC    | no ip routing                                  | Disables IP routing on the router                                                                                                                                                                               |
| GC    | ip routing                                     | Enables IP routing on the router                                                                                                                                                                                |
| CR    | passive-interface                              | Enables the suppression of routing updates over some interfaces while allowing updates to be exchanged normally over other interfaces                                                                           |
| #     | debug ip rip                                   | Enables RIP debugging, which allows you to monitor RIP updates                                                                                                                                                  |
| #     | no debug all                                   | Disables all debugging activities                                                                                                                                                                               |
| #     | debug all                                      | Enables all debugging options                                                                                                                                                                                   |
| #     | undebug all                                    | Disables all debugging activities                                                                                                                                                                               |
| > #   | show ip route                                  | Displays the router's routing table                                                                                                                                                                             |
| > #   | ping [ip address / host name]                  | Allows you to verify that a host is reachable either by IP address or host name                                                                                                                                 |
| > #   | telnet [ip address]                            | Allows the user to start a telnet session with a telnet server                                                                                                                                                  |
| > #   | show ip protocol                               | Shows statistics for the IP protocol, such as routing protocol information, timers, networks serviced, and gateway information                                                                                  |
| > #   | show ip interfaces [interface type and number] | Shows statistics for interfaces configured for IP; adding the specific interface type and number is optional; if you only type <code>show ip interface</code> , all interfaces configured with IP will be shown |

## Access Lists

Access lists allow you to control the types of packets that are allowed to traverse the router. Table D-7 illustrates the commands for IP access list creation and configuration.

| Mode | Command Syntax                                                                                                                                                                            | Description                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| GC   | access-list [list #] [permit   deny] [ip address] [mask]                                                                                                                                  | Creates a standard IP access list                                                                                             |
| GC   | access-list [list #] [permit   deny] [protocol] [source IP address] [source wildcard mask] [operator] [port] [destination IP address] [destination wildcard mask] [operator] [port] [log] | Creates an extended IP access list                                                                                            |
| GC   | no access-list [list #]                                                                                                                                                                   | Removes the access list indicated                                                                                             |
| GC   | ip access-list [standard/extended] [name]                                                                                                                                                 | Creates a named access list (IOS 11.2 or higher)                                                                              |
| IF   | ip access-group [list number/name] [in / out]                                                                                                                                             | Applies an IP access list to the interface                                                                                    |
| IF   | no ip access-group [list #] [in / out]                                                                                                                                                    | Removes an IP access list from the interface                                                                                  |
| CL   | access-class [access-list #] [in/out]                                                                                                                                                     | Links an existing access list to VTY lines                                                                                    |
| #    | show ip access-lists                                                                                                                                                                      | Shows all IP access lists                                                                                                     |
| #    | show access-list [list #]                                                                                                                                                                 | Allows you to review all access lists; you can enter the access list number you want to view instead of reviewing all of them |

**Table D-7** Access list configuration and status commands

## WAN Configuration

The following commands in Table D-8 cover the WAN configuration techniques mentioned in this course. These commands allow you to configure PPP and Frame Relay interfaces.

| Mode     | Command Syntax          | Description                                                                  |
|----------|-------------------------|------------------------------------------------------------------------------|
| IF<br>CS | bandwidth [bandwidth]   | Sets the bandwidth advertised on the serial interface in kilobits per second |
| IF       | clock rate [clock rate] | Sets the clock rate in bits per second for a serial interface                |

**Table D-8** WAN configuration commands (continued)

| Mode  | Command Syntax                         | Description                                                                                                                                                                                            |
|-------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IF CS | encapsulation<br>[WAN protocol]        | Sets the encapsulation type for a serial interface; common options are PPP, Frame Relay, and HDLC; for example, to set the interface to PPP encapsulation, type encapsulation ppp                      |
| IF CS | ppp authentication<br>[chap / pap]     | Sets the authentication type for ppp encapsulation; can be chap or pap; if both pap and chap are used, the order in which they are entered on the command line is the order in which they will be used |
| IF CS | frame-relay interface-dlci<br>[dlci #] | Configures a DLCI number for a serial interface using Frame Relay encapsulation                                                                                                                        |
| IF CS | frame-relay lmi-type<br>[lmi-type]     | Sets the LMI type for a Frame Relay interface; options are cisco, q933i, and ansi                                                                                                                      |
| #     | show frame-relay lmi                   | Allows you to view configuration and interface statistics concerning your Frame Relay interfaces using LMI; also shows LMI type                                                                        |
| #     | show frame-relay map                   | Displays the Frame Relay map                                                                                                                                                                           |

## SWITCH/VLAN Configuration

The following commands in Table D-9 cover the VLAN configuration techniques mentioned in this course. These commands work only on VLAN-enabled devices and assume configuration via a Cisco Catalyst 1900.

| Mode | Command Syntax                               | Description                                                                                 |
|------|----------------------------------------------|---------------------------------------------------------------------------------------------|
| #    | show vlan [#]                                | Shows the VLAN configuration of the switch. It can be specific to a particular VLAN number. |
| #    | show vtp status                              | Shows vtp status of the various VLANs                                                       |
| #    | show mac-address-table                       | Shows the port to mac address assignments                                                   |
| GC   | interface range<br>[interface slot/#-slot/#] | Allows you to configure more than one interface at a time                                   |
| CS   | encapsulation<br>[isl/dot1q] [#]             | Configures the trunking protocol (isl or dot1q) for a particular vlan                       |
| IF   | switchport access vlan [#]                   | Assigns a port to a specific VLAN                                                           |
| IF   | switchport mode access                       | Configures the port for normal switching                                                    |
| IF   | switchport mode trunk                        | Configures the port to forward traffic from multiple VLANs                                  |
| IF   | switchport trunk allowed<br>vlan [#]         | Tells the port which vlans can be forwarded over the link                                   |

**Table D-9** VLAN configuration commands (continued)

## 452 Appendix D Command Summary

| Mode | Command Syntax                                                 | Description                                                                                                                                          |
|------|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| #    | vlan database                                                  | Enters VLAN configuration mode                                                                                                                       |
| CV   | vtp password [word]                                            | Sets the VTP password for a domain                                                                                                                   |
| CV   | vtp server                                                     | Sets the current device as a VTP server                                                                                                              |
| CV   | vtp client                                                     | Configures the current device as a VTP client                                                                                                        |
| CV   | vtp transparent                                                | Sets the current device in VTP transparent mode                                                                                                      |
| CV   | vtp domain                                                     | Sets the VTP domain name                                                                                                                             |
| CV   | vtp pruning [enable/disable]                                   | Enables or disables VTP pruning                                                                                                                      |
| CV   | vlan [#] name [name]                                           | Configures the name of the specified VLAN number                                                                                                     |
| GC   | interface vlan 1                                               | Enters interface configuration mode for vlan 1, which is where you would configure an IP address                                                     |
| IF   | switchport port-security mac-address [address]                 | Assigns a particular MAC address to a port so that no other MAC address is allowed to use that port                                                  |
| IF   | switchport port-security maximum [#]                           | Tells the port it can only learn up to a certain number of MAC addresses                                                                             |
| IF   | switchport port-security mac-address sticky                    | Dynamically learned MAC addresses that are saved with the switch configuration so that they do not need to be relearned when the switch is restarted |
| IF   | switchport port-security violation [protect/restrict/shutdown] | Tells the port what to do in the event of a security violation                                                                                       |
| GC   | spanning-tree priority [#]                                     | Set the priority to 0 to make the switch the root bridge                                                                                             |
| GC   | spanning-tree vlan 1 priority [#]                              | Set the priority for a specific vlan                                                                                                                 |
| #    | show spanning-tree                                             | Shows the spanning tree particulars and status                                                                                                       |
| IF   | spanning-tree portfast                                         | Use the portfast option on this interface                                                                                                            |

appendix

E

## Troubleshooting Summary

This appendix lists router and switch commands that help you troubleshoot your network.

**454** Appendix E Troubleshooting Summary

The tables in this appendix list the mode, command syntax, and description of each troubleshooting command. The mode column indicates the configuration mode you must be in to properly execute the command. The symbols used in the mode columns are as follows:

- >: Symbolizes user mode, in which the command prompt looks like `hostname>`
- #: Symbolizes privileged mode, or enable mode, in which the command prompt looks like `hostname#`

If both symbols are shown in the mode field, the command works with both modes.



This is not a comprehensive guide to all commands and options you can use to troubleshoot a router or switch; such a guide would be too large for this appendix. This abridged guide summarizes only the commands covered in this course. To see a larger list of Cisco commands, visit the Cisco Web site at [www.cisco.com/univercd/cc/td/doc/product/software/ios100/rpcr/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios100/rpcr/index.htm).

## Router Troubleshooting Commands

The show and debug commands in Table E-1 are used on routers to help troubleshoot connectivity and correct operation. When possible, the table lists a figure in this book that shows this command in use.

| Mode | Command                               | Use                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Corresponding Figure      |
|------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| >, # | <code>ping [host/ip address]</code>   | Sends five ICMP echo requests to the specified host or IP address to ensure connectivity. If there are no replies, then your connection is not viable.                                                                                                                                                                                                                                                                                                                         |                           |
| #    | <code>ping</code>                     | When a normal ping command is sent from a router, the source address of the ping is the IP address of the interface that the packet uses to exit the router. If an extended ping command is used, the source IP address can be changed to any IP address on the router. The extended ping is used to perform a more advanced check of host "reachability" and network connectivity. To use extended ping, simply enter the ping command in privileged mode with no parameters. | Figure E-1                |
| #    | <code>telnet [host/ip address]</code> | Creates a telnet connection to a host or IP address and allows you to remotely administer that device.                                                                                                                                                                                                                                                                                                                                                                         |                           |
| #    | <code>show running-config</code>      | Shows the current running configuration in RAM, which is useful for determining existing settings on your router.                                                                                                                                                                                                                                                                                                                                                              | Figure 5-7<br>Figure 5-16 |
| #    | <code>show version</code>             | Shows the IOS version currently operating on your device. Also provides configuration register settings that can help in password recovery.                                                                                                                                                                                                                                                                                                                                    | Figure 5-15<br>Figure 6-7 |

**Table E-1** Router troubleshooting commands (*continued*)

| Mode | Command                            | Use                                                                                                                                                                                                                                                                                                                                                                                         | Corresponding Figure                      |
|------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| #    | show interfaces [type] [slot/#]    | Provides details about the physical or logical interfaces on a router, including IP address, bandwidth settings, duplex settings (Eth), clock rate (serial), and more. It also shows the status of the interface, both Physical layer and Data Link layer.                                                                                                                                  | Figure 5-17<br>Figure 6-2<br>Figure 11-21 |
| #    | show flash                         | Shows all current IOS images and configurations saved in flash memory, and indicates whether you have enough memory to store multiple copies of the IOS.                                                                                                                                                                                                                                    | Figure 6-6                                |
| #    | show cdp neighbor                  | Shows an overview of all directly connected Cisco devices, regardless of their Layer 3 address (e.g., IPX, IP, AppleTalk).                                                                                                                                                                                                                                                                  | Figure 6-4                                |
| #    | show cdp neighbor detail           | Shows neighbor device ID, Layer 3 protocol information (for example, IP addresses), device platform, device capabilities, local interface type and outgoing remote port ID, hold-time value (in seconds), Cisco IOS software type, and release. The output from this command includes all the Layer 3 addresses of the neighbor device interfaces (up to one Layer 3 address per protocol). |                                           |
| #    | show ip protocol                   | Shows values about all routing protocols and routing protocol timer information associated with the router on which you issue this command (for example, which networks are being advertised by which protocols, such as RIP, EIGRP, and OSPF).                                                                                                                                             | Figure 7-13                               |
| #    | show ip route                      | Displays the contents of the IP routing table.                                                                                                                                                                                                                                                                                                                                              | Figure 7-15<br>Figure 7-16<br>Figure 8-21 |
| #    | show ip interface [type] [slot/#]  | Shows IP-related information about a particular interface, including the assigned IP address, whether any ACLs are set, whether the interface is up or down, and what type of IP switching is enabled.                                                                                                                                                                                      | Figure 10-12<br>Figure 10-16              |
| #    | show access-lists                  | Shows all standard and extended access lists, as well as the statements (in order) included in each list.                                                                                                                                                                                                                                                                                   | Figure 10-11<br>Figure 10-16              |
| #    | show ip access-lists               | Shows only IP standard and extended access lists, as well as the statements (in order) included in each list.                                                                                                                                                                                                                                                                               | Figure 10-11<br>Figure 10-23              |
| #    | show frame-relay pvc [dlci number] | Displays the status of all PVCs or a specified PVC. This command is useful for viewing the number of BECN and FECN packets received by the router. It also shows whether a PVC is active, inactive, or deleted.                                                                                                                                                                             | Figure 11-22                              |
| #    | show frame-relay map               | Displays the current map entries and information about the connections. This command is useful for discovering a DLCI and its associated remote IP address. This is either discovered dynamically via inverse ARP or by a static entry.                                                                                                                                                     | Figure 11-23                              |
| #    | show history                       | Shows all recent commands that have been issued in the IOS CLI. The default is to buffer 10 commands, but you can show up to 256.                                                                                                                                                                                                                                                           |                                           |

(continued)

**456** Appendix E Troubleshooting Summary

| Mode | Command              | Use                                                                                                           | Corresponding Figure |
|------|----------------------|---------------------------------------------------------------------------------------------------------------|----------------------|
| #    | show starting-config | Shows the saved configuration in NVRAM. This configuration is loaded by default when a router restarts.       |                      |
| #    | show frame-relay lmi | Displays LMI traffic statistics and specifies which type of LMI is being used (Cisco, ANSI, or Q.933a).       | Figure 11-24         |
| #    | debug all            | Turns on debugging for all processes running on your router. (Warning: Never do this on a production router!) | Figure 6-3           |
| #    | debug ip rip         | Turns on debugging for all RIP events, such as periodic updates and triggered updates.                        |                      |

```

Router A#ping
Protocol [ip]:
Target IP address: 192.168.40.1

!---- The address to ping.

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.23.2

!---Ping packets will be sourced from this address.

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.
Sending 5, 100-byte ICMP Echos to 162.108.21.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms

!--- Ping is successful.

Router A#

```

**Figure E-1** Ping command output

## Switch Troubleshooting Commands

The show commands in Table E-2 are used on switches to help troubleshoot connectivity and correct operation. Note that there are some differences from routers, as Access Catalyst switches from Cisco deal primarily with Layer 2 of the OSI model.

| Mode | Command                | Use                                                                                                                                                                                                                                           | Corresponding Figure |
|------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| #    | show mac-address-table | Shows all currently learned MAC addresses in the CAM (content addressable memory) table. These are either learned dynamically by the switch or entered permanently with the mac-address-table permanent command in global configuration mode. | Figure E-2           |
| #    | show port-security     | Shows the port security settings for the switch and its ports                                                                                                                                                                                 |                      |
| #    | show spanning-tree     | Displays the spanning tree state information                                                                                                                                                                                                  |                      |
| #    | show vlan [number]     | Shows information about VLANs that are configured on the switch. The command can also specify a particular VLAN.                                                                                                                              | Figure E-3           |
| #    | show vtp               | Shows general information about the VLAN trunking protocol                                                                                                                                                                                    | Figure E-4           |

**Table E-2** Switch troubleshooting commands

```
wg_sw_1900#show mac-address-table
Number of permanent addresses : 0
Number of restricted static addresses : 0
Number of dynamic addresses : 6

Address          Dest           Interface  Type   Source Interface List
-----
00E0.1E5D.AE2F  Ethernet      0/2        Dynamic  A11
00D0.588F.B604  FastEthernet  0/26       Dynamic  A11
00E0.1E5D.AE2B  FastEthernet  0/26       Dynamic  A11
0090.273B.87A4  FastEthernet  0/26       Dynamic  A11
00D0.588F.B600  FastEthernet  0/26       Dynamic  A11
00D0.5892.38C4  FastEthernet  0/27       Dynamic  A11
```

**Figure E-2** show mac-address-table command output

| VLAN Name             | Status    | Ports           |      |        |        |          |      |        |        |
|-----------------------|-----------|-----------------|------|--------|--------|----------|------|--------|--------|
| 1 default             | Enabled   | 1-12, AUI, A, B |      |        |        |          |      |        |        |
| 10 Engineering        | Enabled   |                 |      |        |        |          |      |        |        |
| 20 HR                 | Enabled   |                 |      |        |        |          |      |        |        |
| 30 Sales              | Enabled   |                 |      |        |        |          |      |        |        |
| 40 Marketing          | Enabled   |                 |      |        |        |          |      |        |        |
| 1002 fddi-default     | Suspended |                 |      |        |        |          |      |        |        |
| 1003 token-ring-defau | Suspended |                 |      |        |        |          |      |        |        |
| 1004 fddinet-default  | Suspended |                 |      |        |        |          |      |        |        |
| 1005 trnet-default    | Suspended |                 |      |        |        |          |      |        |        |
| VLAN                  | Type      | SAID            | MTU  | Parent | RingNo | BridgeNo | Stp  | Trans1 | Trans2 |
| 1                     | Ethernet  | 100001          | 1500 | 0      | 0      | 0        | Unkn | 1002   | 1003   |
| 10                    | Ethernet  | 100010          | 1500 | 0      | 1      | 1        | Unkn | 0      | 0      |
| 20                    | Ethernet  | 100020          | 1500 | 0      | 1      | 1        | Unkn | 0      | 0      |
| 30                    | Ethernet  | 100030          | 1500 | 0      | 1      | 1        | Unkn | 0      | 0      |
| 40                    | Ethernet  | 100040          | 1500 | 0      | 1      | 1        | Unkn | 0      | 0      |

--More--

**Figure E-3** show vlan command output

**458 Appendix E Troubleshooting Summary**

```
VLAN1 is executing the IEEE compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, address 0001.961D.6B40
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32768, address 0001.961D.6B40
Root port is N/A, cost of root path is 0
Topology change flag not set, detected flag not set
Topology changes 0, last topology change occurred 0d00h00m00s ago
Times: hold 1, topology change 8960
      hello 2, max age 20, forward delay 15
Timers: hello 2, topology change 35, notification 2
Port Ethernet 0/1 of VLAN1 is Forwarding
Port path cost 100, Port priority 128
Designated root has priority 32768, address 0001.961D.6B40
Designated bridge has priority 32768, address 0001.961D.6B40
Designated port is 1, path cost 0
Timers: message age 20, forward delay 15, hold 1
Port Ethernet 0/2 of VLAN1 is Forwarding
Port path cost 100, Port priority 128
Designated root has priority 32768, address 0001.961D.6B40
Designated bridge has priority 32768, address 0001.961D.6B40
Designated port is 2, path cost 0
Timers: message age 20, forward delay 15, hold 1
--More--
```

**Figure E-4** show vtp command output

---

## Using Troubleshooting Commands

When using show and debug commands, it is important to know the difference between the two. The show commands create a snapshot of a particular process or device configuration. By contrast, the debug commands are like Web cameras that constantly monitor the processes and activities you specify.

Typically, you use show commands on production routers and switches, as they are low in CPU and memory utilization. These commands usually provide information you need to know about a particular issue. On the other hand, if a problem is sporadic or only occurs at certain times during a process, then debug commands will serve you well; you can constantly monitor (and log) events as they occur.

You must be careful with debug commands. Because they use CPU and memory, having too many debug processes running at the same time can affect the performance of a router or switch. A good example is Network Address Translation (NAT) debugging. Because every packet that goes through the router must be translated if it goes outside the network interface, you will be processing a message for each packet. This can not only double your CPU utilization, it will also overwhelm a person monitoring these events. You could also overflow your memory if you have logging enabled.

Always remember to turn debugging off. For example, you can use the no debug [process] command, where [process] is the process you started. The best practice is to use the no debug all command or u all, which is a shortcut for undebug all. These commands turn off all possible debugging on a device.

---

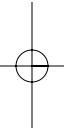
## Troubleshooting Example

Suppose you receive a call at the Help desk from a user who can no longer access her file server. You walk to her desk and ask if she has changed anything on her computer. She says no. You open a command prompt and type ping fileserver1. The computer responds “Destination unreachable”. You suspect a routing problem, because you added a new router on her floor over the weekend. You thank the user, walk into your router closet with your laptop, and plug into the new router.

Because you have a small network, you are using RIPv2 as your routing protocol. You log in to the router, go to the privileged mode prompt, and type `show ip protocols` to see the list of routing protocols running on the router. You notice that RIPv2 is running, but there are no networks being advertised. You then issue the `show ip route` command, which shows that you know only the directly connected routes.

You deduce that someone forgot to use the `network` command to identify the interfaces that would be advertising and using RIPv2. You quickly enter router configuration mode and type the two `network` statements that identify the two directly connected networks. You exit the configuration modes by typing `end`.

Back in privileged mode, you type `show ip protocols` again and notice that the router is now advertising on those routes. You then type `show ip route` and notice that four new routes have appeared with R's next to them, identifying them as RIP learned routes. You call the user, who gives you the good news that she can now see the file server and download the files she needs.



# Index

## A

AAA (Authentication, Authorization, and Accounting) model, 397  
 access control lists (ACLs), creating using SDM, 280–285  
 Access layer, Cisco Three-Layer Hierarchical model, 77  
 access lists, 259–296, 378. *See also* access control lists (ACLs)  
     commands, 450  
     controlling VTY line access, 279–280  
     extended IP access lists, 273–278  
     extended, lab, 584–587  
     labs, 579–590  
     names, 279  
     names, lab, 588–590  
     problems, 261–262  
     rules, 262–264  
     standard IP access lists, 265–273  
     usage, 260–261  
 access rate, Frame Relay, 316  
 ACLs (access control lists), creating using SDM, 280–285  
 active hubs, 27  
 ad hoc mode, 30  
 adaptive cut-through, 351  
 Address Resolution Protocol (ARP), 63–66  
     ARP cache life, 65–66  
     ARP request frames, 65  
     ARP requests, 64

ARP tables, 63, 67–68

IP and MAC header information in ARP request and reply, lab, 486–488

RARP compared, 67

adjacencies database, OSPF, 223

administrative distance, 183  
     changing, 188–189

Advance Research Projects Agency (ARPA), 54

Advance Research Projects Agency Network (ARPANET), 54

Advanced Firewall Configuration Wizard, 286

AES, 402

AH (Authentication Header), 401–402

alignment errors, 341

American Registry of Internet Numbers (ARIN), 89

amplifiers, 26

analog computers, 26

antistatic vacuum, 442

any keyword, 269

AppleTalk Control Protocol (ATCP), 302

Application layer

    OSI (layer 7), 7, 13

    TCP/IP, 55–56

areas, OSPF, 223–224

ARIN (American Registry of Internet Numbers), 89

ARP. *See* Address Resolution Protocol (ARP)

    ARP cache life, 65–66

ARP replies, 65

IP and MAC header information, lab, 486–488

ARP request(s), 64

IP and MAC header information, lab, 486–488

ARP request frames, 65

ARP tables, 63, 67–68

ARPA (Advance Research Projects Agency), 54

ARPANET (Advance Research Projects Agency Network), 54

AS(s) (autonomous systems), 175

ASCII, 12

asymmetric key encryption, 396

asymmetric switching, 348

ATCP (AppleTalk Control Protocol), 302

attenuation, 26

authentication, 397

    IPSEC protocols, 402

    OSPF, 228–230

    PPP, configuring, 306–308

Authentication, Authorization, and Accounting (AAA) model, 397

Authentication Header (AH), 401–402

autonomous systems (ASs), 175

AUX line password, 125

auxiliary ports (AUXs), 118

## B

backing up, CDP, 160–161

backoff periods, 40, 338

**638** Index

- backup designated routers (BDRs), 224, 225
- backward explicit congestion notification (BECN), 317
- bandwidth, switched, 346
- Basic Firewall Configuration Wizard, 286, 287–295
- Basic Service Set (BSS), 30
- bastion hosts, 393
- BDRs (backup designated routers), 224, 225
- BECN (backward explicit congestion notification), 317
- Berkeley Software Distribution UNIX (BSD UNIX), 54
- BGP (Border Gateway Protocol), 176
- BIA (Burned in Address), 10
- binary numbers, conversion to hexadecimal and decimal numbers, 106–107
- lab, 504–506
- bit time, 340
- blocking state, switch ports, 368
- BMP, 12
- boot system commands
- CDP, 160
  - lab, 539–542
- boot-sector viruses, 392
- bootstrap program, 132
- Border Gateway Protocol (BGP), 176
- BPDUs (bridge protocol data units), 367
- bridge(s), 33–35
- advantages and disadvantages, 35
  - connecting networks, lab, 474–475
- LAN segmentation, 344–345
- multiport, 346
- operation, lab, 477–478
- root, 367
- source-routing, 34–35
- switches versus, lab, 478–481
- translation, 35
- transparent, 34
- bridge protocol data units (BPDUs), 367
- bridging tables, 345
- broadcast(s), 339
- directed, 95
  - flooded, 95
- broadcast domains, 38
- broadcast frames, 33
- broadcast storms, 35, 339
- brouters, 39–40
- operation, lab, 477–478
- BSD UNIX (Berkeley Software Distribution UNIX), 54
- BSS (Basic Service Set), 30
- buffer(s), 62
- buffering, 62
- Burned in Address (BIA), 10
- C**
- cable, fiber-optic, 2
- cable preparation tool, 438
- cable testing tools, 439
- cable ties, 440
- CAM (content-addressable memory), 348
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD), 10, 30, 40–41
- collision domains, 41
- collisions, 40
- Ethernet, 338–339
- carrier signals, 40, 338
- CBPDU (configuration bridge protocol data units), 367
- CBS (Committed Burst Size), Frame Relay, 316
- CCIT (Consultative Committee on International Telephony and Telegraphy), 308
- CCNA certification objectives, 423–427
- CDP (Cisco Discovery Protocol), 155–156
- cdp command, lab, 535–539
- Challenge Handshake Authentication Protocol (CHAP), 304, 397
- configuring PPP, lab, 592–595
- channel service unit/data service unit (CSU/DSU), 309
- CHAP. *See* Challenge Handshake Authentication Protocol (CHAP)
- checking interfaces, routers, 152–155
- clearing counters, 154
  - debugging, 154–155
- CIDR (Classless Inter-Domain Routing), 101
- CIR (Committed Information Rate), Frame Relay, 316
- Cisco Discovery Protocol (CDP), 155–156
- Cisco Internetwork Operating System (IOS), 118–132, 156–161
- backing up and restoring, 160–161
- command history, 130

- configuration modes, 123–125  
configuration register, 156–158  
configuring router identification, 130–132  
connecting via terminal programs, 120  
enhanced editing, 129–130  
passwords, 125–129  
ROM Monitor mode, 158  
RxBoot mode, 159–160  
system configuration dialog, 121  
upgrading, 161  
user interface, 121–123
- Cisco routers, Internet resources, 431  
Cisco Security Audit Wizard, 410–415  
Cisco Security Device Manager (SDM). *See* Security Device Manager (SDM)  
Cisco Three-Layer Hierarchical model, 76–78  
    Access layer, 77  
    Core layer, 77–78  
    Distribution layer, 77  
classful networks, 103  
Classless Inter-Domain Routing (CIDR), 101  
classless networks, 103  
client(s), 3  
    VTP, 377  
client/server networks, 3  
client-to-site VPNs, 400  
collision(s)  
    Ethernet, 338  
    late, 341  
    collision domains, 28, 41  
    collision errors, Ethernet, 341  
    command(s). *See also specific commands*  
        access lists, 450  
        identification, 444–445  
        interface configuration, 447–448  
        IP, 448–449  
        mistyped, 130  
        navigation, 444–445  
        passwords, 446  
        router and switch examination, 447  
        router/switch general and startup configuration, 446  
        VLAN configuration, 451–452  
    WAN configuration, 450–451  
command executive (EXEC), 118  
command history, 130  
    lab, 519–523  
command-line Help, lab, 519–523  
command-line interface, configuring switches, lab, 604–609  
Committed Burst Size (CBS), Frame Relay, 316  
Committed Information Rate (CIR), Frame Relay, 316  
configuration  
    default routes, 189–190  
    DHCP, lab, 572–577  
    DNS, lab, 575–577  
    duplex mode, 353  
    EIGRP, 217–219  
    EIGRP, lab, 561–563  
Frame Relay. *See* Frame Relay configuration  
HyperTerminal, 120  
NAT, labs, 570–572, 575–577  
OSPF, single-area, 227–228  
OSPF, single-area, lab, 563–567  
PPP, with CHAP and PAP, lab, 592–595  
RIP routing for each major network, 182–183  
RIPv2, lab, 557–561  
router identification, 130–132  
routers. *See* router configuration  
STP, 369  
switch ports, 353  
switches, using command-line interface, lab, 604–609  
configuration bridge protocol data units (CBPDU), 367  
configuration register, 147  
    CDP, 156–158  
    lab, 539–542  
congestion, Frame Relay, 317  
congestion avoidance, 62  
connectionless protocols, 11  
connection-oriented protocols, 11, 12  
console password, 125  
console port (console), 118  
Consultative Committee on International Telephony and Telegraphy (CCIT), 308  
content-addressable memory (CAM), 348  
contention, 36  
contention methods, 338

**640** Index

- context-sensitive Help, Cisco router, 123
- Coordinated Universal Time (UTC), 132
- copy commands, router, 147–148
- Core layer, Cisco Three-Layer Hierarchical model, 77–78
- cost, OSPF, 221–223
- count-to-infinity problems, 177
- CPE (customer premises equipment), 308
- CRC (Cyclic Redundancy Check), 9
- crimp tools, 438
- CSMA/CD. *See* Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- CSU/DSU (channel service unit/data service unit), 309
- customer premises equipment (CPE), 308
- cut-through forwarding, 349–350
- Cyclic Redundancy Check (CRC), 9
- D**
- Data Link Connection Identifier (DLCI) numbers, 310
- Data Link layer (layer 2), 7, 9–11 addresses, lab, 468–471
- data packets, IP and MAC header information, lab, 489–491
- data terminal equipment (DTE), 308
- database servers, 3
- datagrams, 11
- date, router, configuring, 132
- debug all command, 456
- debug ip rip command, 183, 184, 456
- decimal numbers, conversion to binary and hexadecimal numbers, 106–107
- lab, 504–506
- default gateway, 64
- default routes, configuring, 189–190
- default VLAN, 370
- defining a maximum, 178
- demilitarized zone (DMZ), 395
- designated routers (DRs), 224–225
- destination unreachable message, 62
- DHCP. *See* Dynamic Host Configuration Protocol (DHCP)
- DHCP ACK message, 246
- DHCP DISCOVER message, 246
- DHCP OFFER message, 246
- DHCP relay, 246
- DHCP REQUEST message, 246
- Diffusing Update Algorithm (DUAL), 214–217
- Dijkstra's Shortest Path First Algorithm, 226
- directed broadcasts, 95
- disabled state, switch ports, 368
- distance-vector routing protocols, 176–178, 180, 220
- Distribution layer, Cisco Three-Layer Hierarchical model, 77
- DLCI (Data Link Connection Identifier) numbers, 310
- DMZ (demilitarized zone), 395
- DNS. *See* Domain Name Service (DNS)
- domain(s)
- collision, 28
  - VTP, 377
- Domain Name Service (DNS), 56, 57, 244–245
- configuration, lab, 575–577
- configuring DNS lookup, 245
- configuring using SDM, 251–252
- down-when-looped command, 304–305
- DR(s) (designated routers), 224–225
- DRAM (dynamic random access memory), 134
- DTE (data terminal equipment), 308
- DUAL (Diffusing Update Algorithm), 214–217
- dual stack, 108
- dual-homed bastion, 394
- duplex communications, 41–42
- duplex mode, configuring, 353
- Dynamic Host Configuration Protocol (DHCP), 57, 246–248
- configuration, lab, 572–577
- configuring router to be DHCP server, 246–248
- configuring using SDM, 252–253
- monitoring, 248
- dynamic NAT, 240
- configuring, 242–243
- dynamic random access memory (DRAM), 134
- dynamic routing protocols, 188
- dynamic VLANs, static VLANs versus, 373
- E**
- EAP (Extensible Authentication Protocol), 31
- EBCDIC, 12

- EBS (Excess Burst Size), Frame Relay, 316
- echo request/reply message, 62
- EGPs (Exterior Gateway Protocols), 175
- EIA/TIA (Electronic Industries Alliance/Telecommunications Industries Association) 568B specifications, 8
- 802 standards. *See* IEEE (Institute of Electrical and Electronics Engineers)
- EIGRP. *See* Enhanced Interior Gateway Routing Protocol (EIGRP)
- electromagnetic interference (EMI), 3
- Electronic Industries Alliance/ Telecommunications Industries Association (EIA/TIA) 568B specifications, 8
- EMI (electromagnetic interference), 3
- enable mode, 123
- enable mode prompt, 123
- enable password, 125, 126–127
- enable secret password, 125, 126–127
- Encapsulating Security Protocol (ESP), 402
- encapsulation, 13–14
- lab, 466–468
- encryption, 396
- IPSec algorithms, 402
- end systems, 4
- enhanced editing features, lab, 519–523
- Enhanced Interior Gateway Routing Protocol (EIGRP), 175, 210–219
- components, 213–217
- configuration, 217–219
- configuration, lab, 561–563
- DUAL, 214–217
- metric, 211
  - neighbor discovery and maintenance, 213
  - PDMs, 213
  - RTP, 213–214
- errors, Ethernet, 341
- ESP (Encapsulating Security Protocol), 402
- ESS (Extended Service Set), 30
- established parameter, extended IP access lists, 277–278
- Ethernet, 10, 28, 40–42, 338–341
- broadcasts, 339
  - collision domain, 338–339
  - collision errors, 341
  - collisions, 338
  - CSMA/CD, 40–41, 338–339
  - Fast Ethernet, 41
  - frame size errors, 341
  - Gigabit Ethernet, 41
  - half- and full-duplex communications, 41–42
  - latency, 340
  - exam preparation, Internet resources, 431
- Excess Burst Size (EBS), Frame Relay, 316
- EXEC (command executive), 118
- EXEC mode, 122, 124
- expectational acknowledgement, 59
- extended access lists, lab, 584–587
- extended IP access lists, 273–278
- established parameter, 277–278
  - examples, 271–277
  - monitoring, 278
- extended mode ping, 151
- Extended Service Set (ESS), 30
- Extensible Authentication Protocol (EAP), 31
- Exterior Gateway Protocols (EGPs), 175
- extractors, 441
- magnetic, 440
- extranets, 4
- F**
- Fast Ethernet, 41, 342
- FCSs. *See* frame check sequence(s); frame check sequence (FCS) errors
- FD (feasible distance), DUAL, 214
- FDDI (IEEE 802.10), 374
- feasibility condition, DUAL, 214
- feasible distance (FD), DUAL, 214
- feasible successor, DUAL, 214
- fiber-optic cable, 2
- file servers, 3
- File Transfer Protocol (FTP), 55
- firewalls, 393–395
- configuration using SDM, lab, 631–633
- flash memory, routers, 133
- flashlights, pocket, 436
- flood(s), 179
- flooded broadcasts, 95
- flush interval, 183
- forwarding methods, 349–351
- forwarding state, switch ports, 368

**642** Index

- FRADs (Frame Relay access devices), 310
- fragment-free forwarding, 350–351
- frame check sequence(s) (FCSs), 341
- frame check sequence (FCS) errors, 341
- frame filtering, 373–374
- frame format, Frame Relay, 317–318
- frame identification, 374
- Frame Relay, 308–326
- configuring routers, lab, 600–602
  - configuring test network, lab, 595–598
  - frame formats, 317–318
  - LMI, 312–316
  - monitoring, 324–326
  - performance parameters, 316–317
  - static mapping, 324
  - topologies, 318–319
  - virtual circuits, 310–312
- Frame Relay access devices (FRADs), 310
- Frame Relay assembler/dissembler, 310
- Frame Relay configuration, 319–324
- keepalive, 324
  - multipoint, using subinterface, 321–322
  - multipoint, with two routers, 319–321
  - non-Cisco routers, 324
  - point-to-point, using subinterfaces, 322–323
  - static mapping, 324
- Frame Relay maps, 310–312
- Frame Relay network devices (FRNDs), 310
- Frame Relay switch, 308
- configuring router to simulate, lab, 598–600
- Frame Relay switching table, 311
- frame size errors, Ethernet, 341
- frame tagging, 374
- frame transmission, 70–76
- dynamic and static routing tables, 72–73
  - routers, 70–72
  - routing packets, 74–76
  - transmitting packets to remote segments, 73
- FRNDs (Frame Relay network devices), 310
- FTP (File Transfer Protocol), 55
- full-duplex communications, 41–42
- Ethernet, 343–344
- G**
- gateways, 40
- collision domains, 338
  - default, 64
  - operation, lab, 477–478
- Generic Routing Encapsulation (GRE), 401
- Gigabit Ethernet, 41, 342–343
- global configuration modes, 123, 124
- GRE (Generic Routing Encapsulation), 401
- H**
- half-duplex communications, 41–42
- Ethernet, 343–344
- hardware
- connections, lab, 508–511
  - security, 390–391
- Hashed Message Authentication Codes (HMACs), 402
- HDLC (High-Level Data Link Control), 303
- hex keyset, 436
- hexadecimal numbers, 105–107
- conversion to binary and decimal numbers, 106–107
  - conversion to binary and decimal numbers, lab, 504–506
- High-Level Data Link Control (HDLC), 303
- High-Speed Serial Interface (HSSI), 302
- HMACs (Hashed Message Authentication Codes), 402
- hold-down timers, 178
- hop count, 174
- host name, setting on switches, 352
- HSSI (High-Speed Serial Interface), 302
- HTTP (Hypertext Transfer Protocol), 56
- hubs, 27
- active, 27
  - advantages and disadvantages, 28
  - connecting networks, lab, 474–475
  - nonswitching, 378
  - operation, lab, 477–478
  - passive, 27
  - performance evaluation, lab, 609–612

- HyperTerminal, configuring, 120  
lab, 511–513
- Hypertext Transfer Protocol (HTTP), 56
- I**
- IANA (Internet Assigned Numbers Authority), 89
- ICANN (Internet Corporation for Assigned Names and Numbers), 89
- ICMP (Internet Control Message Protocol), 62
- ICMP flood, 70
- identification commands, 444–445
- IDSs (Intrusion Detection Systems), 395
- IEEE (Institute of Electrical and Electronics Engineers), 9  
802.1q standard, 374  
802.1x, 31  
802.3, 40  
802.3ab standard, 41  
802.3u standard, 41, 342  
802.3z, 41  
802.10 (FDDI), 374  
802.11 standard, 29–30, 30  
802.11i, 31
- IFG (interframe gap), 40
- IGPs. *See* Interior Gateway Protocols (IGPs)
- IGRP (Interior Gateway Routing Protocol), 175, 186–187
- IKE (Internet Key Exchange), 402
- implicit deny any statement, 260
- inbound traffic, access lists, 263
- information request/reply message, 62
- infrared, 2
- infrastructure mode, 30
- initial configuration dialog, 120–121
- initial sequence numbers (ISNs), 59
- Institute of Electrical and Electronics Engineers. *See* IEEE (Institute of Electrical and Electronics Engineers)
- interface(s)  
command-line, configuring switches, lab, 604–609  
configuration commands, 447–448  
descriptions, lab, 533–535  
routers, 134–136  
switches. *See* switch user interfaces
- interface configuration mode, 123, 124
- interframe gap (IFG), 40
- interframe gaps, 338
- Interior Gateway Protocols (IGPs), 175  
distance-vector routing protocols, 176–178, 180, 220
- EIGRP. *See* Enhanced Interior Gateway Routing Protocol (EIGRP)
- IGRP, 175, 186–187
- link-state routing protocols, 176, 178–180, 220
- OSPF. *See* Open Shortest Path First (OSPF)
- RIP. *See* Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol (IGRP), 175, 186–187
- International Organization for Standardization (ISO), 5
- International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), 308
- Internet Assigned Numbers Authority (IANA), 89
- Internet Control Message Protocol (ICMP), 62
- Internet Corporation for Assigned Names and Numbers (ICANN), 89
- Internet Key Exchange (IKE), 402
- Internet Protocol (IP), 62. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP)  
on routes, 149  
version 4, IPv6 versus, 107–109  
version 6. *See* IPv6
- Internet resources, 430–431
- Internet Security Association and Key Management Protocol (ISAKMP), 402
- internetwork(s), 37, 173
- Internetwork layer, TCP/IP, 55, 62–70
- Internetwork Operating System. *See* Cisco Internetwork Operating System (IOS)
- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), 6, 7, 173–174
- interpacket gaps (IPGs), 40, 338
- Inter-Switch Link (ISL) protocol, 374
- intranets, 4
- Intrusion Detection Systems (IDSs), 395
- Intrusion Prevention Systems (IPSs), 395

**644** Index

inverse masks, 265  
**IOS.** *See Cisco Internetwork Operating System (IOS)*  
 IP access lists  
   extended, 273–278  
   standard, 265–273  
 IP address(ing), 38, 77, 87–111  
   advantages of NAT over, 238  
   broadcast types, 95  
   configuring, lab, 526–530  
   decoding IP addresses, labs, 496–500  
   hexadecimal numbers, 105–107  
   IP classes, 89–92  
   IPv4 versus IPv6, 107–109  
   labs, 493–506  
   MAC addresses compared, 88–89  
   network addressing, 92–94  
   routers, 72  
   subdividing IP classes, 95–102  
   subnet masking, 96–98  
   subnetting. *See subnetting*  
   switches, 352  
   transitioning to IPv6, 108–109  
 IP classes, 89–92  
   Class A, 89–90  
   Class B, 90  
   Class C, 90–91, 97–98  
   Class D, 91  
   Class E, 91  
   private IP ranges, 91–92  
   subdividing, 95–102  
 IP commands, 448–449

IP connectivity, 149–155  
   checking interfaces, 152–155  
   IP host names, 150–151  
   IP route, 152  
   ping command, 151  
   Telnet, 150  
   trace command, 151–152  
 IP Control Protocol (IPCP), 302  
 IP hosts, configuring, lab, 526–530  
 IP Security Protocol (IPSec), 107, 401–402  
   authentication algorithms, 402  
   encryption algorithms, 402  
   key management, 402  
   protocols, 401–402  
   transform sets, 402  
 IPCP (IP Control Protocol), 302  
 IPGs (interpacket gaps), 40, 338  
 IPS(s) (Intrusion Prevention Systems), 395  
 IPSec. *See IP Security Protocol (IPSec)*  
 IPv6  
   IPv4 versus, 107–109  
   transitioning to, 108–109  
 IPv4, IPv6 versus, 107–109  
 IPX Control Protocol (IPXCP), 302  
 IPXCP (IPX Control Protocol), 302  
 IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange), 6, 7, 173–174  
 ISAKMP (Internet Security Association and Key Management Protocol), 402  
 ISL (Inter-Switch Link) protocol, 374  
 ISNs (initial sequence numbers), 59

ISO (International Organization for Standardization), 5  
 ITU-T (International Telecommunication Union-Telecommunication Standardization Sector), 308  
**J**  
 jam signals, 40, 338  
**K**  
 keepalive frames, 152  
 keepalive packets, 312  
   Frame Relay configuration, 324  
 key management, IPSec, 402  
 labs  
   ARP request and reply IP and MAC header information, 486–488  
   binary/decimal/hexadecimal conversions, 504–506  
   boot system commands, 539–542  
   bridges versus switches, 478–481  
   cdp command, 535–539  
   configuration register, 539–542  
   configuring Cisco route using system configuration dialog, 513–517  
   configuring HyperTerminal to access Cisco router, 511–513  
   configuring IP addresses and IP hosts, 526–530  
   configuring message and interface description, 533–535  
   configuring passwords, 517–519  
   configuring routers for Frame Relay, 600–602

- configuring switches using command-line interface, 604–609
- connection-oriented versus connectionless communications, 471–472
- data encapsulation steps, 466–468
- Data Link layer addresses, 468–471
- data packet IP and MAC header information, 489–491
- decoding IP addresses, 496–500
- device functions, 477–478
- DHCP configuration, 572–575, 575–577
- DNS configuration, 575–577
- EIGRP configuration, 561–563
- enhanced editing features, 519–523
- extended IP access list creating and application, 584–587
- firewall configuration using SDM, 631–633
- Frame Relay network setup, 595–598
- hardware connections, 508–511
- Help system, 519–523
- hub performance evaluation, 609–612
- IP addressing schemes, 494–496, 500–503
- LAN switching concepts and terminology, 618–620
- named IP access list creating and application, 588–590
- NAT configuration, 570–572, 575–577
- Network layer addresses, 468–471
- OSI model, 464–466
- OSPF configuration, 563–567
- ping command, 535–539
- PPP configuration with CHAP and PAP, 592–595
- RARP request IP and MAC header information, 488–489
- RIP configuration, 551–553
- RIPv2 configuration, 557–561
- router-on-a-stick configuration, 620–627
- routing protocol characteristics, 556–557
- routint terms and concepts, 546–547
- SDM configuration of NAT, DHCP, and DNS, 575–577
- SDM interface, 542–544
- Security Audit Wizard, 630–631
- Show command, 519–523
- simulating Frame Relay switch, 598–600
- simulating networks, 474–476
- standard IP access list creation and application, 580–583
- static route configuration, 548–551
- switch performance evaluation, 612–615
- switching concepts and terminology, 618–620
- telnet command, 535–539
- TFTP serve installation, configuration, and use, 531–533
- trace command, 535–539
- VPN creation using SDM, 634–636
- wireless, 481–483
- L**
- LAN(s). *See* local area networks (LANs)
- LAN emulation (LANE), 374
- LAN segmentation, 344–345
- bridges, 344–345
- routers, 345
- LAN switching, 346–351, 365–384
- adaptive cut-through, 351
- segmentation with switches, 346–347
- STP. *See* Spanning Tree Protocol (STP)
- switch operations, 348
- switching methods, 348–351
- virtual LANs. *See* virtual local area networks (VLANs)
- LANE (LAN emulation), 374
- late collisions, 341
- latency, 40
- Ethernet, 340
- Layer 2 Tunneling Protocol (L2TP), 401
- layering. *See also* Cisco Three-Layer Hierarchical model; Open Systems Interconnection (OSI) model; Transmission Control Protocol/Internet Protocol (TCP/IP)
- reasons for, 5–6
- LCP. *See* Link Control Protocol (LCP)
- learning state, switch ports, 368
- line configuration mode, 123–124

**646** Index

- line passwords, setting, 127–129
- link(s), VLANs, 375–376
- Link Control Protocol (LCP), 302, 303, 304–305  
link configuration, 305
- Link Quality Monitoring (LQM), 305
- link-state, OSPF, 224
- link-state advertisements (LSAs), 178, 220
- link-state algorithm, 73
- link-state packets (LSPs), 178–179
- link-state routing protocols, 176, 178–180, 220
- listening state, switch ports, 368
- LLC (Logical Link Control) layer, 9
- LMI. *See* Local Management Interface (LMI)
- local area networks (LANs), 3  
segmentation. *See* LAN segmentation  
segments, 10–11  
switching terminology and concepts, lab, 618–620
- Local Management Interface (LMI), 312–316  
encapsulation types, 313–316  
inverse ARP, 312–313
- logic bombs, 392
- logical addresses, 11, 173  
physical addresses versus, 38
- Logical Link Control (LLC) layer, 9
- lookup, DNS, 245  
configuring, 245
- loopback addresses, 89
- loopback command, 304
- LQM (Link Quality Monitoring), 305
- LSAs (link-state advertisements), 178, 220
- LSPs (link-state packets), 178–179
- L2TP (Layer 2 Tunneling Protocol), 401
- M**
- MAC addresses  
bridges, 33–34  
frame transmission, 70  
IP addresses compared, 88–89  
switches, 36
- MAC (Media Access Control) layer, 9, 10
- macro viruses, 391
- magnetic extractor, 440
- malware, 391–392  
types, 391–392  
user training, 392  
virus prevention software, 392
- management VLAN, 370
- MANs (metropolitan area networks(s)), 3
- MD5, 402
- MD5 algorithm, 125
- MD5 authentication, 208
- media, 3
- Media Access Control (MAC) layer, 9, 10
- media access methods, 40, 338.  
*See also* Ethernet
- memory, flash, routers, 133
- metrics, 174–175  
EIGRP, 211
- metropolitan area networks (MANs), 3
- microsegmentation, 346  
bandwidth, 36
- midpoint configurations, inverse ARP, 312
- modes  
IEEE 802.11 standard, 30
- switch user interfaces, 351–352
- modified cut-through, 351
- monitoring, 183–186
- multicast addresses, 91
- multicast traffic, 345
- multicasting, 91
- multicasts, 179
- multiport bridges, 346
- N**
- named access lists, 279  
lab, 588–590
- NAT. *See* Network Address Translation (NAT)
- navigation commands, 444–445
- NBMA (nonbroadcast multiaccess), Frame Relay, 316
- NCPs (Network Control Protocols), 302
- neighbor discovery and maintenance, EIGRP, 213
- NetBEUI, 172
- network(s)  
simulating, lab, 474–475  
stub, 187
- network access methods, 40, 338.  
*See also* Ethernet
- Network Address Translation (NAT), 107, 238–244  
advantages over IP addressing, 238

- configuration, labs, 570–572, 575–577  
 configuring, 241–244  
 configuring using SDM, 249–251  
 dynamic, 240, 242–243  
 overlapping, 241  
 PAT (overloading), 240–241, 243–244  
 static, 239–240, 241–242
- network addressing, 92–94  
 broadcast addresses, 94  
 lab, 468–471  
 subnet addresses, 93–94
- Network Control Protocols (NCPs), 302
- Network File System (NFS), 56
- network interface cards (NICs), 4  
 MAC addresses, 10
- Network Interface Layer, TCP/IP, 55, 70
- Network layer (layer 3), 7, 11  
 addresses, lab, 468–471
- Network News Transfer Protocol (NNTP), 57
- network operating systems (NOSs), 4
- network services, 237–254. *See also* Domain Name Service (DNS); Dynamic Host Configuration Protocol (DHCP); Network Address Translation (NAT)
- Network Time Protocol (NTP), 57
- networking  
 Internet resources, 431  
 origin, 2  
 reasons for using, 2  
 terminology, 3–4
- networking hardware, 4  
 networking professional's toolkit, 433–442  
 NFS (Network File System), 56  
 nibbles, 106  
 NIC errors, 341  
 NICs. *See* network interface cards (NICs)  
 NNTP (Network News Transfer Protocol), 57  
 no access-list [list number] command, 261, 263  
 nonbroadcast multiaccess (NBMA), Frame Relay, 316  
 nonroutable protocols, 172  
 nonswitching hubs, 378  
 nonvolatile random access memory (NVRAM), 133–134  
 NOSs (network operating systems), 4  
 NTP (Network Time Protocol), 57  
 NVRAM (nonvolatile random access memory), 133–134
- 100Base-FX, 41, 342  
 100Base-T4, 41, 342  
 100Base-TX, 41, 342  
 1000Base-CX, 41, 343  
 1000Base-LX, 41, 343  
 1000Base-SX, 41, 343  
 1000Base-T, 41  
 1000Base-TX, 343
- O**
- Open Shortest Path First (OSPF), 175, 220–228  
 adjacencies dialog box, 223  
 areas, 223–224  
 authentication, 228–230
- BDRs, 224, 225  
 configuration, lab, 563–567  
 cost, 221–223  
 DRs, 224–225  
 links and link-state, 221  
 operation, 225–227  
 router ID, 225  
 single-area configuration, 227–228  
 topological database, 224
- Open Systems Interconnection (OSI) model, 4–14  
 Application layer (layer 7), 7, 13  
 Data Link layer (layer 2), 7, 9–11  
 Data Link layer (layer 2), lab, 468–471  
 labs, 463–472  
 layer functions, 6–14  
 Network layer (layer 3), 7, 11  
 peer communication, 6  
 Physical layer (layer 1), 7, 8–9  
 Presentation layer (layer 6), 7, 12–13  
 reasons for layering, 5–6  
 Session layer (layer 5), 7, 12  
 Transport layer (layer 4), 7, 11–12
- operating systems  
 Cisco IOS. *See* Cisco Internetwork Operating System (IOS)  
 network, 4  
 optical repeaters, 26  
 Organizational Unit Identifier (OUI), 10

**648** Index

OSI model. *See* Open Systems Interconnection (OSI) model  
 OSPF. *See* Open Shortest Path First (OSPF)  
 OUI (Organizational Unit Identifier), 10  
 overlapping, PAT, 241  
 overloading, 240–241  
     configuring PAT, 243–244  
 oversubscription, Frame Relay, 317

**P**

packet(s), 11  
     routing, 74–76  
     transmitting to remote segments, 73  
 Packet Internet Groper (Ping), 68–69  
 packet switching, 37  
 packet-filtering routers, 393  
 PAP. *See* Password Authentication Protocol (PAP)  
 parameter problem message, 62  
 partial masking, 266  
 passive hubs, 27  
 password(s)  
     Cisco routers, 125–129  
     commands, 446  
     configuring, lab, 517–519  
     enable, 125, 126–127  
     enable secret, 125, 126–127  
     line, setting, 127–129  
     router password recovery, 161–162  
     switch user interfaces, 351–352  
     virtual terminal, 125

Password Authentication Protocol (PAP), 304, 397  
     configuring PPP, lab, 592–595  
 PAT. *See* Port Address Translation (PAT)  
 patch management, 399  
 PDMs (Protocol Dependent Modules), 210, 213  
 PDN (public data network), 308  
 PDUs (protocol data units), 13, 14  
 peer communication, 6  
 peer-to-peer networks, 3, 172  
 permissions, 396  
 Per-VLAN STP (PVSTP), 368–369  
 physical addresses, 10  
     logical addresses versus, 38  
 Physical layer (layer 1), 7, 8–9  
 physical path loops, 366  
 physical security, 390–391  
 Ping (Packet Internet Groper), 68–69  
 ping command, 151, 454  
     lab, 535–539  
 pliers, 435  
 pocket flashlights, 436  
 point-to-point configurations, inverse ARP, 312  
 Point-to-Point Tunneling Protocol (PPTP), 400  
 polymorphic viruses, 392  
 POP3 (Post Office Protocol 3), 57  
 port(s)  
     switches, securing, 353–354  
     switches, states, 367–368  
     TCP/IP Transport layer, 56–58  
 Port Address Translation (PAT), 240–241  
     configuring, 243–244, 251  
 port forwarding, 241  
 port-based memory buffering, 348  
 POST (power-on self test), 147  
 Post Office Protocol 3 (POP3), 57  
 power-on self test (POST), 147  
 PPP, 302–308  
     configuration with CHAP and PAP, lab, 592–595  
     configuring authentication, 306–308  
     confirming communications, 308  
     establishing communications, 305–306  
     frame format, 303–305  
     in protocol stack, 302–303  
 PPP frame  
     elements, 304  
     format, 303–305  
 PPTP (Point-to-Point Tunneling Protocol), 400  
 precision knife, 437  
 Presentation layer (layer 6), 7, 12–13  
 print servers, 3  
 private IP ranges, 91–92  
 privileged EXEC mode, 123, 124  
 propagation delay, Ethernet, 340  
 protocol(s), 6. *See also specific protocols*  
     connectionless, 11  
     connection-oriented, 11, 12  
     IPSec, 401–402  
     nonroutable, 172  
     routed, 63, 173–174  
     routing, 72–73

- Session layer, 12  
 Transport layer, 11–12  
 protocol analyzers, 339  
 protocol data units (PDUs), 13, 14  
 Protocol Dependent Modules (PDMs), 210, 213  
 public data network (PDN), 308  
 punch-down block tool, 439  
 PVSTP (Per-VLAN STP), 368–369
- Q**  
 quad zero routes, 189
- R**  
 RADIUS (Remote Authentication Dial-in User Service), 397  
 RADIUS server, 306  
 random access memory (RAM), 134  
 rapid spanning tree protocol (RSTP), 370  
 RARP. *See* Reverse Address Resolution Protocol (RARP)  
 RARP clients, 67  
 RARP request(s), IP and MAC header information, lab, 488–489  
 RARP request frames, 66–67  
 RASs (remote access servers), 3  
 RD (reported distance), DUAL, 214  
 read-only memory (ROM), routers, 132  
 redirect message, 62  
 Reliable Transport Protocol (RTP), 213–214  
 reload command, 261–262  
 remote access servers (RASs), 3  
 Remote Authentication Dial-in User Service (RADIUS), 397  
 remote login application (rlogin), 56
- Remote Procedure Call (RPC), 12  
 remote segments, transmitting packets to, 73  
 repeaters, 9, 26–27  
     advantages and disadvantages, 28  
     operation, lab, 477–478  
     optical, 26  
 reported distance (RD), DUAL, 214  
 Requests for Comments (RFCs), 54  
 reset packets (RSTs), 61  
 restoring, CDP, 160–161  
 Reverse Address Resolution Protocol (RARP), 63, 66  
     ARP compared, 67  
     RARP clients, 67  
     request frames, 66–67  
     requests, IP and MAC information, lab, 488–489  
 RFCs (Requests for Comments), 54  
 RIP. *See* Routing Information Protocol (RIP)  
 RJ-45 to DB-9 connectors, 118  
 RJ-45 to RJ-45 rollover cables, 118  
 rlogin (remote login application), 56  
 ROM (read-only memory), routers, 132  
 ROM Monitor, 147  
 ROM Monitor mode, CDP, 158  
 root bridges, 367  
 root devices, 367  
 route aggregation, 101–102  
 Route Switch Modules (RSMs), 380  
 routed protocols, 63, 173–174
- router(s), 37–39  
     advantages and disadvantages, 38–39  
 CDP, 155–156  
 configuration. *See* router configuration  
 connecting networks, lab, 474–475  
 copy commands, 147–148  
 creating firewall using SDM, 286–295  
 date, configuring, 132  
 enabling IP, 149  
 examination commands, 447  
 flash memory, 13  
 frame transmission, 70–72  
 general and startup configuration commands, 446  
 interfaces, 134–136  
 IP addresses, 72  
 IP connectivity. *See* IP connectivity  
 LAN segmentation, 345  
 multipoint Frame Relay configuration with two routers, 319–321  
 non-Cisco, enabling Frame Relay, 324  
 NVRAM, 133–134  
 operation, lab, 477–478  
 packet-filtering, 393  
 password recovery, 161–162  
 physical versus logical addresses, 38  
 RAM/DRAM, 134  
 ROM, 132  
 SDM, 162  
 startup. *See* router startup

**650** Index

- router(s) (*continued*)  
 stub, 187  
 time, configuring, 132  
 troubleshooting commands, 454–456
- router configuration  
 changes, methods for making, 148–149  
 configuring HyperTerminal to access Cisco router, lab, 511–513  
 configuring IP addresses and hosts, lab, 526–530  
 configuring message and interface description, lab, 533–535  
 configuring routers for Frame Relay, lab, 600–602  
 configuring to be DHCP server, 246–248  
 configuring using System Configuration dialog, lab, 513–517  
 router configuration files, 147–148
- router configuration modes, 123–124
- router startup, 146–149  
 change process, 148–149  
 configuration files, 147–148  
 POST, 147
- router-on-a-stick, 380  
 configuration, lab, 620–627
- routing, 118–139. *See also* router(s)  
 benefits, 118  
 Cisco IOS. *See* Cisco Internetwork Operating System (IOS)  
 router components, 132–136
- static, 187–190  
 terminology and concepts, 546–547
- Routing Information Protocol (RIP), 175  
 characteristics, lab, 556–557  
 configuration, lab, 551–553  
 configuring RIP routing for each major network, 182–183  
 enabling RIP routing, 181–182  
 RIPv1, 180–186  
 RIPv2, 206–210  
 RIPv2, lab, 557–561
- routing loops, 177
- routing protocols, 72–73, 174–193, 199–232  
 classful, 200–204  
 classless, 204–205  
 controlling route traffic, 230  
 dynamic, 188
- IDGPs. *See* Enhanced Interior Gateway Routing Protocol (EIGRP); Interior Gateway Protocols (IGPs); Open Shortest Path First (OSPF); Routing Information Protocol (RIP)
- labs, 545–553  
 static routing, 187–190
- routing tables, 71  
 dynamic versus static, 72–73
- RPC (Remote Procedure Call), 12
- RSMs (Route Switch Modules), 380
- RST(s) (reset packets), 61
- RSTP (rapid spanning tree protocol), 370
- RTP (Reliable Transport Protocol), 213–214
- RxBoot mode, CDP, 158–159
- S**
- SANs (storage-area networks), 3–4
- screwdriver, 435
- SDM. *See* Security Device Manager (SDM)
- Secure Shell (SSH) protocol, 398
- Secure Sockets Layer (SSL), 397
- security, 389–417  
 authentication, 397  
 CDP, 156  
 Cisco Security Audit wizard, 410–415  
 disabling unnecessary services, 389–399  
 encryption, 396–397  
 firewalls, 393–395  
 hardware protection, 390–391  
 IPSec, 401–402  
 labs, 629–636  
 malware prevention, 391–392  
 patch management, 399  
 permissions, 396  
 SDM, 403–410  
 security policies, 390  
 software protection, 391  
 SSH connections, 398  
 switch ports, 353–354  
 VPNs, 400–401  
 WLANs, 30–31
- Security Audit Wizard, 410–415
- lab, 630–631

- Security Device Manager (SDM), 162, 248–253, 249–251, 251–252, 252–253  
configuring PAT, 251  
creating access control lists, 280–285  
creating router firewall, 286–295  
creating VPNs, 403–410  
firewall configuration, lab, 631–633  
interface, lab, 542–544  
Security Audit Wizard, lab, 630–631  
VPN creation, lab, 634–636  
security policies, 390  
segment(s), 32  
    remote, transmitting packets to, 73  
segmentation, 32–33  
segmenting traffic, 26  
Serial Line Internet Protocol (SLIP), 302  
servers, VTP, 377  
Service Set Identifier (SSID), 30  
Services for Macintosh, 40  
Session layer (layer 5), 7, 12  
SHA-1, 402  
shared memory buffering, 348  
Shortest Path First (SPF) algorithm, 178  
show access-lists command, 455  
show cdp neighbor command, 455  
show cdp neighbor detail command, 455  
show flash command, 455  
show frame-relay lmi command, 456  
show frame-relay map command, 455  
show frame-relay pvc command, 455  
show history command, 455  
show interfaces command, 455  
show ip access-lists command, 455  
show ip interface command, 455  
show ip protocol command, 183–184, 185–186, 455  
show ip route command, 455  
show mac-addresss-table command, 457  
show port-security command, 457  
show running-config command, 454  
show spanning-tree command, 457  
show starting-config command, 456  
show version command, 454  
show vlan command, 457  
show vtp command, 457  
Simple Mail Transfer Protocol (SMTP), 56  
Simple Network Management Protocol (SNMP), 56  
single homed bastion, 393–394  
site-to-site VPNs, 400–401  
sliding windows, 61–62  
SLIP (Serial Line Internet Protocol), 302  
slot time, 340  
SMTP (Simple Mail Transfer Protocol), 56  
SNMP (Simple Network Management Protocol), 56  
software  
    security, 391  
    virus prevention, 392  
solder, 434  
solder wick, 434  
soldering iron, 434  
source quench message, 62  
source-routing bridges, 34–35  
Spanning Tree Algorithm (STA), 367  
Spanning Tree Protocol (STP), 366–370  
    building a logical path, 367  
    configuring, 369  
    per-VLAN, 368–369  
    port states, 367–368  
    portfast feature, 369  
    rapid, 370  
    topology changes, 368  
SPF (Shortest Path First) algorithm, 178  
split horizon, 178, 314–316  
    with poison reverse, 178  
SQL (Structured Query Language), 12  
SSH (Secure Shell) protocol, 398  
SSID (Service Set Identifier), 30  
SSL (Secure Sockets Layer), 397  
STA (Spanning Tree Algorithm), 367  
stable states, switch ports, 367–368  
standard IP access lists, 265–273  
    examples, 268–273  
    monitoring, 273

**652** Index

- standardization, VLANs, 373–374  
 standards organizations, Internet resources, 430  
 startup-config, 147  
 static address to DLCI Frame Relay map, 324  
 static NAT, 239–240  
     configuring, 241–242  
 static routes, 187–190  
     adding, 187–190  
     configuration, alb, 548–551  
     configuring default routes, 189–190  
 static VLANs, dynamic VLANs versus, 373  
 stealth viruses, 392  
 storage-area networks (SANs), 3–4  
 store-and-forward forwarding, 350  
 STP. *See* Spanning Tree Protocol (STP)  
 Structured Query Language (SQL), 12  
 stub networks, 187  
 stub routers, 187  
 subinterfaces, 311–312  
 subnet(s), 92  
 subnet masking, 96–98  
 subnetting, 98–105  
     CIDR, 101  
     subnetting formulas, 100–101  
     summarization, 101–102  
     variable length subnet masks, 102–105  
 subnetworks, 38  
 successor  
 DUAL, 214  
 feasible, DUAL, 214  
 summarization, 101–102  
 supernetting, 101  
 switch(es), 35–37, 346  
     advantages and disadvantages, 36–37  
     bridges versus, lab, 478–481  
     configuring using command-line interface, lab, 604–609  
     connecting networks, lab, 474–475  
     examination commands, 447  
     general and startup configuration commands, 446  
     LAN switching, 346–347  
     operations, 348  
     operations, lab, 477–478  
     performance evaluation, lab, 612–615  
     switching methods, 348–351  
     troubleshooting commands, 456–458  
 switch user interfaces, 351–354  
     configuring duplex mode, 353  
     configuring switch ports, 353  
     IP addresses, 352  
     modes and passwords, 351–352  
     securing switch ports, 353–354  
     setting host name, 352  
 switched bandwidth, 346  
 switching, 337–359  
     asymmetric, 348  
     Ethernet, 338–341  
     Fast Ethernet, 342  
     Gigabit Ethernet, 342–343  
 half-and full-duplex communications, 343–344  
 labs, 603–615, 617–627  
 LANs, 346–351  
 LANs, terminology and concepts, lab, 618–620  
 switch user interfaces. *See* switch user interfaces  
 symmetric key encryption, 396  
 system configuration dialog, 120–121  
 configuring Cisco router, lab, 513–517
- T**
- TACACS (Terminal Access Controller Access Control System), 306  
 TACACS+ (Terminal Access Controller Access Control System Plus), 397  
 TCP/IP. *See* Transmission Control Protocol/Internet Protocol (TCP/IP)  
 technical forums, Internet resources, 431  
 technology reference, Internet resources, 430  
 telnet (terminal emulation protocol), 56  
 telnet command, 454  
     lab, 535–539  
 Terminal Access Controller Access Control System (TACACS), 306  
 Terminal Access Controller Access Control System Plus (TACACS+), 397  
 terminal emulation protocol (telnet), 56  
 terminal programs, 120

- TFTP servers. *See* Trivial File Transfer Protocol (TFTP) servers
- three-way handshake, 58–61
- time, router, configuring, 132
- time exceeded message, 62
- timestamp request/reply message, 62
- time-to-live (TTL) counters, 69, 151
- Token Ring, 28
- topological database, OSPF, 224
- topologies, 27, 178
  - Frame Relay, 318–319
  - STP, 368
- trace command, 151–152
  - lab, 535–539
- Trace utility, 69–70
- transform sets, IPSec, 402
- transitory states, switch ports, 368
- translation bridges, 35
- Transmission Control Protocol/Internet Protocol (TCP/IP), 6, 53–82, 173–174
  - Application layer, 55–56
  - Cisco Three-Layer Hierarchical model, 76–78
  - frame transmission. *See* frame transmission
  - Internetwork layer, 55, 62–70
  - labs, 485–491
  - layers, 7
  - Network Interface Layer, 55, 70
  - origins, 54
  - Transport layer, 55, 58–62
- transmission time, Ethernet, 340
- transparent bridges, 34
- Transport layer (OSI layer 4), 7, 11–12
- Transport layer (TCP/IP), 55, 58–62
  - ports, 56–58
  - sliding windows, 61–62
  - three-way handshake, 58–61
  - transport mode, IPSec, 401
  - triggered updates, 179
  - 3DES, 402
  - Trivial File Transfer Protocol (TFTP) servers, 55, 119, 147
    - installation, configuration, and use, lab, 531–533
  - Trojan horses, 392
  - troubleshooting
    - example, 458–459
    - routers, 454–456
    - switches, 456–458
    - using, 458
    - WLANs, 31–32
  - TTL (time-to-live) counters, 69, 151
  - tunnel mode, IPSec, 401
  - tunneling, 108–109
  - tweezers, 441
- U**
- unicasts, 346
- UNIX, TCP/IP, 54
- unnecessary services, disabling, 398–399
- upgrading, CDP, 161
- user interfaces
  - routers, 121–123
  - switches. *See* switch user interfaces
- user mode, 122, 124
- UTC (Coordinated Universal Time), 132
- V**
- variable length subnet masking (VLSM), 102–105, 175
- virtual circuits, 36, 310–312
  - DLCI, 310
  - Frame Relay maps, 310–312
- virtual local area networks (VLANs), 370–381
  - benefits, 372–373
  - configuration commands, 451–452
  - creating, 374–375
  - dynamic versus static, 373
  - link types and configuration, 375–376
  - management (default), 370
  - routers, 378–381
  - standardization, 373–374
  - trunking protocol, 377–378
- virtual private networks (VPNs), 4, 400–401
  - client-to-site, 400
  - creating using SDM, 403–410
  - creating using SDM, lab, 634–636
  - site-to-site, 400–401
- virtual terminal(s) (VTYs), 118
- virtual terminal password, 125
- virus(es), 391–392
- virus prevention software, 392
- VLAN(s). *See* virtual local area networks (VLANs)
- VLAN trunking protocol (VTP), 377–378
  - device modes, 377
  - domains, 377
  - pruning, 378

**654** Index

VLSM (variable length subnet masking), 102–105, 175

VPNs. *See* virtual private networks (VPNs)

VTP. *See* VLAN trunking protocol (VTP)

VTP client mode, 377

VTP domains, 377

VTP pruning, 378

VTP server mode, 377

VTP transparent mode, 377

VTY lines, controlling access, 279–280

VTYs (virtual terminals), 118

**W**

WANs. *See* wide area networks (WANs)

WAV, 12

Web servers, 3

Well Known Port Numbers, 57

WEP (Wired Equivalency Protocol), 31

wide area networks (WANs), 3

configuration commands, 450–451

segments, 10–11

Wi-Fi Protected Access (WPA), 31

Wi-Fi Protected Access version 2 (WPA2), 31

wildcard masks, 265

wire cutters, 437

Wired Equivalency Protocol (WEP), 31

wireless access points. *See also* wireless local area networks (WLANS)

advantages and disadvantages, 32

wireless local area networks (WLANS), 28–32

connectivity, 30

network components, 30

parameters and terminology, lab, 481–483

security measures, 30–31

standards and organizations, 29–30

troubleshooting, 31–32

wireless access points, 28–29

WLANS. *See* wireless local area networks (WLANS)

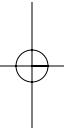
worms, 391

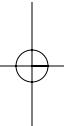
WPA (Wi-Fi Protected Access), 31

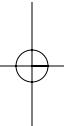
WPA2 (Wi-Fi Protected Access version 2), 31

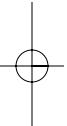
**X**

X-Windows, 12









This book is intended to be sold with a CD-ROM. If this book does not contain a CD-ROM, you are not getting the full value of your purchase.

This CD-ROM contains CoursePrep test prep resources from MeasureUp™.

This CD-ROM also contains CertBlaster® software from DTI Publishing. The unlock code for the exam is c\_ccna (case sensitive).

If the disks/CDs in this book are missing or if the package containing them has been opened, this book is not returnable. By opening and breaking the seal on this package, you are agreeing to be bound by the following agreement:

The software included with this product may be copyrighted, in which case all rights are reserved by the respective copyright holder. You are licensed to use software copyrighted by the Publisher and its licensor on a single computer. You may copy and/or modify the software as needed to facilitate your use of it on a single computer. Making copies of the software for any other purpose is a violation of the United States copyright laws.

This software is sold as is without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Neither the publisher nor its dealers or distributors assume any liability for any alleged or actual damages arising from the use of this program. (Some states do not allow for the excusing of implied warranties, so the exclusion may not apply to you.)