

# A Practical Guide to Advanced Networking

Third Edition

Jeffrey S. Beasley  
Piyasat Nilkaew

Software Enclosed



# A PRACTICAL GUIDE TO ADVANCED NETWORKING

JEFFREY S. BEASLEY AND PIYASAT NILKAEW

Pearson  
800 East 96th Street  
Indianapolis, Indiana 46240 USA

# A PRACTICAL GUIDE TO ADVANCED NETWORKING

## Copyright © 2013 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-4904-8

ISBN-10: 0-7897-4904-1

The Library of Congress Cataloging-in-Publication Data is on file.

Printed in the United States of America

First Printing: November 2012

## Trademarks

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

## Warning and Disclaimer

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

## Bulk Sales

Pearson IT Certification offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

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

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

**International Sales**  
**international@pearsoned.com**

## ASSOCIATE PUBLISHER

Dave Dusthimer

## EXECUTIVE EDITOR

Brett Bartow

## SENIOR DEVELOPMENT EDITOR

Christopher Cleveland

## MANAGING EDITOR

Sandra Schroeder

## PROJECT EDITOR

Mandie Frank

## COPY EDITOR

Sheri Cain

## INDEXER

Ken Johnson

## PROOFREADERS

Leslie Joseph  
Dan Knott

## TECHNICAL EDITORS

Iantha Finley Malbon  
Wayne Randall

## PUBLISHING COORDINATOR

Vanessa Evans

## INTERIOR DESIGNER

Gary Adair

## COVER DESIGNER

Chuti Prasertsith

## COMPOSITOR

Bronkella Publishing

# CONTENTS AT A GLANCE

Introduction	xvi
<b>1</b> Network Infrastructure Design	2
<b>2</b> Advanced Router Configuration I	52
<b>3</b> Advanced Router Configuration II	98
<b>4</b> Configuring Juniper Routers	158
<b>5</b> Configuring and Managing the Network Infrastructure	188
<b>6</b> Analyzing Network Data Traffic	226
<b>7</b> Network Security	266
<b>8</b> IPv6	306
<b>9</b> Linux Networking	336
<b>10</b> Internet Routing	396
<b>11</b> Voice over IP	428
Glossary	456
Index	472

# TABLE OF CONTENTS

Introduction	xvi
<b>CHAPTER 1 Network Infrastructure Design</b>	<b>2</b>
Chapter Outline	3
Objectives	3
Key Terms	3
INTRODUCTION	4
1-1 PHYSICAL NETWORK DESIGN	4
Core	5
Distribution Layer	5
Access Layer	6
Data Flow	6
Selecting the Media	6
1-2 IP SUBNET DESIGN	7
IP Address Range	8
Determining the Number of Subnetworks Needed for the Network	9
Determining the Size or the Number of IP Host Addresses Needed for the Network	11
IP Assignment	15
1-3 VLAN NETWORK	16
Virtual LAN (VLAN)	17
VLAN Configuration	18
VLAN Tagging	23
802.1Q Configuration	25
Networking Challenge: Static VLAN Configuration	26
Configuring the HP Procurve Switch	27
1-4 ROUTED NETWORK	28
Router	29
Gateway Address	30
Network Segments	31
Multilayer Switch	32
Layer 3 Routed Networks	33
Routed Port Configuration	33
InterVLAN Routing Configuration	35
Serial and ATM Port Configuration	37
Summary	44
Questions and Problems	46

<b>CHAPTER 2</b>	<b>Advanced Router Configuration I</b>	<b>52</b>
	Chapter Outline	53
	Objectives	53
	Key Terms	53
	Introduction	54
2-1	CONFIGURING STATIC ROUTING	54
	Gateway of Last Resort	61
	Configuring Static Routes	61
	Load Balancing and Redundancy	68
	Networking Challenge—Static Routes	70
2-2	DYNAMIC ROUTING PROTOCOLS	70
	Distance Vector Protocols	73
	Link State Protocols	74
2-3	CONFIGURING RIPv2	75
	Configuring Routes with RIP	77
	Configuring Routes with RIP Version 2	82
	Networking Challenge—RIP	84
2-4	TFTP—Trivial File Transfer Protocol	85
	Configuring TFTP	85
	Summary	89
	Questions and Problems	89
<b>CHAPTER 3</b>	<b>Advanced Router Configuration II</b>	<b>98</b>
	Chapter Outline	99
	Objectives	99
	Key Terms	99
	INTRODUCTION	101
3-1	CONFIGURING LINK STATE PROTOCOLS—OSPF	101
	Link State Protocols	102
	Configuring Routes with OSPF	103
	Load Balancing and Redundancy with OSPF	109
	Networking Challenge—OSPF	111
3-2	CONFIGURING LINK STATE PROTOCOLS—IS-IS	112
	Configuring Routes with IS-IS	113
	Load Balancing and Redundancy with IS-IS	117
	Networking Challenge: IS-IS	118



<b>CHAPTER 5</b>	<b>CONFIGURING AND MANAGING THE NETWORK INFRASTRUCTURE</b>	<b>188</b>
	Chapter Outline	189
	Objectives	189
	Key Terms	189
	Introduction	190
5-1	DOMAIN NAME AND IP ASSIGNMENT	190
5-2	IP MANAGEMENT WITH DHCP	195
	DHCP Data Packets	197
	DHCP Deployment	201
5-3	SCALING THE NETWORK WITH NAT AND PAT	204
	Configuring NAT	205
5-4	DOMAIN NAME SERVICE (DNS)	209
	DNS Tree Hierarchy	210
	DNS Resource Records	214
	Summary	220
	Questions and Problems	220
<b>CHAPTER 6</b>	<b>Analyzing Network Data Traffic</b>	<b>226</b>
	Chapter Outline	227
	Objectives	227
	Key Terms	227
	INTRODUCTION	228
6-1	PROTOCOL ANALYSIS/FORENSICS	228
	Basic TCP/UDP Forensics	234
	ARP and ICMP	236
6-2	WIRESHARK PROTOCOL ANALYZER	239
	Using Wireshark to Capture Packets	243
6-3	ANALYZING NETWORK DATA TRAFFIC	244
	Configuring SNMP	244
	NetFlow	250
6-4	FILTERING	251
	FTP Filtering	256
	Right-Click Filtering Logic Rules	258
	Filtering DHCP	260
	Summary	262
	Questions and Problems	262

<b>CHAPTER 7</b>	<b>Network Security</b>	<b>266</b>
	Chapter Outline	267
	Objectives	267
	Key Terms	267
	INTRODUCTION	268
	7-1 DENIAL OF SERVICE	268
	Distributed Denial of Service Attacks (DDoS)	270
	7-2 FIREWALLS AND ACCESS LISTS	270
	Network Attack Prevention	272
	Access Lists	272
	7-3 Router Security	279
	Router Access	280
	Router Services	282
	Router Logging and Access-List	283
	7-4 Switch Security	285
	Switch Port Security	286
	Switch Special Features	288
	7-5 Wireless Security	289
	7-6 VPN Security	292
	VPN Tunneling Protocols	293
	Configuring a VPN Virtual Interface (Router to Router)	294
	Troubleshooting the VPN Tunnel Link	299
	Summary	302
	Questions and Problems	302
<b>CHAPTER 8</b>	<b>IPv6</b>	<b>306</b>
	Chapter Outline	307
	Objectives	307
	Key Terms	307
	Introduction	308
	8-1 Comparison of IPv6 and IPv4	308
	8-2 IPV6 ADDRESSING	311
	8-3 IPv6 Network Settings	315
	8-4 Configuring a Router for IPv6	320
	8-5 IPv6 Routing	324
	IPv6: Static	324
	IPv6: RIP	324
	IPv6: OSPF	325

IPv6: EIGRP	325
IPv6: IS-IS	326
8-6 Troubleshooting IPv6 Connection	327
Summary	329
Questions and Problems	329
<b>CHAPTER 9 Linux Networking</b>	<b>336</b>
Chapter Outline	337
Objectives	337
Key Terms	337
INTRODUCTION	338
9-1 LOGGING ON TO LINUX	339
Adding a User Account	340
9-2 LINUX FILE STRUCTURE AND FILE COMMANDS	344
Listing Files	344
Displaying File Contents	346
Directory Operations	348
File Operations	351
Permissions and Ownership	353
9-3 LINUX ADMINISTRATION COMMANDS	357
The <i>man</i> (manual) Command	358
The <i>ps</i> (processes) Command	359
The <i>su</i> (substitute user) Command	362
The <i>mount</i> Command	362
The <i>shutdown</i> Command	364
Linux Tips	364
9-4 ADDING APPLICATIONS TO LINUX	365
9-5 LINUX NETWORKING	371
Installing SSH	375
The FTP Client	376
DNS Service on Linux	376
Changing the Hostname	377
9-6 TROUBLESHOOTING SYSTEM AND NETWORK PROBLEMS WITH LINUX	378
Troubleshooting Boot Processes	378
Listing Users on the System	380
Network Security	382
Enabling and Disabling Boot Services	382

9-7	MANAGING THE LINUX SYSTEM	385
	Summary	390
	Questions and Problems	391
<b>CHAPTER 10 Internet Routing</b>		<b>396</b>
	Chapter Outline	397
	Objectives	397
	Key Terms	397
	INTRODUCTION	398
10-1	INTERNET ROUTING—BGP	398
	Configuring a WAN Connection	398
	Configuring an Internet Connection	400
10-2	CONFIGURING BGP	401
	Configuring BGP	401
	Networking Challenge: BGP	409
10-3	BGP BEST PATH SELECTION	410
10-4	IPv6 OVER THE INTERNET	412
10-5	CONFIGURE BGP ON JUNIPER ROUTERS	415
	Summary	421
	Questions and Problems	421
<b>CHAPTER 11 Voice over IP</b>		<b>428</b>
	Chapter Outline	429
	Objectives	429
	Key Terms	429
	INTRODUCTION	430
11-1	THE BASICS OF VOICE OVER IP	430
11-2	VOICE OVER IP NETWORKS	433
	Replacing an Existing PBX Tie Line	433
	Upgrading Existing PBXs to Support IP Telephony	435
	Switching to a Complete IP Telephony Solution	436
11-3	QUALITY OF SERVICE	438
	Jitter	438
	Network Latency	439
	Queuing	439
	QoS Configuration Example	440

11-4	ANALYZING VoIP DATA PACKETS	442
	Analyzing VoIP Telephone Call Data Packets	446
11-5	VoIP SECURITY	449
	Summary	452
	Questions and Problems	452

	<b>Key Terms Glossary</b>	<b>456</b>
--	---------------------------	------------

	<b>Index</b>	<b>472</b>
--	--------------	------------

## ABOUT THE AUTHORS

**Jeffrey S. Beasley** is with the Department of Engineering Technology and Surveying Engineering at New Mexico State University. He has been teaching with the department since 1988 and is the co-author of *Modern Electronic Communication and Electronic Devices and Circuits*, and the author of *Networking*.

**Piyasat Nilkaew** is a network engineer with 15 years of experience in network management and consulting, and has extensive expertise in deploying and integrating multiprotocol and multivendor data, voice, and video network solutions on limited budgets.

## DEDICATIONS

*This book is dedicated to my family, Kim, Damon, and Dana. —Jeff Beasley*

*This book is dedicated to Jeff Harris and Norma Grijalva. Not only have you given me my networking career, but you are also my mentors. You inspire me to think outside the box and motivate me to continue improving my skills. Thank you for giving me the opportunity of a lifetime. I am very grateful. —Piyasat Nilkaew*

## ACKNOWLEDGMENTS

I am grateful to the many people who have helped with this text. My sincere thanks go to the following technical consultants:

- Danny Bosch and Matthew Peralta for sharing their expertise with optical networks and unshielded twisted-pair cabling, and Don Yates for his help with the initial Net-Challenge Software.
- Abel Sanchez, for his review of the Linux Networking chapter.

I also want to thank my many past and present students for their help with this book:

- David Potts, Jonathan Trejo, and Nate Murillo for their work on the Net-Challenge Software. Josiah Jones, Raul Marquez Jr., Brandon Wise, and Chris Lascano for their help with the Wireshark material. Also, thanks to Wayne Randall and Iantha Finley Malbon for the chapter reviews.

Your efforts are greatly appreciated.

I appreciate the excellent feedback of the following reviewers: Phillip Davis, DeMar College, TX; Thomas D. Edwards, Carteret Community College, NC; William Hessmiller, Editors & Training Associates; Bill Liu, DeVry University, CA; and Timothy Staley, DeVry University, TX.

My thanks to the people at Pearson for making this project possible: Dave Dusthimer, for providing me with the opportunity to work on this book, and Vanessa Evans, for helping make this process enjoyable. Thanks to Brett Bartow, Christopher Cleveland, and all the people at Pearson, and to the many technical editors for their help with editing the manuscript.

Special thanks to our families for their continued support and patience.

—Jeffrey S. Beasley and Piyasat Nilkaew

## ABOUT THE TECHNICAL REVIEWERS

**Wayne Randall** started working in the Information Technology field in 1994 at Franklin Pierce College (now Franklin Pierce University) in Rindge, NH, before becoming a Microsoft Certified Trainer and a consultant at Enterprise Training and Consulting in Nashua, NH.

Wayne acquired his first certification in Windows NT 3.51 in 1994, became an MCSE in NT 4.0 in 1996, was a Certified Enterasys Network Switching Engineer in 2000, and then worked as a networking and systems consultant from 2001 to 2006 before becoming a director of IT for a privately held company. Wayne currently works for Bodycote, PLC, as a network engineer/solutions architect. Bodycote has 170 locations across 27 countries with 43 locations in North America. Wayne has taught for Lincoln Education since 2001 and developed curricula for it since 2011. Mr. Randall holds a BA in American Studies from Franklin Pierce University.

**Iantha Finley Malbon**'s teaching career has spanned 20 years from middle school to collegiate settings and is currently a CIS professor at Virginia Union University. She is also an adjunct professor at ECPI University, having previously served as CIS Department Chair, teaching Cisco routing, networking, and Information Technology courses. She implemented the Cisco Academy for Hanover Schools and was the CCAI for the Academy. She earned her master's degree in Information Systems from Virginia Commonwealth University and bachelor's degree in Technology Education from Virginia Tech. She holds numerous certifications including CCNA, Network+, A+, and Fiber Optic Technician.

## WE WANT TO HEAR FROM YOU!

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

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

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

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

Email: [feedback@pearsonitcertification.com](mailto:feedback@pearsonitcertification.com)

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

## READER SERVICES

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

## INTRODUCTION

This book looks at advanced computer networking. It first guides readers through network infrastructure design. The readers are then introduced to configuring static, RIPv2, OSPF, ISIS, EIGRP routing protocols, techniques for configuring Juniper router, managing the network infrastructure, analyzing network data traffic using Wireshark, network security, IPv6, Linux networking, Internet routing, and Voice over IP. After covering the entire text, readers will have gained a solid knowledge base in advanced computer networks.

In my years of teaching, I have observed that technology students prefer to learn “how to swim” after they have gotten wet and taken in a little water. Then, they are ready for more challenges. Show the students the technology, how it is used, and why, and they will take the applications of the technology to the next level. Allowing them to experiment with the technology helps them to develop a greater understanding. This book does just that.

## ORGANIZATION OF THE TEXT

This textbook is adapted from the second edition of *Networking*. This third volume has been revised and reorganized around the needs of advanced networking students. This book assumes that the students have been introduced to the basics of computer networking. Throughout the text, the students are introduced to more advanced computer networking concepts. This involves network infrastructure design, advanced router configuration, network security, analyzing data traffic, Internet routing, and Voice over IP.

# Key Pedagogical Features

- Chapter Outline, Key Terms, and Introduction at the beginning of each chapter clearly outline specific goals for the reader. An example of these features is shown in Figure P-1.

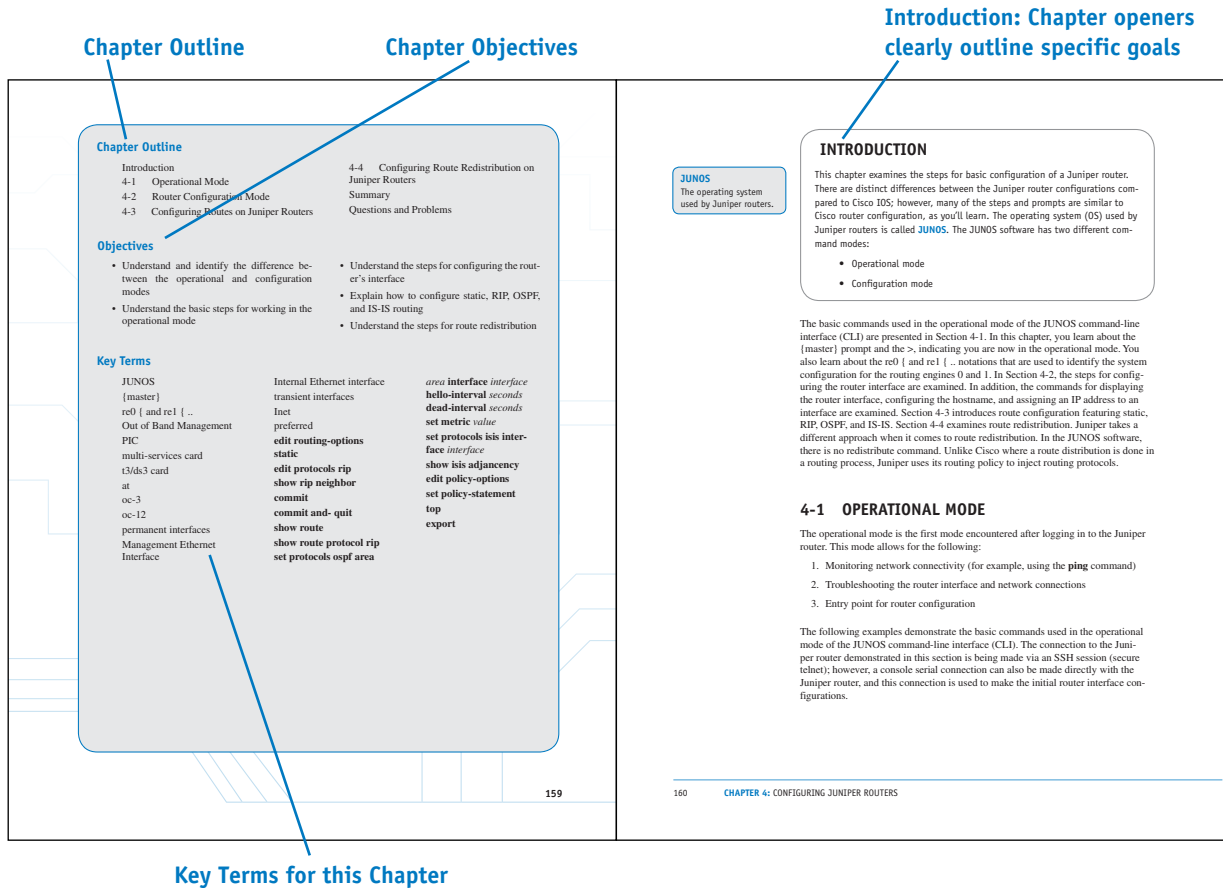


FIGURE P-1

- Net-Challenge Software provides a simulated, hands-on experience in configuring routers and switches. Exercises provided in the text (see Figure P-2) and on the CD challenge readers to undertake certain router/network configuration tasks. The challenges check the students' ability to enter basic networking commands and set up router function, such as configuring the interface (Ethernet and Serial) and routing protocols (that is, static, RIPv2, OSPF, ISIS, EIGRP, BGP, and VLANs). The software has the look and feel of actually being connected to the router's and switch console port.

**Net-Challenge exercises are found throughout the text where applicable**

**Exercises challenge readers to undertake certain tasks**

**Networking Challenge—OSPF**

Use the Net-Challenge Simulator Software included with the text's companion CD-ROM to demonstrate that you can configure OSPF for Router A in the campus LAN (the campus LAN is shown in Figure 3-2 and is displayed by clicking the View Topology button when the software is started). Place the Net-Challenge CD-ROM in your computer's drive. Open the Net-Challenge folder and click **NetChallenge V3-2.exe**. When the software is running, click the **Select Router Challenge** button to open a **Select Router Challenge** drop-down menu. Select **Chapter 3—OSPF**. This opens a checkbox that can be used to verify that you have completed all the tasks:

1. Enter the privileged EXEC mode on the router.
2. Enter the router's terminal configuration mode: **Router(config)**.
3. Set the hostname to *Router A*.
4. Configure the FastEthernet0/0 interface with the following:  
IP address: 10.10.20.250  
Subnet mask: 255.255.255.0
5. Enable the FA0/0 interface.
6. Configure the FastEthernet0/1 interface with the following:  
IP address: 10.10.200.1  
Subnet mask: 255.255.255.0
7. Enable the FA0/1 interface.
8. Configure the FastEthernet0/2 interface with the following:  
IP address: 10.10.100.1  
Subnet mask: 255.255.255.0

FIGURE P-2

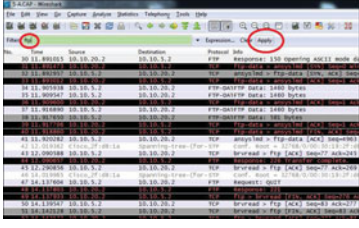
- The textbook features and introduces how to use the *Wireshark Network Protocol Analyzer*. Examples of using the software to analyze data traffic are included throughout the text, as shown in Figure P-3.

Examples using the Wireshark protocol analyzer are included throughout the text where applicable

**FTP Filtering**

The following example demonstrates the process by which Wireshark filtering can be used to isolate File Transfer Protocol (FTP) out of a large list of packets. This can be useful for several reasons. You can use filtering rules to help us find usernames and passwords being used to connect to the FTP servers as well as get an idea of the kind of data that is being transferred.

Start this exercise by opening the capture file 5-A.cap in Wireshark. This is not a huge file, but it's a little difficult to sort through all of it just by looking. Click **Expression** and scroll down until you reach **FTP—File Transfer Protocol (FTP)**. Click **OK** and the Filter for FTP is now displayed, as shown in Figure 6-30.



**FIGURE 6-30** Adding the FTP filter

Click **Apply**, and the packet list is thinned out to 15 total packets relating to the FTP protocol, as shown in Figure 6-31. From this, we are able to view the username and password used to establish the FTP connection. In this case, the username and passwords are listed in plaintext, as well as the file that was accessed. Most times, a secure version of FTP (SFTP) will be used and this information will be encrypted. This same rule can also be applied by using the right-click method as previously shown.

Find a packet that is using the FTP protocol (for example, packet 44). Navigate to the datagram field and select the FTP row. Right click → **Apply as Filter** → **Selected**. This will generate the same results provided in Figure 6-32 that are used for the FTP filter.

256 CHAPTER 6: ANALYZING NETWORK DATA TRAFFIC

FIGURE P-3

- Numerous worked-out examples are included in every chapter to reinforce key concepts and aid in subject mastery, as shown in Figure P-4.

Configuring, analyzing, and troubleshooting sections guide readers through advanced techniques in networking

Screen captures and network topologies guide students through different hands-on activities

**FIGURE 2-11** An example of (a) a contiguous network and (b) a discontiguous network

**Configuring Routes with RIP**

The first step in configuring the router for RIP is to set up the interfaces. This includes assigning an IP address and a subnet mask to the interface using the command `ip address A.B.C.D. subnet-mask`. Next, the interface is enabled using the `no shut` command. The following are the steps for configuring the FastEthernet0/1 interface on Router A in the campus network shown previously in Figure 2-10:

```

Router# conf t
RouterA# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fa0/1
Router(config-if)# ip address 10.10.200.1 255.255.255.0
Router(config-if)# no shut
00:59:03: MLINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1, changed state to up

Next, enter the router's configuration mode [Router(config)#] and input the command router rip to use the RIP routing protocol. The next step is to specify the network that uses RIP for routing. These two steps are shown here:
Router(config)# router rip
Router(config-router)# network 10.0.0.0

```

2-3: CONFIGURING RIPV2 77

**FIGURE 11-15** The exchange of voice packets (code 41) between the two IP phones

**Analyzing VoIP Telephone Call Data Packets**

This section examines the data packets that are being exchanged in a VoIP telephone call. The test setup for the VoIP telephone call is shown in Figure 11-16. This picture shows that the network consists of two VoIP telephones, two call processors, and two routers. The data packets were captured using a network protocol analyzer. The computer running the protocol analyzer and the two call processors were connected to a networking hub so that each share the Ethernet data link. This was done so that all the VoIP data packets being exchanged between the telephones, the call processors, and the routers could be captured at the same time with one protocol analyzer.

**FIGURE 11-16** The test setup for the VoIP telephone call

446 CHAPTER 11: VOICE OVER IP

FIGURE P-4

- Key Terms and their definitions are highlighted in the margins to foster inquisitiveness and ensure retention. This is illustrated in Figure P-5.

Key terms are highlighted in the text and defined in the margin

**Link State Protocol**  
Establishes a relationship with a neighboring router and uses route advertisements to build routing tables.

**Hello Packets**  
Used in the OSPF protocol to verify that the links are still communicating.

**Areas**  
The partition of a large OSPF network into smaller OSPF networks.

**Backbone**  
The primary path for data traffic to and from destinations and sources in the campus network.

**Variable Length Subnet Masks (VLSM)**  
Enables the use of subnet masks to better fit the needs of the network, thereby minimizing the waste of IP addresses when interconnecting subnets.

**Link State Protocols**

Link state protocols establish a relationship with a neighboring router. The routers exchange LSAs to update neighbors regarding route status. The LSAs are sent only if there is a change or loss in the network routes and the link state protocols converge to route selection quickly. This is a distinct advantage over distance vector protocols that exchange updated routing tables at fixed time intervals and are slow to converge. In fact, link state routing protocols are replacing distance vector protocols in most modern networks. Link state protocols are also called *shortest-path first* protocols, based on the algorithm developed by E. W. Dijkstra. Link state protocols use "Hello" packets to verify that communication is still established with neighbor routers. The key issues of link state protocols are summarized as follows:

- Finds neighbors/adjacencies
- Uses route advertisements to build routing table
- Sends "Hello" packets
- Sends updates when routing changes

OSPF sends small "Hello" packets at regular time intervals to adjacent routers to verify that the link between two routers is active and the routers are communicating. If a router fails to respond to a Hello it is assumed that the link or possibly the router is down. The OSPF Hello packet captured with a network protocol analyzer is discussed in Section 3-5.

OSPF uses the concept of **areas** to partition a large network into smaller networks. The advantage of this is that the routers have to calculate routes only for their area. If a route goes down in a given area, only the routers in that area have to calculate new routes. Any number between 0 and 4,294,967,295 ( $2^{32} - 1$ ) can be used; however, area 0 is reserved for the root area, which is the **backbone** for the network. The backbone is the primary path for data traffic to and from destinations and sources in the campus network. All areas must connect to area 0, and area 0 cannot be split. The area numbers can also be expressed in IP notation—for example, area 0 could be 0.0.0.0—or you can specify an area as 192.168.25.0 or in subnet notation. Hence, the need for the large upper-area number ( $2^{32} - 1$ ) = 255.255.255.255 when converted to a decimal number.

OSPF allows the use of **variable length subnet masks (VLSM)**, which enable different size subnets in the network to better meet the needs of the network and more efficiently use the network's limited IP address space. For example, point-to-point inter-router links don't need a large block of addresses assigned to them. Figure 3-1 illustrates an example of an inter-router link.

**FIGURE 3-1** An inter-router link subnetted to provide for two host IP addresses, a network address, and a broadcast address

102 CHAPTER 3: ADVANCED ROUTER CONFIGURATION II

FIGURE P-5

xxi

- Extensive Summaries, Questions, and Problems, as well as Critical Thinking Questions, are found at the end of each chapter, as shown in Figure P-6.

Summary of key concepts

Questions and problems are organized by section

Critical Thinking questions and problems further develop analytical skills

<p><b>SUMMARY</b></p> <p>This chapter presented examples of configuring routing protocols. The network challenge exercises provided the opportunity for the student to test her or his configuration skill prior to actually configuring a real router. The student should be able to configure and verify operation of the following protocols:</p> <ul style="list-style-type: none"> <li>Static</li> <li>RIP/RIPv2</li> <li>OSPF</li> <li>ISIS</li> <li>EIGRP</li> </ul> <p>Additionally, this chapter examined the steps for route redistribution. The last section examined the OSPF Hello packets.</p> <p><b>QUESTIONS AND PROBLEMS</b></p> <p><b>Section 3-1</b></p> <p>1. OSPF is (select all that apply)</p> <ol style="list-style-type: none"> <li>a. Open Shortest Path First routing protocol</li> <li>b. An open protocol</li> <li>c. Developed specifically for TCP/IP networks</li> <li>d. Developed specifically for IPX networks</li> <li>e. A distance vector protocol</li> <li>f. A dynamic routing protocol</li> <li>g. A link state protocol</li> <li>h. A high consumer of bandwidth</li> </ol> <p>2. In OSPF, route updates are sent in the form of</p> <ol style="list-style-type: none"> <li>a. Link state advertisements</li> <li>b. Exchanging routing tables every 30 seconds</li> <li>c. Exchanging routing tables every 90 seconds</li> <li>d. IETF packets</li> </ol> <p>3. The OSPF routing protocol uses these to verify that a link between two routers is active and the routers are communicating</p> <ol style="list-style-type: none"> <li>a. LSAs</li> <li>b. Hello packets</li> <li>c. ARP messages</li> <li>d. Ping</li> </ol>	147	154	<p>62. OSPF multicasts are sent out as what class of address?</p> <ol style="list-style-type: none"> <li>a. Class A</li> <li>b. Class B</li> <li>c. Class C</li> <li>d. Class D</li> <li>e. Class E</li> </ol> <p>63. OSPF Hello packets are sent out every</p> <ol style="list-style-type: none"> <li>a. 30 seconds</li> <li>b. 90 seconds</li> <li>c. 10 seconds</li> <li>d. None of these answers are correct</li> </ol> <p>64. The Router ID (RID) in OSPF Hello packets is chosen from</p> <ol style="list-style-type: none"> <li>a. Loopback addresses</li> <li>b. OSPF 16P_Router</li> <li>c. Highest IP address on an interface</li> <li>d. a and c</li> <li>e. b and c</li> </ol> <p><b>Critical Thinking</b></p> <p>65. You are configuring a router connection to a remote network. What protocol would you select if there is only one network route to the remote network? Explain why you selected the protocol.</p> <p>66. You are configuring the routing protocols for a small network. What routing protocol would you select and why?</p> <p>67. Router A and Router B are connected and both are running OSPF protocol. The following is a sample configuration from Router A:</p> <pre> interface FastEthernet0/0 ip address 10.10.3.1 255.255.255.252 duplex auto speed auto ! interface FastEthernet0/1 ip address 10.100.1.1 255.255.255.0 duplex auto speed auto ! ip route 172.16.0.0 255.255.0.0 Null 0 ! router ospf 200 network 10.0.0.0 0.255.255.255 area 0 </pre>
---	-----	-----	---

FIGURE P-6

- An extensive Glossary is found at the end of this book and offers quick, accessible definitions to key terms and acronyms, as well as an exhaustive Index (see Figure P-7).

## Complete Glossary of terms and acronyms provide quick reference

## Exhaustive Index provides quick reference

<p><b>6to4 Prefix</b> A technique that enables IPv6 hosts to communicate over the IPv4 Internet.</p> <p><b>802.1Q</b> This standard defines a system of VLAN tagging for Ethernet frames.</p> <p><b>2001:DB8::/32 Prefix</b> This IPv6 address prefix is reserved for documentation. This is recommended by RFC3849 to reduce the likelihood of conflict and confusion when using the IPv6 address in examples, books, documentation, or even in test environments.</p> <p><b>.int</b> Intergovernmental domain registries is used for registering organizations established by international treaties between or among national governments.</p> <p><b>(master)</b> The prompt indicating you are in the master routing engine mode on a Juniper router.</p> <p><b>A Record (Address Record)</b> This maps a hostname to an IP address.</p> <p><b>AAA</b> Authentication, Authorization, and Accounting.</p> <p><b>ABR</b> Area border routers.</p> <p><b>Access Layer</b> Where the networking devices in a LAN connect together.</p> <p><b>Access Lists (ACL)</b> A basic form of firewall protection used to tell a networking device who and what are allowed to enter or exit a network.</p> <p><b>ACK</b> Acknowledgment packet.</p> <p><b>address-family ipv6</b> The command used to specify that IPv6 is specified.</p> <p><b>Administrative Distance (AD)</b> A number assigned to a protocol or route to declare its reliability.</p> <p><b>Advertise</b> The sharing of route information.</p> <p><b>AES</b> Advance Encryption Standard. A 128-bit block data encryption technique.</p> <p><b>AF33</b> Assured Forwarding class 3. Created to ensure the VoIP signaling or handshake.</p> <p><b>AH</b> Authentication Header. A security protocol used by IPsec that guarantees the authenticity of the IP packets.</p> <p><b>AMI</b> Alternate mark inversion. A fundamental line coding scheme developed for transmission over T1 circuits.</p> <p><b>Anycast Address</b> Obtained from a list of addresses.</p> <p><b>Area 0</b> In OSPF, this is the root area and is the backbone for the network.</p> <p><b>Area ID</b> Analogous to OSPF area number, and it is used by L2 routers.</p> <p><b>Areas</b> The partition of a large OSPF network into smaller OSPF networks.</p> <p><b>ARIN</b> American Registry for Internet Numbers. Allocates Internet Protocol resources, develops consensus-based policies, and facilitates the advancement of the Internet through information and educational outreach.</p> <p><b>ARP</b> Address Resolution Protocol, used to map an IP address to its MAC address.</p> <p><b>arp -a</b> The command used to view the ARP cache.</p> <p><b>ARP Broadcast</b> Used to inform everyone on the network that it now is the owner of the IP address.</p> <p><b>ARP Reply</b> A network protocol where the MAC address is returned.</p> <p><b>AS</b> Autonomous System. These numbers are used by various routing protocols and are a collection of connected Internet Protocol (IP) routing prefixes. Autonomous systems separate organizational networks.</p> <p><b>ASN</b> Autonomous systems number is used to distinguish separate networks and to prevent routing loops.</p> <p><b>at</b> Asynchronous Transmission Mode (ATM) connection for a Juniper router.</p> <p><b>ATM</b> Asynchronous transfer mode.</p> <p><b>Authoritative Name Server</b> A name server that is authorized and configured to answer DNS queries for a particular domain or zone.</p> <p><b>Automatic Private IP Addressing (APIPA)</b> A self-assigned IP address in the range of 169.254.1.0-169.254.254.255.</p> <p><b>autonomous-system [AS_Number]</b> This command is used in JUNOS to define the BGP AS for the router.</p> <p><b>B8Z5</b> Bipolar 8 zero substitution. A data encoding format developed to improve data transmission over T1 circuits.</p> <p><b>Backbone</b> The primary path for data traffic to and from destinations and sources in the campus network.</p> <p><b>Backup Designated Router (BDR)</b> The router or routers with lower priority.</p>	<p><b>Numbers</b></p> <p><b>3DES</b> (Triple Data Encryption Standard), ESP, 306</p> <p><b>6to4 prefix (IPv6 addresses), 314</b></p> <p><b>802.1Q, 18, 24-26</b></p> <p><b>2001, DB8::/32 prefix and IPv6 router configuration, 324</b></p> <p><b>Symbols</b></p> <p>? (question mark), JUNOS operating system, 161</p> <p><b>A</b></p> <p><b>AAA</b> (Authentication, Authorization, and Accounting), 281</p> <p><b>ABR</b> (area border routers), 112</p> <p><b>access layer, 6</b></p> <p><b>access-list 100 deny udp any any eq 161 command, ACL configuration, 273</b></p> <p><b>access-list 100 deny udp any any eq snmp command, ACL configuration, 274</b></p> <p><b>access-list permit ip any any command, ACL configuration, 274</b></p> <p><b>accounting (security), 281</b></p> <p><b>ACK</b> (Acknowledgment) packets, TCP three-way handshakes, 230</p> <p><b>ACL</b> (Access Lists), 270-272. See also filter lists</p> <p><b>access-list 100 deny udp any any eq 161 command, 273</b></p> <p><b>access-list 100 deny udp any any eq snmp command, 274</b></p> <p><b>access-list permit ip any any command, 274</b></p> <p><b>configure terminal command, 273</b></p> <p><b>edge routers, 273-275</b></p> <p><b>extended ACL, 273</b></p> <p><b>false TCP headers, 278</b></p> <p><b>hosts, 277</b></p> <p><b>ip access-group 100 out command, 274</b></p> <p><b>IP addresses, stopping data traffic from, 277-278</b></p> <p><b>permit ip any any command, 274-276</b></p> <p><b>placement of, 274</b></p> <p><b>removing data hosts, stopping data traffic from, 277</b></p> <p><b>router logging, 283-285</b></p> <p><b>show access-list 100 command, 274</b></p> <p><b>show access-list command, 275-276</b></p> <p><b>SMB, 273-275</b></p> <p><b>standard ACL, 273</b></p> <p><b>UDP, 276</b></p> <p><b>AD</b> (Administrative Distance), 71</p> <p><b>address family ipv6 command, IPv6 Internet routing via BGP4+, 413</b></p> <p><b>Address field</b> (show ip eigrp neighbors command), 125</p> <p><b>administration (Linux), 389</b></p> <p><b>!v system-config -v command, 385</b></p> <p><b>security, 387</b></p> <p><b>system-config: [tool-name] command, 385</b></p> <p><b>system-config-date command, 386</b></p> <p><b>system-config-network command, 388</b></p> <p><b>administration commands (Linux)</b></p> <p><b>df command, 363</b></p> <p><b>df -h command, 364</b></p> <p><b>history command, 364</b></p> <p><b>kill (PID) command, 361</b></p> <p><b>kill -9 (PID) command, 361</b></p> <p><b>man command, 358-359</b></p> <p><b>mount command, 358, 362</b></p> <p><b>ps command, 358-361</b></p> <p><b>shutdown command, 358, 364</b></p> <p><b>shutdown -h now command, 364</b></p> <p><b>su command, 358, 362</b></p> <p><b>Tab key shortcut, 364</b></p> <p><b>umount command, 364</b></p> <p><b>up arrow shortcut, 364</b></p> <p><b>advertise</b> connected policies, Juniper router route redistribution, 179</p> <p><b>advertise_igmp policies, Juniper router route redistribution, 179</b></p> <p><b>advertise_rip policies, Juniper router route redistribution, 179</b></p> <p><b>advertise_static policies, Juniper router route redistribution, 180</b></p> <p><b>advertising networks, 75</b></p> <p><b>AES</b> (Advance Encryption Standard)</p> <p><b>ESQ, 201</b></p> <p><b>WPX2, 201</b></p> <p><b>AF33</b> (Assured Forwarding class 3), VoIP class maps, 441</p> <p><b>AH</b> (Authentication Headers), troubleshooting VPN tunnels, 300</p> <p><b>allow-snmp term</b> (filter lists), 279</p> <p><b>AMI</b> (alternate mark inversion), 38</p> <p><b>anycast IPv6 addresses, 314</b></p> <p><b>AP</b> (access points), NSEL and IS-IS, 113</p> <p><b>APIPA</b> (Automatic Private IP Addressing), 196</p> <p><b>Area ID, IS-IS, 112</b></p> <p><b>areas</b> (OSPF), 102, 105</p> <p><b>A records</b> (Address records), DNS, 214, 218-219</p> <p><b>ARIN</b> (American Registry for Internet Numbers), IP address assignments, 191</p>
---	--

FIGURE P-7

## **Accompanying CD-ROM**

The CD-ROM packaged with the text includes the captured data packets used in the text. It also includes the Net-Challenge Software, which was developed specifically for this text.

## **Instructor Resources**

The Instructor's Manual to accompany *A Practical Guide to Advanced Networking*, (ISBN: 978-0-132-88303-0) provides the entire book in PDF format along with instructor notes for each section within each chapter, recommending key concepts that should be covered in each chapter. Solutions to all Chapter Questions and Problems sections are also included. In addition, the instructor can also access 13 lab and lab-related exercises and a test bank with which to generate quizzes on the material found within the student edition of the book.

*This page intentionally left blank*