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

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

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

TABLE OF CONTENTS

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, DelMar 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

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 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.

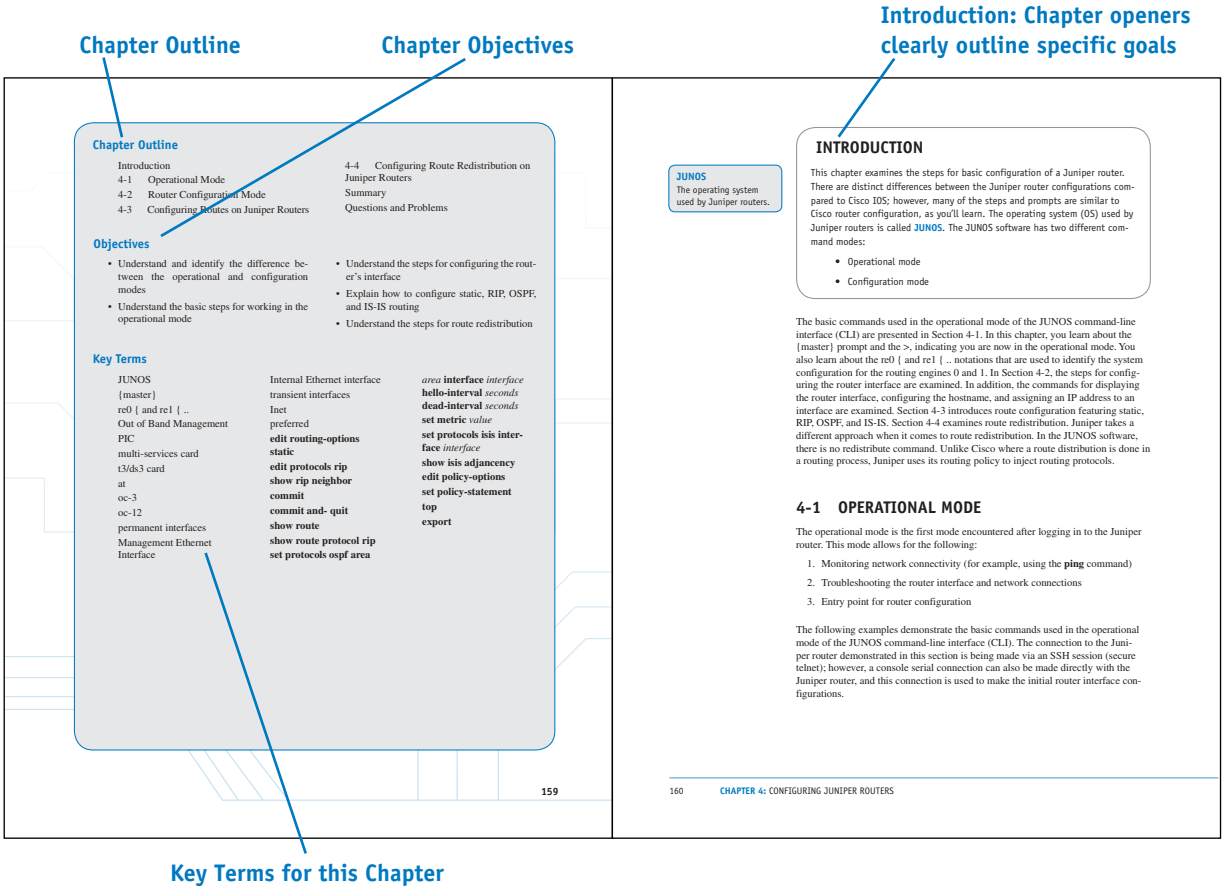


FIGURE P-1

- 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.

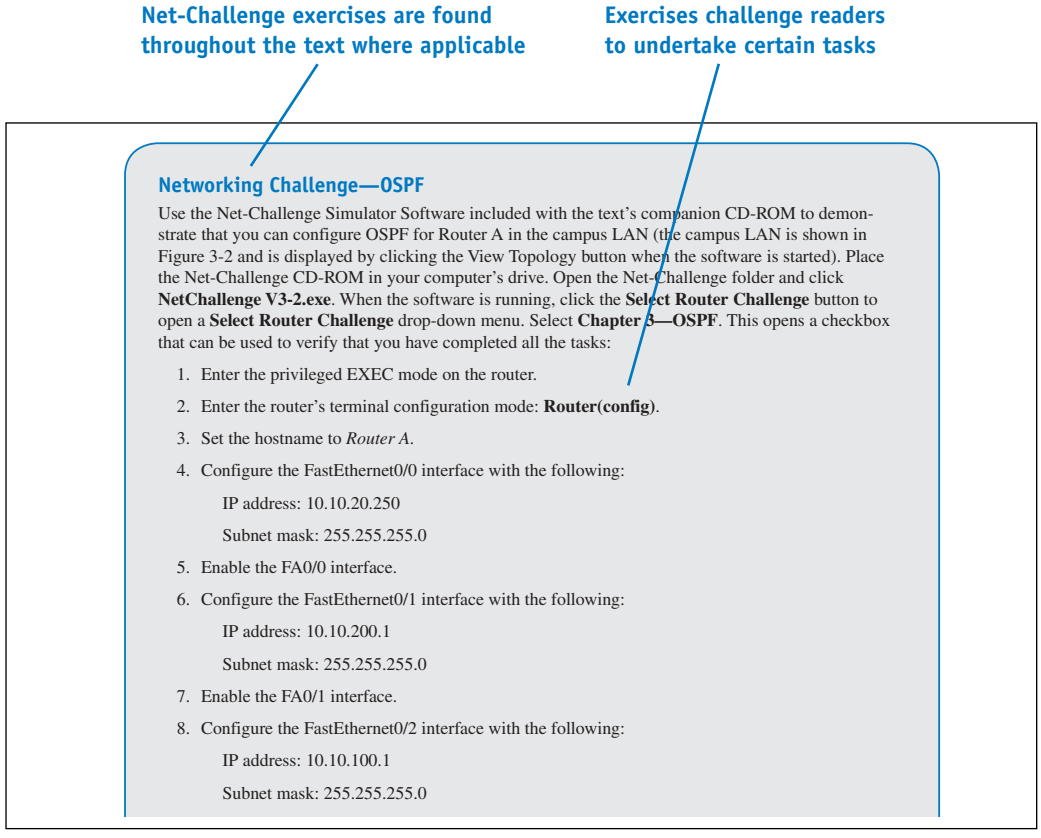
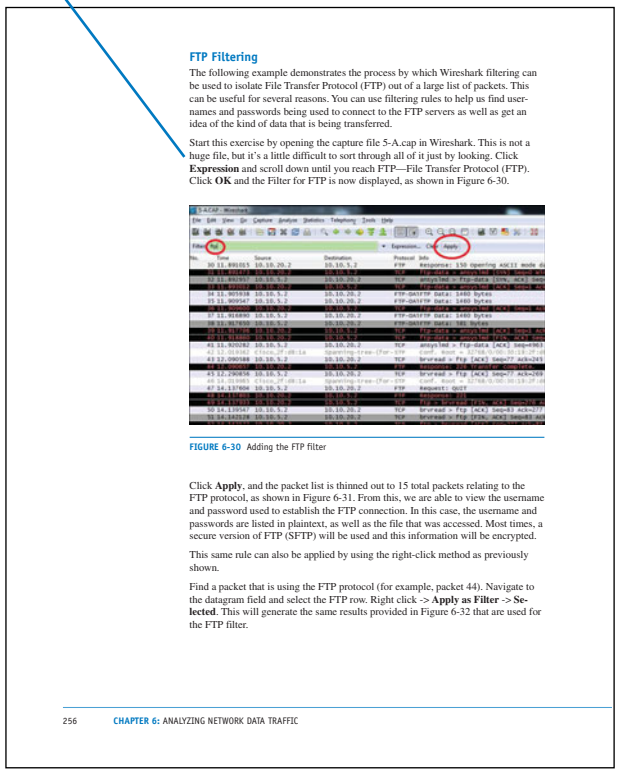


FIGURE P-2

- 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.

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

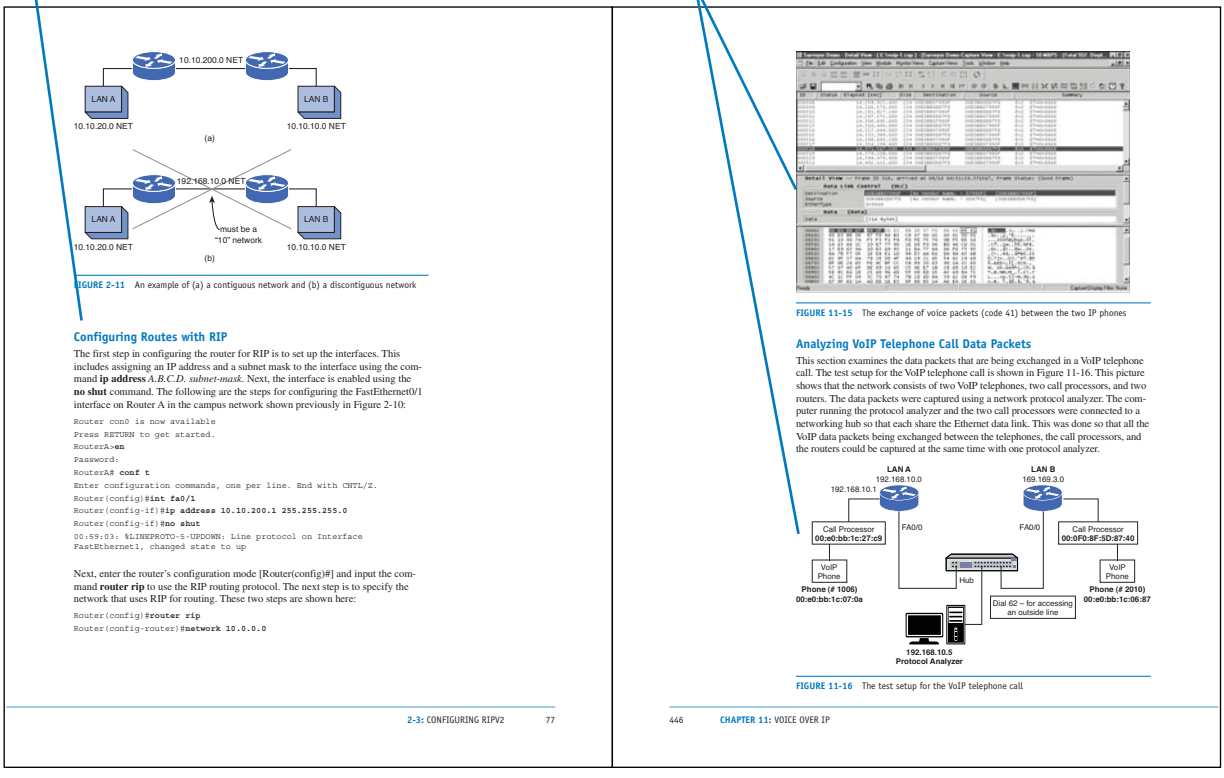
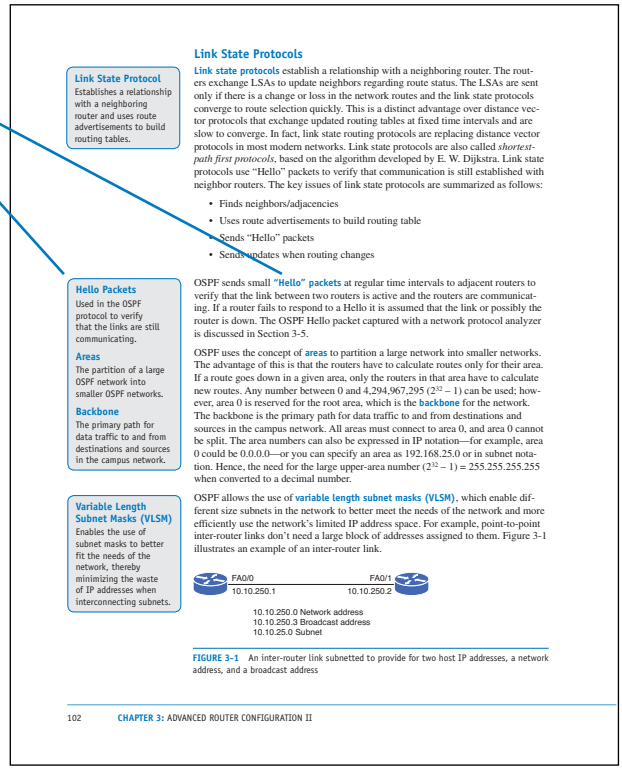


FIGURE P-4

- 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.

10.10.250.0 Network address
10.10.250.3 Broadcast address
10.10.25.0 Subnet

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

FIGURE P-5

- 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.

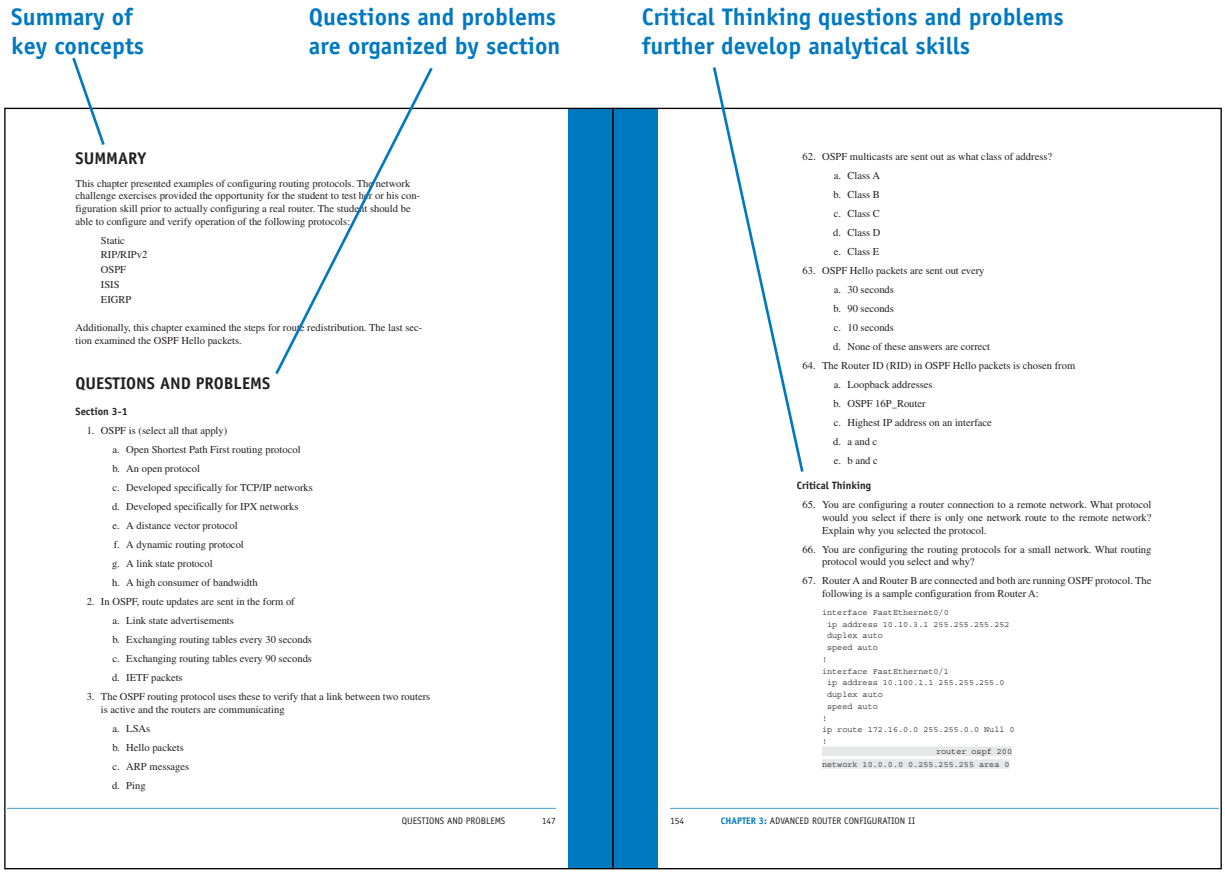
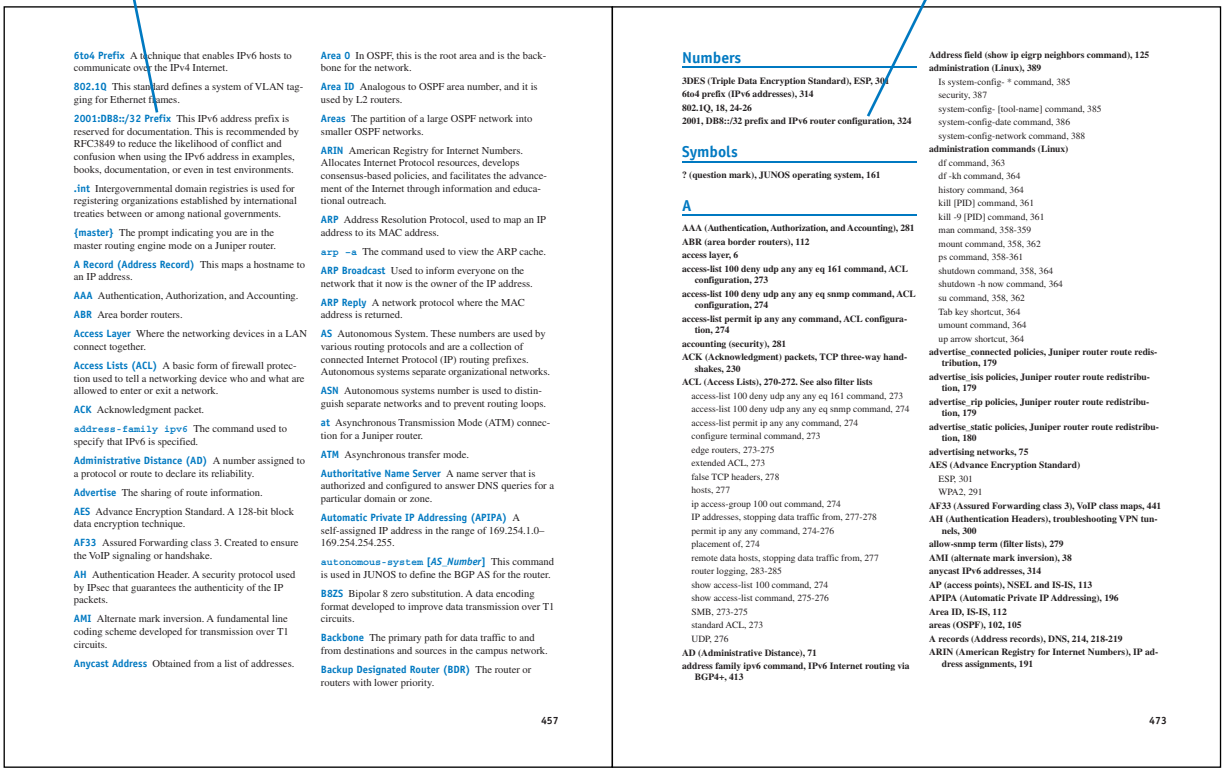


FIGURE P-6

- 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



6to4 Prefix A technique that enables IPv6 hosts to communicate over the IPv4 Internet.

802.1Q This standard defines a system of VLAN tagging for Ethernet frames.

2001:DB8::/32 Prefix 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.

.int Intergovernmental domain registries is used for registering organizations established by international treaties between or among national governments.

{master} The prompt indicating you are in the master routing engine mode on a Juniper router.

A Record (Address Record) This maps a hostname to an IP address.

AAA Authentication, Authorization, and Accounting.

ABR Area border routers.

Access Layer Where the networking devices in a LAN connect together.

Access Lists (ACL) A basic form of firewall protection used to tell a networking device who and what are allowed to enter or exit a network.

ACK Acknowledgment packet.

address-family ipv6 The command used to specify that IPv6 is specified.

Administrative Distance (AD) A number assigned to a protocol or route to declare its reliability.

Advertise The sharing of route information.

AES Advance Encryption Standard. A 128-bit block data encryption technique.

AF33 Assured Forwarding class 3. Created to ensure the VoIP signaling or handshake.

AH Authentication Header. A security protocol used by IPsec that guarantees the authenticity of the IP packets.

AMI Alternate mark inversion. A fundamental line coding scheme developed for transmission over T1 circuits.

Anycast Address Obtained from a list of addresses.

Area 0 In OSPF, this is the root area and is the backbone for the network.

Area ID Analogous to OSPF area number, and it is used by L2 routers.

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

ARIN 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.

ARP Address Resolution Protocol, used to map an IP address to its MAC address.

arp -a The command used to view the ARP cache.

ARP Broadcast Used to inform everyone on the network that it now is the owner of the IP address.

ARP Reply A network protocol where the MAC address is returned.

AS 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.

ASN Autonomous systems number is used to distinguish separate networks and to prevent routing loops.

at Asynchronous Transmission Mode (ATM) connection for a Juniper router.

ATM Asynchronous transfer mode.

Authoritative Name Server A name server that is authorized and configured to answer DNS queries for a particular domain or zone.

Automatic Private IP Addressing (APIPA) A self-assigned IP address in the range of 169.254.1.0–169.254.254.255.

autonomous-system *[AS_Number]* This command is used in JUNOS to define the BGP AS for the router.

B8ZS Bipolar 8 zero substitution. A data encoding format developed to improve data transmission over T1 circuits.

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

Backup Designated Router (BDR) The router or routers with lower priority.

457

Numbers

Symbols

A

473

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