

A Practical Guide to Advanced Networking

Third Edition

Jeffrey S. Beasley
Piyasat Nilkaew

Software Enclosed



FREE SAMPLE CHAPTER



SHARE WITH OTHERS

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

TABLE OF CONTENTS

Introduction

xvi

CHAPTER 1 Network Infrastructure Design 2

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

CHAPTER 2	Advanced Router Configuration I	52
	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
CHAPTER 3	Advanced Router Configuration II	98
	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

CHAPTER 5	CONFIGURING AND MANAGING THE NETWORK INFRASTRUCTURE	188
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
CHAPTER 6	Analyzing Network Data Traffic	226
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

CHAPTER 7 Network Security	266
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
 CHAPTER 8 IPv6	 306
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
 CHAPTER 9 Linux Networking	 336
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
CHAPTER 10	Internet Routing	396
	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
CHAPTER 11	Voice over IP	428
	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

Key Terms Glossary	456
---------------------------	------------

Index	472
--------------	------------

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.

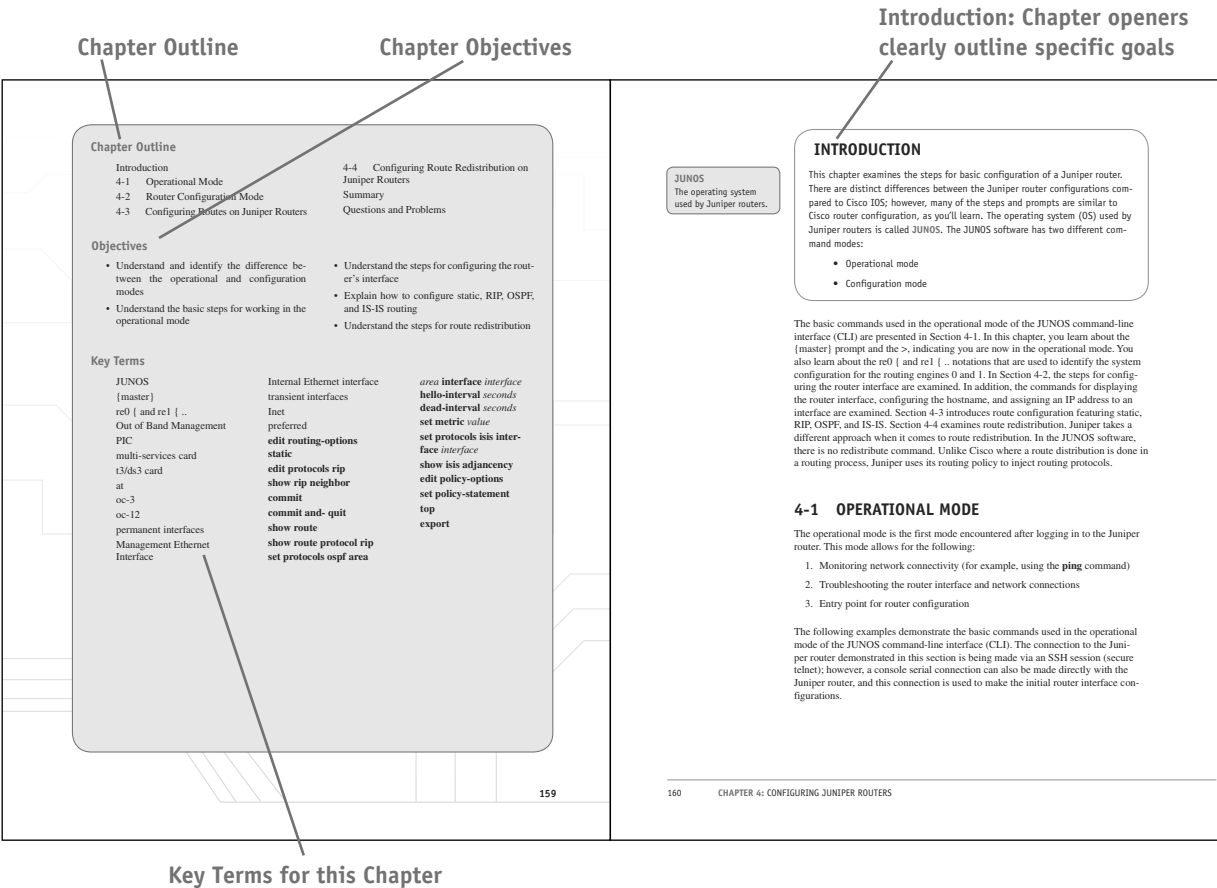


FIGURE P-1

- 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.

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

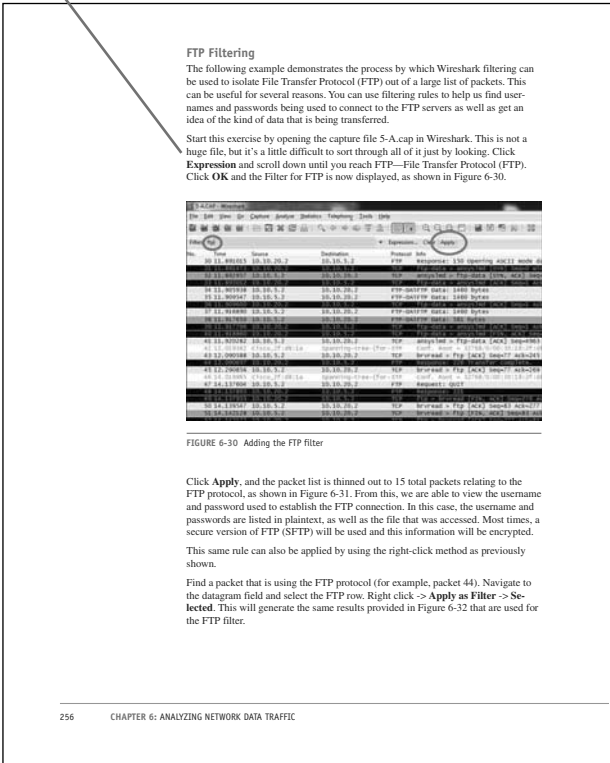


FIGURE P-3

- 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

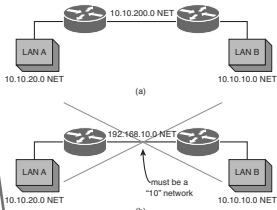


FIGURE 2-11 An example of (a) a contiguous network and (b) a discontinuous network

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
Press RETURN to get started.
RouterA>en
Password:
RouterA# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip address 10.10.200.1 255.255.255.0
Router(config-if)#no shut
00:59:03: LINEPROTO-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 RIPV277

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




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.

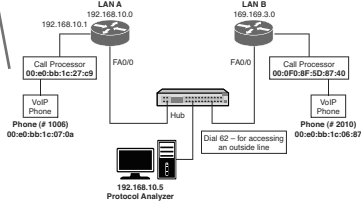


FIGURE 11-16 The test setup for the VoIP telephone call

446CHAPTER 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

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.

Summary of key concepts

Questions and problems are organized by section

Critical Thinking questions and problems further develop analytical skills

<p>SUMMARY</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"> Static RIP/RIPv2 OSPF ISIS EIGRP <p>Additionally, this chapter examined the steps for route redistribution. The last section examined the OSPF Hello packets.</p> <p>QUESTIONS AND PROBLEMS</p> <p>Section 3-1</p> <ol style="list-style-type: none"> 1. OSPF is (select all that apply) <ol style="list-style-type: none"> a. Open Shortest Path First routing protocol b. An open protocol c. Developed specifically for TCP/IP networks d. Developed specifically for IPX networks e. A distance vector protocol f. A dynamic routing protocol g. A link state protocol h. A high consumer of bandwidth 2. In OSPF, route updates are sent in the form of <ol style="list-style-type: none"> a. Link state advertisements b. Exchanging routing tables every 30 seconds c. Exchanging routing tables every 90 seconds d. IETF packets 3. The OSPF routing protocol uses these to verify that a link between two routers is active and the routers are communicating <ol style="list-style-type: none"> a. LSAs b. Hello packets c. ARP messages d. Ping 	<p>QUESTIONS AND PROBLEMS 147</p>	<ol style="list-style-type: none"> 62. OSPF multicasts are sent out as what class of address? <ol style="list-style-type: none"> a. Class A b. Class B c. Class C d. Class D e. Class E 63. OSPF Hello packets are sent out every <ol style="list-style-type: none"> a. 30 seconds b. 90 seconds c. 10 seconds d. None of these answers are correct 64. The Router ID (RID) in OSPF Hello packets is chosen from <ol style="list-style-type: none"> a. Loopback addresses b. OSPF 16P_Router c. Highest IP address on an interface d. a and c e. b and c <p>Critical Thinking</p> <ol style="list-style-type: none"> 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. 66. You are configuring the routing protocols for a small network. What routing protocol would you select and why? 67. Router A and Router B are connected and both are running OSPF protocol. The following is a sample configuration from Router A: <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>6to4 Prefix A technique that enables IPv6 hosts to communicate over the IPv4 Internet.</p> <p>802.1Q This standard defines a system of VLAN tagging for Ethernet frames.</p> <p>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.</p> <p>.int Intergovernmental domain registries is used for registering organizations established by international treaties between or among national governments.</p> <p>(master) The prompt indicating you are in the master routing engine mode on a Juniper router.</p> <p>A Record (Address Record) This maps a hostname to an IP address.</p> <p>AAA Authentication, Authorization, and Accounting.</p> <p>ABR Area border routers.</p> <p>Access Layer Where the networking devices in a LAN connect together.</p> <p>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.</p> <p>ACK Acknowledgment packet.</p> <p>address-family ipv6 The command used to specify that IPv6 is specified.</p> <p>Administrative Distance (AD) A number assigned to a protocol or route to declare its reliability.</p> <p>Advertise The sharing of route information.</p> <p>AES Advance Encryption Standard. A 128-bit block data encryption technique.</p> <p>AF33 Assured Forwarding class 3. Created to ensure the VoIP signaling or handshake.</p> <p>AH Authentication Header. A security protocol used by IPsec that guarantees the authenticity of the IP packets.</p> <p>AMI Alternate mark inversion. A fundamental line coding scheme developed for transmission over T1 circuits.</p> <p>Anycast Address Obtained from a list of addresses.</p> <p>Area 0 In OSPF, this is the root area and is the backbone for the network.</p> <p>Area ID Analogous to OSPF area number, and it is used by L2 routers.</p> <p>Areas The partition of a large OSPF network into smaller OSPF networks.</p> <p>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.</p> <p>ARP Address Resolution Protocol, used to map an IP address to its MAC address.</p> <p>arp -a The command used to view the ARP cache.</p> <p>ARP Broadcast Used to inform everyone on the network that it now is the owner of the IP address.</p> <p>ARP Reply A network protocol where the MAC address is returned.</p> <p>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.</p> <p>ASN Autonomous systems number is used to distinguish separate networks and to prevent routing loops.</p> <p>at Asynchronous Transmission Mode (ATM) connection for a Juniper router.</p> <p>ATM Asynchronous transfer mode.</p> <p>Authoritative Name Server A name server that is authorized and configured to answer DNS queries for a particular domain or zone.</p> <p>Automatic Private IP Addressing (APIPA) A self-assigned IP address in the range of 169.254.1.0–169.254.254.255.</p> <p>autonomous-system [AS-Number] This command is used in JUNOS to define the BGP AS for the router.</p> <p>B8ZS Bipolar 8 zero substitution. A data encoding format developed to improve data transmission over T1 circuits.</p> <p>Backbone The primary path for data traffic to and from destinations and sources in the campus network.</p> <p>Backup Designated Router (BDR) The router or routers with lower priority.</p> <p>457</p>	<p>Numbers</p> <p>3DES (Triple Data Encryption Standard), ESP, 304</p> <p>6to4 prefix (IPv6 addresses), 314</p> <p>802.1Q, 18, 24–26</p> <p>2001, DB8::/32 prefix and IPv6 router configuration, 324</p> <p>Symbols</p> <p>? (question mark), JUNOS operating system, 161</p> <p>A</p> <p>AAA (Authentication, Authorization, and Accounting), 281</p> <p>ABR (area border routers), 112</p> <p>access layer, 6</p> <p>access-list 100 deny udp any any eq 161 command, ACL configuration, 273</p> <p>access-list 100 deny udp any any eq snmp command, ACL configuration, 274</p> <p>access-list permit ip any any command, ACL configuration, 274</p> <p>accounting (security), 281</p> <p>ACK (Acknowledgment) packets, TCP three-way handshakes, 230</p> <p>ACL (Access Lists), 270–272. See also filter lists</p> <p>access-list 100 deny udp any any eq 161 command, 273</p> <p>access-list 100 deny udp any any eq snmp command, 274</p> <p>access-list permit ip any any command, 274</p> <p>configure terminal command, 273</p> <p>edge routers, 273–275</p> <p>extended ACL, 273</p> <p>false TCP headers, 278</p> <p>hosts, 277</p> <p>ip access-group 100 out command, 274</p> <p>IP addresses, stopping data traffic from, 277–278</p> <p>permit ip any any command, 274–276</p> <p>placement of, 274</p> <p>routing data hosts, stopping data traffic from, 277</p> <p>router logging, 283–285</p> <p>show access-list 100 command, 274</p> <p>show access-list command, 275–276</p> <p>SMB, 273–275</p> <p>standard ACL, 273</p> <p>UDP, 276</p> <p>AD (Administrative Distance), 71</p> <p>address family ipv6 command, IPv6 Internet routing via BGP4+, 413</p> <p>Address field (show ip eigrp neighbors command), 125</p> <p>administration (Linux), 389</p> <p>! system-config -> command, 385</p> <p>security, 387</p> <p>system-config: [tool-name] command, 385</p> <p>system-config-date command, 386</p> <p>system-config-network command, 388</p> <p>administration commands (Linux)</p> <p>df command, 363</p> <p>df -h command, 364</p> <p>history command, 364</p> <p>kill (PID) command, 361</p> <p>kill -9 (PID) command, 361</p> <p>man command, 358–359</p> <p>mount command, 358, 362</p> <p>ps command, 358–361</p> <p>shutdown command, 358, 364</p> <p>shutdown -h now command, 364</p> <p>su command, 358, 362</p> <p>Tab key shortcut, 364</p> <p>umount command, 364</p> <p>up arrow shortcut, 364</p> <p>advertise, connected policies, Juniper router route redistribution, 179</p> <p>advertise, isis policies, Juniper router route redistribution, 179</p> <p>advertise, rip policies, Juniper router route redistribution, 179</p> <p>advertise, static policies, Juniper router route redistribution, 180</p> <p>advertising networks, 75</p> <p>AES (Advance Encryption Standard)</p> <p>ESP, 301</p> <p>WPA2, 291</p> <p>AF33 (Assured Forwarding class 3), VoIP class maps, 441</p> <p>AH (Authentication Headers), troubleshooting VPN tunnels, 300</p> <p>allow-snmp term (filter lists), 279</p> <p>AMI (alternate mark inversion), 38</p> <p>anycast IPv6 addresses, 314</p> <p>AP (access points), NSEL and IS-IS, 113</p> <p>APIPA (Automatic Private IP Addressing), 196</p> <p>Area ID, IS-IS, 112</p> <p>areas (OSPF), 102, 105</p> <p>A records (Address records), DNS, 214, 218–219</p> <p>ARIN (American Registry for Internet Numbers), IP address assignments, 191</p> <p>473</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



8

CHAPTER

IPV6

Chapter Outline

Introduction

8-1 Comparison of IPv6 and IPv4

8-2 IPv6 Addressing

8-3 IPv6 Network Settings

8-4 Configuring a Router for IPv6

8-5 IPv6 Routing

8-6 Troubleshooting the IPv6 Connection

Questions and Problems

Summary

Objectives

- Develop an understanding of the fundamentals of IPv6
- Define the structure of IPv6
- Understand the IPv6 addressing and its prefix
- Be able to represent the IPv6 with correct notation
- Be able to configure basic IPv6 on computers
- Be able to configure basic IPv6 on routers
- Recognize the IPv6 stateless autoconfiguration settings
- Be able to provide basic IPv6 troubleshooting

Key Terms

IPv6

IPng

datagram

IPsec

stateless address autoconfiguration (SLAAC)

full IPv6 address

double-colon notation

network prefix

prefix length

interface identifier

unicast address

global unicast address

multicast address

anycast address

6to4 prefix

FP

TLA ID (0x2002)

V4ADDR

SLA ID

Interface ID

IPv6 stateless autoconfiguration

link-local address

FE80::/64

Neighbor Solicitation

Duplicate Address Detection (DAD)

Privacy Extensions for Stateless Address Autoconfiguration

MLD (Multicast Listener Discovery)

ipv6 unicast-routing

ipv6 enable

show ipv6 interface

ipv6 address *ipv6 interface address*

eui-64

ND protocol

RA messages

router solicitation messages

2001:DB8::/32 Prefix

RIPng

rip_tag

OSPFv3

ping6

traceroute6/tracert6

INTRODUCTION

This chapter looks at IPv6, the IP addressing system that has been developed to replace IPv4. IP version 4 (IPv4) is the current TCP/IP addressing technique being used on the Internet. The address space for IPv4 is running out, even though there is a theoretical limit of approximately 4.3 billion unique IPv4 addresses. However, not all the IPv4 addresses can be used, because there are IPv4 address blocks reserved for special purposes, such as multicast, unspecified future use, local identification, loopback, and private use. These special purpose reserved addresses account for around 600 million unique addresses.

Address space for IPv4 is quickly running out due to the rapid growth of the Internet and the development of new Internet-compatible mobile technologies. Examples of this include the IP addressable telephone, wireless personal digital assistants (PDAs), cell phones, game consoles, and home-networking systems. There have been many predictions of when the IPv4 address pool will be exhausted. The answer to this question is not clear. Techniques such as Network Address Translation/Port Address Translation (NAT/PAT), Dynamic Host Control Protocol (DHCP), and Classless Inter-Domain Routing (CIDR) have been implemented to prolong the life of IPv4. These techniques reuse the existing IPv4 address space and handle the address space allocation more efficiently.

IPv6

IP version 6.

IPng

Next generation IP.

A solution to the limited number of available IPv4 addresses is to migrate to IPv6. IP version 6 (**IPv6**) is the solution proposed by the Internet Engineering Task Force (IETF) for expanding the possible number of IP addresses to accommodate the growing users on the Internet. IPv6, introduced in 1999, is also called **IPng**.

This chapter provides a comparison of IPv6 and IPv4 in Section 8-1. The structure of the IPv6 address is examined in Section 8-2. Concepts such as the network prefix and the prefix length are examined. IPv6 network settings are examined in Section 8-3. Steps for configuring IPv6 in both the Windows and Mac OS X environments are examined. The steps for configuring a router to run IPv6 are examined in section 8-4. This chapter concludes with a look at troubleshooting the IPv6 connection in Section 8-5.

8-1 COMPARISON OF IPV6 AND IPV4

IPv4 and IPv6 are not compatible technologies, and they cannot communicate directly with each other. So, before migrating to an IPv6 environment, the network devices and network equipment need to be IPv6 compatible or enabled. Most likely new network hardware and software will have to be acquired to make the network IPv6 ready. A good migration plan has to be developed to prepare for IPv6. The investment of time, money, and training is required for a successful adoption of IPv6.

The size of the IPv6 address is increased to 128 bits, which is four times larger than the 32-bit address space IPv4 is using. This significantly increases the number of available IP addresses. By doing this, the theoretical number of unique addresses increases from 4.3x10⁹ (IPv4) to 3.4x10³⁸ in IPv6. This is a staggering number considering the world population is 7x10⁹ people.

Increasing the number of bits for the address also results in changing the IP header size. The IPv4 **datagram** is shown in Figure 8-1. A datagram is a self-contained entity that carries sufficient information to be routed from source to destination without relying on previous data exchanges between the source and destination computers or the transporting network.

The IPv4 header size is comprised of the information detailed in Figure 8-1. A total of 64 bits are used to define the source and destination IP addresses. Note that both the source and destination addresses are 32 bits in length. The combination of the two gives 64 bits. The total length of the IPv4 header is 160 bits; therefore, this means 160 – 64 = 96 bits are used to make up the remaining fields.

Datagram
A self-contained entity that carries sufficient information to be routed from source to destination without relying on previous data exchanges between the source and destination computers or the transporting network.

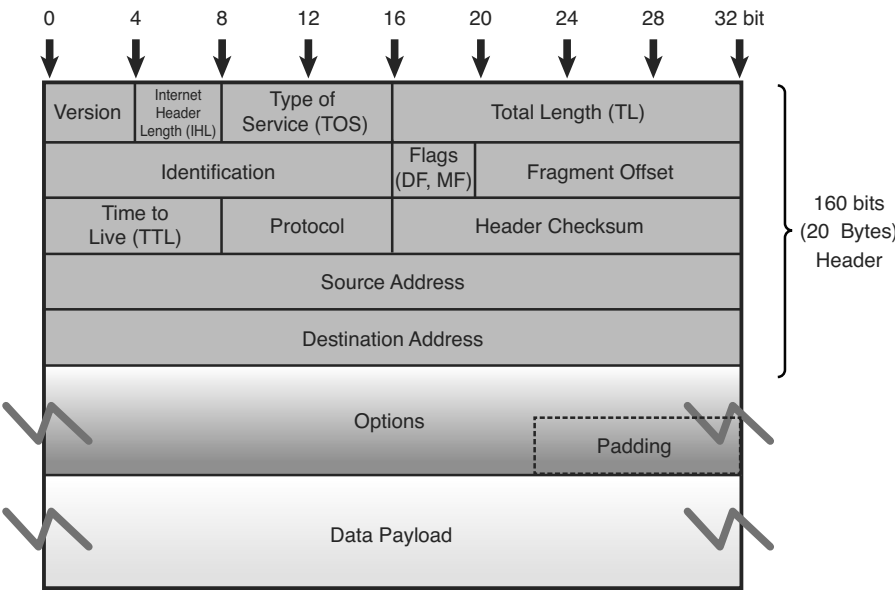


FIGURE 8-1 The IPv4 Datagram (160 bits-96 bits for header fields)

Figure 8-2 shows the IPv6 datagram. The IPv6 header size is 320 bits; however, 256 bits are used to define the source and destination IPv6 addresses. This means that 64 bits are used to define the remaining field as compared to 96 bits for IPv4.

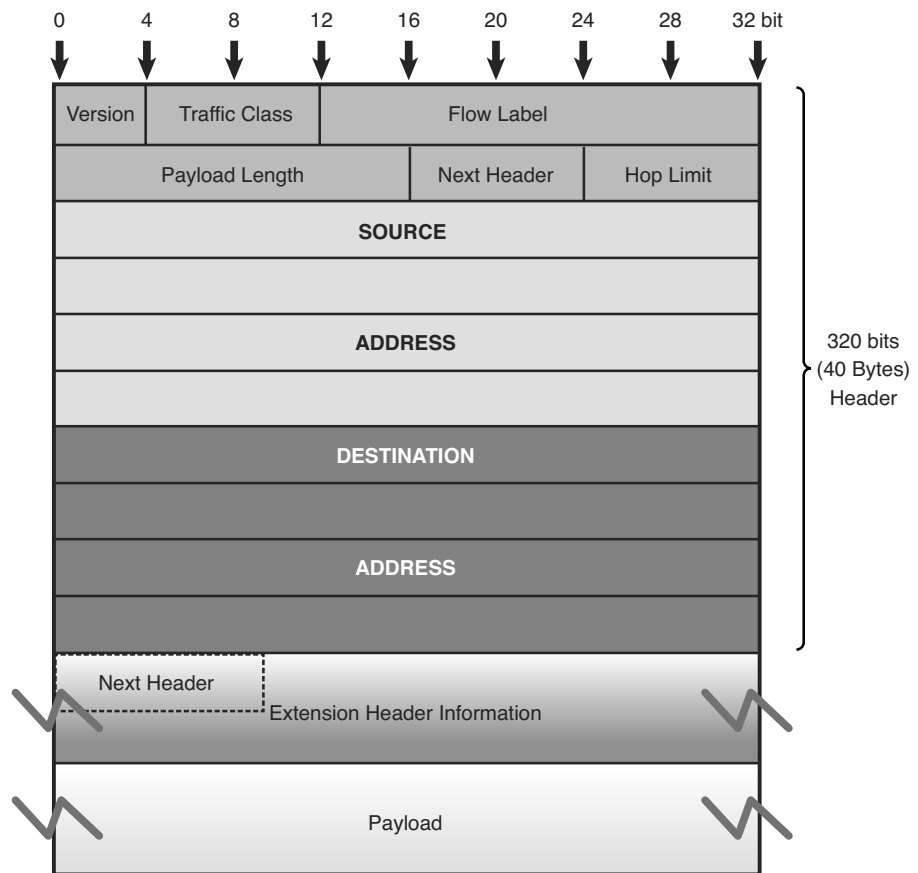


FIGURE 8-2 The IPv6 Datagram (320 bits-64 bits for header fields)

The IPv6 header has been simplified resulting in less header fields than in IPv4. This is designed to make packet processing more efficient by routers and other network equipments. One noticeably missing header field in IPv6 is the checksum field. This means there is no checksum calculation done by the routers in the path. This increases the routing performance and efficiency. The error detection is now done at the link layer and transport layer. In IPv4, the TCP transport layer is required to check the integrity of the packet by doing a checksum calculation. The same cannot be said for the UDP transport layer because the checksum is optional. Now, the checksums are required for both transport layers in IPv6.

IPsec

The IETF standard for securing the IP communications between the network nodes by authenticating and encrypting the session.

One new feature that is built in with IPv6 is the IP security (IPsec). **IPsec** is the IETF standard for securing the IP communications between the network nodes by authenticating and encrypting the session. When using IPv4, a secure network IP communication link generally has to be initiated to provide security similar to an IPsec application. In IPv6, every node is enabled with the IPsec feature. This makes creating end-to-end IPsec sessions much easier to establish. In addition, IPsec feature is a part of the extension headers. In IPv6, there is a mandatory IPv6 main header and then there could be an extension header or extension headers. All

options and special purposed fields can be provisioned into extension headers when needed. IPSec is one of the special options. This is how IPv6 simplifies its header fields.

Another giant step forward taken by IPv6 is the elimination of the broadcast. Broadcasts can cause many problems in computer networks. When a broadcast happens, every computer on the network is interrupted, even if only two computers are involved. The worst case situation is a broadcast storm. When this happens, the performance on a network is severely degraded, and it can bring down an entire network. IPv6 does not use broadcasts. It uses multicasts instead. A multicast is used in the core of many functions in IPv6. The multicast addresses are allocated from the multicast block. Any address starting with “1111 1111” in binary or “FF” in colon hexadecimal notation is an IPv6 multicast address. The concept of colon hexadecimal notation is discussed in Section 8-2. Even though there is no such thing as broadcast, there is a multicast address to the all-host multicast group.

Stateless address autoconfiguration (SLAAC) is another important feature of IPv6. This feature allows for a server-less basic network configuration of the IPv6 computers. With IPv4, a computer generally obtains its network settings from a DHCP server. With IPv6, a computer can automatically configure its network settings without a DHCP server by sending a solicitation message to its IPv6 router. The router then sends back its advertisement message, which contains the prefix information that the computer can use to create its own IPv6 address. This feature significantly helps simplify the deployment of the IPv6 devices, especially in the transient environments such as airports, train stations, stadiums, hotspots, and so on.

Stateless Address Autoconfiguration (SLAAC)

Allows a server-less basic network configuration of the IPv6 computers.

8-2 IPV6 ADDRESSING

It was previously mentioned that IPv6 uses a 128-bit address technique, as compared to IPv4's 32-bit address structure. There is also a difference in the way the IP addresses are listed. IPv6 numbers are written in hexadecimal rather than dotted decimal, as with IPv4. For example, the following is an IPv6 address represented with 32 hexadecimal digits Note: 32 hex digits with 4 bits/hex digit = 128 bits):

6789:ABCD:1234:EF98:7654:321F:EDCB:AF21

This is classified as a **full IPv6 address**. The *full* means that all 32 hexadecimal positions contain a value other than 0.

Why doesn't IPv6 use the “dotted decimal” format of IPv4? The answer is it would take many decimal numbers to represent the IPv6 address. Each decimal number takes at least seven binary bits in ASCII (American Standard Code for Information Interchange) code. For example, the decimal equivalent of the first eight hexadecimal characters in the previous full IPv6 address is

6789:ABCD = 103.137.171.205

The completed decimal equivalent number for the full IPv6 address is

103.137.171.205.18.52.239.152.118.84.50.31.237.203.175.33

Full IPv6 Address

All 32 hexadecimal positions contain a value other than 0.

The equivalent decimal number is 42 characters in length. In fact, the decimal equivalent number could be 48 decimal numbers long.

In terms of bits, one 4 hex bit group requires $4 \times 4 = 16$ bits. Assuming that 8 bits are used to represent the decimal numbers, it will take $12 \times 8 = 96$ bits to express one hex bit group in a decimal format. There is a significant bit savings obtained by expressing the IPv6 address in a hexadecimal format.

Double-Colon Notation

A technique used by IPv6 to remove 0s from the address.

IPv6 uses seven colons (:) as separators to group the 32 hex characters into 8 groups of four. Some IPv6 numbers will have a 0 within the address. In this case, IPv6 allows the number to be compressed to make it easier to write the number. The technique for doing this is called **double-colon notation**. For example, assume that an IPv6 number is as follows:

6789:0000:0000:EF98:7654:321F:EDCB:AF21

Consecutive 0s can be dropped and a double-colon notation can be used as shown:

6789::EF98:7654:321F:EDCB:AF21

Recovering the compressed number in double-colon notation simply requires that all numbers left of the double notation be entered beginning with the leftmost slot of the IPv6 address. Next, start with the numbers to the right of the double colon.

Begin with the rightmost slot of the IPv6 address slots and enter the numbers from right to left until the double colon is reached. Zeros are entered into any empty slots:

6789 :0 :0 :EF98 :7654 :321F :EDCB :AF21

IPv4 numbers can be written in the new IPv6 form by writing the IPv4 number in hexadecimal and placing the number to the right of a double colon. Example 8-1 demonstrates how a dotted-decimal IP number can be converted to IPv6 hexadecimal.

Example 8-1 Convert the IPv4 address of 192.168.5.20 to an IPv6 hexadecimal address

Solution:

First convert each dotted-decimal number to hexadecimal.

Decimal	Hex
192	C0
168	A8
5	05
20	14

(Hint: Use a calculator or a lookup table to convert the decimal numbers to hexadecimal.) The IPv6 address will have many leading 0s; therefore, the IPv6 hex address can be written in double-colon notation as

:: C0A8:0514.

IPv4 addresses can also be written in IPv6 form by writing the IPv4 number in dotted-decimal format, as shown. Note that the number is preceded by 24 hexadecimal 0s:

0000: 0000: 0000: 0000: 0000: 0000:192.168.5.20

This number can be reduced as follows:

::192.168.5.20

Similar to IPv4 classless addresses, IPv6 addresses are fundamentally divided into a network portion followed by a host portion. The network portion is called the **network prefix** and the number of bits used is the **prefix length**. The prefix is represented with a slash followed by the prefix length. This is the same notation used to designate the CIDR in IPv4. For example, the IPv6 address of 2001:DB8:FEED:BEEF::12 has a 64-bits network prefix. It then can be represented as 2001:DB8:FEED:BEEF::12/64. However, the concept of a CIDR is not relevant in IPv6, because there is enough IP address space for everyone. So, in IPv6, the host portion of the address or what is called the **interface identifier** is always 64-bits in length. This automatically leaves 64 bits as the network prefix. In a typical IPv6 customer site, a network of /48 is usually allocated by IANA. This provides the site with 65,536 subnets, which is more than sufficient. This means that when a site is assigned a /48, the site is capable of having up to 65536 subnets and each subnet is capable of hosting more than 1.8×10^{19} IPv6 addresses.

There are three types of IPv6 addresses: unicast, multicast, and anycast. The **unicast** IPv6 address is used to identify a single network interface address and data packets are sent directly to the computer with the specified IPv6 address. There are several types of unicast addresses, including link-local addresses, **global unicast addresses**, and unique local addresses. Link-local addresses are designed to be used for and are limited to communications on the local link. Every IPv6 interface will have one link-local address.

Per RFC 4291, "IP Version6 Addressing Architecture," the network prefix of link-local addresses, is defined as FE80::/10. Unique local unicast addresses are addresses for local use only, and they are similar to the private IP addresses used in IPv4. Unique local unicast addresses use the prefix of FD00::/8 and were designed to replace site-local addresses, which are being deprecated.

Global unicast addresses are equivalent to the public ip addresses in IPv4. They have unlimited scope, and they are routable on the Internet. IANA is responsible for allocating the IPv6 global unicast address space. Currently, the range of allocated IPv6 addresses starts from prefix 2000::/3.

Network Prefix

The network portion of the IPv6 address.

Prefix Length

Number of bits used to make up the network prefix.

Interface Identifier

The host portion of the IPv6 address.

Unicast Address

Used to identify a single network interface address, and data packets are sent directly to the computer with the specified IPv6 address.

Global Unicast Addresses

These are equivalent to the public IP addresses in IPv4.

Multicast Address

Data packets sent to a multicast address are sent to the entire group of networking devices such as a group of routers running the same routing protocol.

Anycast Address

Obtained from a list of addresses.

IPv6 **multicast addresses** are defined for a group of networking devices. Data packets sent to a multicast address are sent to the entire group of networking devices such as a group of routers running the same routing protocol. Multicast addresses all start with the prefix FF00::/8. The next group of characters in the IPv6 multicast address (the second octet) are called the scope. The scope bits are used to identify which ISP should carry the data traffic.

The **anycast IPv6 addresses** might seem like a new type of address, but the concept was not new. Anycast addresses can be thought of as a cross between unicast and multicast addresses. While the unicast traffic sends information to one address and the multicast traffic sends information to every address in the group, the anycast traffic sends information to any one address of the group. The trick is which address of the group to send information to. The most logical and efficient answer is the nearest or the closet address. Similar to multicast where the nodes will join the multicast group, the anycast nodes share the same anycast address. The data will be sent to a node within the anycast group. This node is the nearest to the sender.

Actually, the anycast concept is used in the IPv4 environment today with the root DNS servers. There are 13 DNS root servers in the world, but the DNS query is only sent to one of those servers.

IPv6 addressing is being used in a limited number of network sites (e.g., the federal government); however, the Internet is still running IPv4 and will be for some time. But, there are transition strategies in place to help with the IPv4 to IPv6 transition.

6to4 Prefix

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

One possible transition to IPv6 is called the **6to4 Prefix**, which is essentially a technique that enables IPv6 sites to communicate over the IPv4 Internet. This requires the use of a 6to4 enabled router, which means that 6to4 tunneling has been enabled. This also requires the use of a 6to4 Relay router that forwards 6to4 data traffic to other 6to4 routers on the Internet.

Figure 8-3 illustrates the structure of the 6to4 prefix for hosts. The 32 bits of the IPv4 address fit into the first 48 bits of the IPv6 address.



FIGURE 8-3 The 6to4 prefix format

Note the following shown in Figure 8-3:

- **FP** is the Format Prefix, which is made up of the higher order bits. The **001** indicates that this is a global unicast address. The current list of the IPv6 address allocation can be viewed at www.iana.org/assignments/ipv6-unicast-address-assignments. Currently, IANA allocates 2000::/3 as an IPv6 global pool. 2000 can be written in binary as **0010** 0000 0000 0000. 001 is the 3 highest order bits, which correspond to the FP.
- **TLA ID (0x2002)** are the top-level identifiers that are issued to local Internet registries. These IDs are administered by IANA (<http://www.iana.org/>). The

TLA is used to identify the highest level in the routing hierarchy. The TLA ID is 13 bits long.

- **V4ADDR** is the IPv4 address of the 6to4 endpoint and is 32 bits long.
- **SLA ID** is the Site Level Aggregation Identifier that is used by individual organizations to identify subnets within their site. The SLA ID is 16 bits long.
- **Interface ID** is the Link Level Host Identifier and is used to indicate an interface on a specific subnet. The interface ID is equivalent to the host IP address in IPv4.

The 6to4 prefix format enables IPv6 domains to communicate with each other even if they don't have an IPv6 ISP. Additionally, IPv6 can be used within the intranet, but access to the Internet is still available. The 6to4 provides unicast IPv6 connectivity between IPv6 host and via the IPv4 Internet.

8-3 IPV6 NETWORK SETTINGS

Almost all the modern computer operating systems being used today are IPv6 capable. On most operating systems, the IPv6 configuration settings can be found at the same location where the TCP/IP settings for IPv4 reside. This is provided in the Local Area Connections Properties window for both Windows XP and Windows 7. The Local Area Connections Properties window for Windows XP is provided in Figure 8-4. The Local Area Connections Properties window for Windows 7 is provided in Figure 8-5.

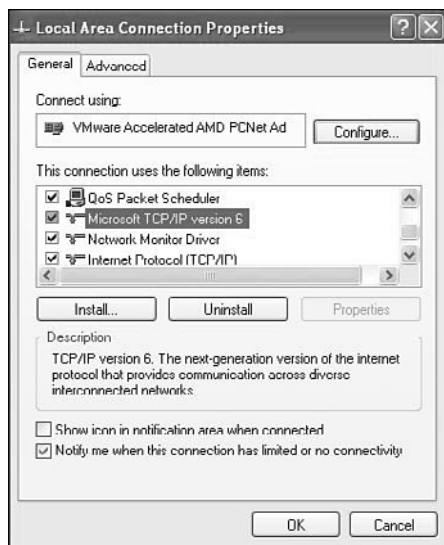


FIGURE 8-4 The Local Area Connections Properties window for Windows XP

There is an option available to obtain the IPv6 configuration automatically as well as an option for manual configuration. This option is available in the Internet Pro-

ocol Version 6 (TCP/IPv6) Properties window, as shown in Figure 8-6. This same feature is available with IPv4. However, Windows XP is one of the exceptions where there is no manual configuration mode for assigning the IPv6 address. The majority of the operating systems enable IPv6 with the automatic configuration mode by default. The following is a summary of the configuration options provided in the TCP/IPv6 Properties window:

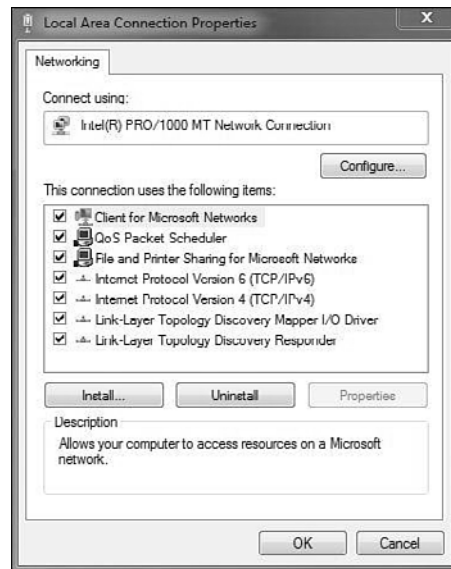


FIGURE 8-5 The Local Area Connections Properties window for Windows 7

- **Obtain an IPv6 address automatically:** In this option, the IPv6 address is automatically configured for this network connection.
- **Use the following IPv6 address:** Specifies the IPv6 address and default gateway are manually configured:
 - **IPv6 address:** This space is used to type in an IPv6 unicast address.
 - **Subnet prefix length:** This space is used to specify the subnet prefix length for the IPv6 address. For unicast addresses, the default value is 64.
 - **Default gateway:** This space is used to enter the IPv6 address for the default gateway.
- **Obtain DNS server address automatically:** This selection indicates the IPv6 addresses for the DNS servers are automatically configured.
- **Use the following DNS server addresses:** This space is used to specify IPv6 addresses of the preferred and alternate DNS servers for this network connection:
 - **Preferred DNS server:** This space is used to input the IPv6 unicast address for the preferred DNS server.
 - **Alternate DNS server:** This space is used to enter the IPv6 unicast address of the alternate DNS server.

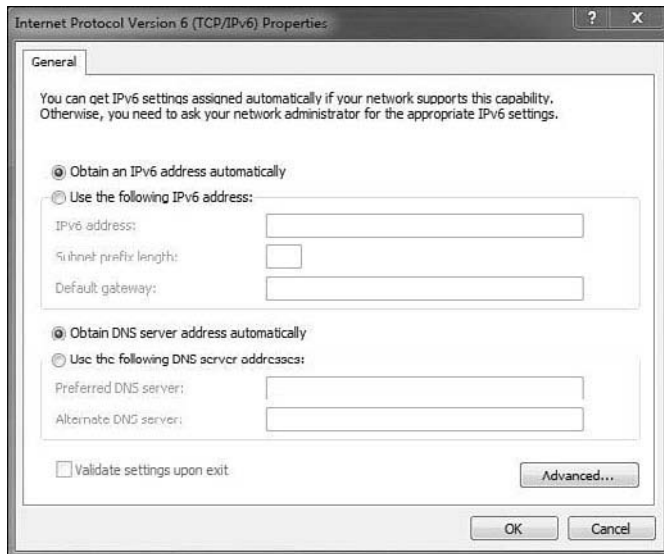


FIGURE 8-6 Internet Protocol Version 6 (TCP/IPv6) Properties window for Windows 7

IPv6 configuration settings are also available for the Mac OS X operating system in the TCP/IP window, as shown in Figure 8-7. The user has the option to configure the IPv6 address automatically or manually. The option for automatically configuring the IPv6 address is selected in Figure 8-7.

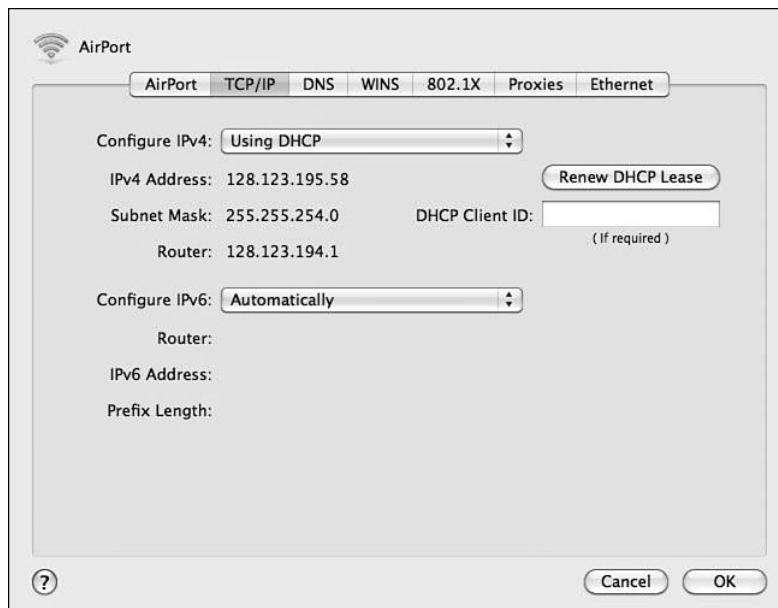


FIGURE 8-7 Mac OS X IPv6 configuration

IPv6 Stateless Autoconfiguration

Enables IPv6-enabled devices that are attached to the IPv6 network to connect to the network without requiring support of an IPv6 DHCP server.

Link-Local Address

Indicates the IP address was self-configured.

In typical places, such as homes and businesses, IPv6 is not yet enabled on the network environment. So, what would happen to all the machines with IPv6 enabled in the automatic configuration mode? The answer is what is called the **IPv6 stateless autoconfiguration**. This feature enables IPv6-enabled devices that are attached to the IPv6 network to connect to the network without requiring support of an IPv6 DHCP server.

This means that, even though an IPv6 DHCP server and an IPv6 enabled router are not involved, any IPv6 machine can self-configure its own **link-local address**. The term link-local address indicates the IP address is self-configured. This means that any IPv6 host should be able to communicate with other IPv6 hosts on its local link or network. The interface identifier of the link-local address is derived by transforming the 48 bits of the EUI-48 MAC address to 64 bits for EUI-64. This EUI-48 to EUI-64 transform algorithm is also used to derive the interface identifier for the global unicast address. Example 8-2 demonstrates how to convert an EUI-48 MAC address of 000C291CF2F7 to a modified EUI-64 format.

Example 8-2

1. Expanding the 48-bit MAC address to a 64-bit format by inserting “FFFE” in the middle of the 48 bits.

000C29 **FFFE** 1CF2F7.
2. Change the seventh bit starting with the leftmost bit of the address from 0 to 1. This seventh bit is referred to as the U/L bit or universal/local bit. 000C29 is 0000 0000 0000 1100 0010 1001 in binary format. When its seventh bit is changed to 1, it becomes 0000 0010 0000 1100 0010 1001, which is 020C29 in hexadecimal number.
3. The result is a modified EUI-64 address format of 020C29FFFE1CF2F7.

FE80::/64

The prefix for a link-local addresses.

Neighbor Solicitation

Purpose of this solicitation is to discover the link-layer address of another IPv6 node or to confirm a previously determined link-layer address.

Duplicate Address Detection (DAD)

Process of detecting another machine with the same IPv6 address.

To complete the autoconfiguration IPv6 address, the subnet prefix of **FE80::/64** is then prepended to the interface identifier resulting in a 128-bit link-local address. To ensure that there is no duplicate address on the same link, the machine sends a **Neighbor Solicitation** message out on the link. The purpose of this solicitation is to discover the link-layer address of another IPv6 node or to confirm a previously determined link-layer address. If there is no response to the message, it assumes that the address is unique and therefore assigns the link-local address to its interface. The process of detecting another machine with the same IPv6 address is called **Duplicate Address Detection (DAD)**. Figures 8-8, 8-9, and 8-10 show the local-link addresses from different operating systems. Look for the FE80:: prefix in each figure.

```

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : nnsu.edu
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
    Physical Address. . . . . : 00-0C-29-1C-F2-F7
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 128.123.195.42
    Subnet Mask . . . . . : 255.255.254.0
    IP Address. . . . . : fe80::20c:29ff:fe1c:f2f7%4
    Default Gateway . . . . . : 128.123.194.1
    DHCP Server . . . . . : 128.123.3.5
    DNS Servers . . . . . : 128.123.3.5
                           128.123.2.19
                           fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    Primary WINS Server . . . . . : 128.123.2.20
    Secondary WINS Server . . . . . : 128.123.2.30
    Lease Obtained. . . . . : Wednesday, November 10, 2010 3:23:25 PM
    Lease Expires . . . . . : Thursday, November 11, 2010 3:23:25 AM

```

FIGURE 8-8 Windows XP—**ipconfig** result with a link-local address

```

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : nnsu.edu
    Description . . . . . : Intel(R) PRO/1000 MT Network Connection
    Physical Address. . . . . : 00-0C-29-02-E5-7E
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::a1b4:6c3d:b953:6e5%11(Preferred)
    IPv4 Address. . . . . : 128.123.194.226(Preferred)
    Subnet Mask . . . . . : 255.255.254.0
    Lease Obtained. . . . . : Wednesday, November 10, 2010 4:30:06 PM
    Lease Expires . . . . . : Thursday, November 11, 2010 4:30:06 AM
    Default Gateway . . . . . : 128.123.194.1
    DHCP Server . . . . . : 128.123.3.5
    DHCPv6 Iaid . . . . . : 234884137
    DHCPv6 Client DUID. . . . . : 00-01-00-01-12-26-27-57-00-0C-29-AE-67-F2

    DNS Servers . . . . . : 128.123.3.5
                           128.123.2.19
    Primary WINS Server . . . . . : 128.123.2.20
    Secondary WINS Server . . . . . : 128.123.2.30
    NetBIOS over Tcpip. . . . . : Enabled

```

FIGURE 8-9 Windows 7—**ipconfig** result with a link-local address

```

en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 90:27:e4:f8:e2:dd
    inet 128.123.195.58 netmask 0xfffffe00 broadcast 128.123.195.255
    inet6 fe80::9227:e4ff:fe8:e2dd%en1 prefixlen 64 scopeid 0x5
    media: <unknown subtype>
    status: active

```

FIGURE 8-10 Mac OS X—**ifconfig** result with a link-local address

The derivation of the IPv6 interface identifier from the MAC address generates some concerns regarding privacy issues. The concern is that the MAC address can be tracked throughout the Internet. A MAC address always attaches to the device *v*, and the interface identifier does not change no matter where it is physically located. The danger of this is that the movement or location of the device can be traced using the MAC address. To remedy these concerns, the IETF created RFC 4941 “Privacy Extensions for Stateless Address Autoconfiguration in IPv6.” This RFC allows the generation of a random identifier with a limited lifetime to replace the machine’s MAC address. An address like this will be difficult to trace because it regularly changes. Figure 8-9 shows the link-local address of a Windows 7 machine, which has been randomly generated. Therefore, this IPv6 address does not appear to be anything resembling its MAC address. The link-local address shown in Figure 8-9 is

fe80::a1b4:6c3d:b953:6e5%11

Privacy Extensions for Stateless Address Autoconfiguration

Allows the generation of a random identifier with a limited lifetime.

where %11 is the interface index or scope ID designated by Windows 7. IPv6 enables a socket application to specify an interface to use for sending data by specifying an interface index. It is possible for a computer to have more than one network interface card (NIC) and as a result to have multiple link-local addresses. Additionally, each link-local address can have a different scope. The purpose of the scope ID is to indicate which address it is used for.

The MAC or physical address is 000C2902E57E.

8-4 CONFIGURING A ROUTER FOR IPV6

Multicast Listener Discovery (MLD)

Enables the switches to listen to MLD packets to determine how to efficiently forward multicast packets to specific listeners on specific ports.

ipv6 unicast-routing

This command activates the IPv6 forwarding mechanism on the routers.

Not every piece of networking equipment is IPv6-capable, and this must be verified before implementing IPv6. IPv6-capable equipment can operate in the IPv4 and IPv6 environment. IPv6 relies heavily on multicast messages for enabling a lot of functions; therefore, the network switches must be able to support IPv6 multicast functions as well. In IPv4, IGMP (Internet Group Management Protocol) is used for determining which computers should join a multicast group. However, IGMP is no longer used in IPv6. For multicast group management, IPv6 uses **Multicast Listener Discovery (MLD)** instead. Similar to IGMP in IPv6, MLD snooping enables the switches to listen to MLD packets to determine how to efficiently forward multicast packets to specific listeners on specific ports.

Today, most routers are IPv6-capable. Those that are not might just require a software upgrade. On Cisco routers, IPv6 is not enabled automatically. To enable IPv6 unicast packet forwarding on Cisco routers, the global command **ipv6 unicast-routing** is entered. The following is the sequence of commands required to enable IPv6 unicast-routing:

```
Router# conf t
Router(config)#
Router(config)# ipv6 unicast-routing
```

ipv6 enable

Enables IPv6 on a specific interface.

The **ipv6 unicast-routing** command only activates the IPv6 forwarding mechanism on the routers. However, IPv6 is still not yet enabled on a specific interface. To enable IPv6 on a specific interface, you must enter the **ipv6 enable** command. The following example shows how to enable IPv6 on a gigabitethernet 3/1 interface. This step requires that the interface must first be selected. In this case, the command **int Gig3/1** is entered from the (config)# prompt. The prompt changes to (config-if)# and the command **ipv6 enable** is entered:

```
int Gig3/1
Router(config)# int Gig3/1
Router(config-if)# ipv6 enable
```

For Cisco routers, enabling IPv6 on the interface automatically configures the link-local address for that interface. The link-local address can only communicate with the IPv6 devices on the same network link.

The command **show running-config** is used to verify the IPv6 configuration. The use of this command is next demonstrated and a portion of the running configuration for interface GigabitEthernet 3/1 is provided:

```
Router#show running-config
.
.
!
interface GigabitEthernet3/1
  no ip address
  ipv6 enable
!
```

Also, the command **show ipv6 interface** can be used to show the state of the IPv6 configuration on the interface. This command shows the IPv6 of the interface. In the following example, it shows that IPv6 is enabled on the interface gigabitEthernet3/1. It shows the interface has a link-local address, but not the global address. Along with that the IPv6 network discovery protocol information is shown:

```
Router#show ipv6 interface gigabitEthernet 3/1
GigabitEthernet3/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::217:DFFF:FEF5:1000
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFF5:1000
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Output features: HW Shortcut Installation
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

The IPv6 global address can be configured on the interface by using the command **ipv6 address ipv6 interface address** issued from the (config-if)# prompt. There are two ways to program the IPv6 interface address. One is to specify the entire 128-bit IPv6 address followed by the prefix length. Another way is to specify a 64-bit prefix and to use the **eui-64** option. Using the option **eui-64** allows the router to choose its own host identifier (right most 64-bits) from the EUI-64 (Extended Universal Identifier-64) of the interface. The following example uses the IPv6 address of 2001:DB88:FEED:BEEF::1 on the router interface. This has a 64-bit network prefix of 2001:DB88:FEED:BEEF.

```
Router(config)# int Gig3/1
Router(config-if)# ipv6 address 2001:DB88:FEED:BEEF::1/64
```

show ipv6 interface

Used to show the state of the IPv6 configuration on the interface.

ipv6 address ipv6 interface address

The command used to configure the IPv6 address on an interface.

eui-64

Allows the router to choose its own host identifier.

Next, the command **show ipv6 interface gigabitEthernet 3/1** is used to display the configuration of the Gig3/1 interface. This time the command shows that the interface gigabitEthernet 3/1 now has an IPv6 global address assigned to it, which is 2001:DB8:FEED:BEEF::1:

```
Router#show ipv6 interface gigabitEthernet 3/1
GigabitEthernet3/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::217:DFFF:FEF5:1000
  Global unicast address(es):
    2001:DB8:FEED:BEEF::1, subnet is 2001:DB8:FEED:BEEF::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FFF5:1000
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Output features: HW Shortcut Installation
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

ND Protocol

Network Discovery Protocol. ICMPv6 messages of the type Router Advertisement (RA).

RA Messages

Router advertisement. This is a response to a link-local router solicitation message.

Router Solicitation Messages

These messages are sent to ask routers to send an immediate RA message on the local link so the host can receive the autoconfiguration information.

Now that IPv6 is enabled on the router, the router can begin to participate in the IPv6 functions. The router plays a key role in the stateless autoconfiguration of an IPv6 network. An IPv6 router uses the **neighbor discovery (ND)** protocol to periodically advertise information messages on the links to which they are connected. These are ICMPv6 messages of the type Router Advertisement (RA). One parameter of the router advertisements is the IPv6 network prefix for the link that can be used for host autoconfiguration. Upon receiving **RA messages**, an unconfigured host can build its global unicast address by prepending the advertised network prefix to its generated unique identifier just like in the link-local address case.

Another way for a host to autoconfigure itself is by sending **router solicitation messages** to the connected routers. These messages are sent to ask routers to send an immediate RA message on the local link, so the host can receive the autoconfiguration information without having to wait for the next scheduled RA. Note: The time interval between RA messages is configurable. By default, router advertisements are sent every 200 seconds in Cisco routers.

As a result, the global unicast address of every machine on this network is the combination of the network prefix of 2001:DB8:FEED:BEEF and the self-generated interface identifier for that machine. Both Figure 8-11 and Figure 8-12 show two IPv6 addresses with the 2001:DB8:FEED:BEEF prefix. There are two IPv6 addresses. One is a global unicast address and another is a random generated identifier as part of the

privacy identifier. This was discussed earlier in this section (see Privacy Extensions for Stateless Autoconfiguration). Microsoft calls this random identifier IPv6 a “temporary IPv6 address.” This is shown to be a temporary address in Windows 7.

```
IP Address . . . . . : 2001:db8:feed:beef:460:45ab:3d6e:56e3
IP Address . . . . . : 2001:db8:feed:beef:20c:29ff:fe1c:f2f7
IP Address . . . . . : fe80::20c:29ff:fe1c:f2f7%4
Default Gateway . . . . . : 128.123.7.1
                        fe80::217:dfff:fe5:1000%4
```

FIGURE 8-11 Windows XP—**ipconfig** result with an IPv6 global unicast address

```
IPv6 Address . . . . . : 2001:db8:feed:beefa1b4:6c3d:b953: 6e5 (Preferred)
Temporary IPv6 Address . . . . . : 2001:db8:feed:beef:44ab:2c4d:f3d0:6674 (Preferred)
Link-local IPv6 Address . . . . . : fe80:a1b4:3c3d:b953:6e5%11 (Preferred)
IPv4 Address . . . . . : 128.123.7.207 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Friday, November 12, 2012 4:49:33 PM
Lease Expires . . . . . : Saturday, November 13, 2012 4:49:33 AM
Default Gateway . . . . . : fe80::217:dfffef5:1000%11
```

FIGURE 8-12 Windows 7—**ipconfig** result with an IPv6 global unicast address

In Windows XP, both of these are presented as IP addresses. Of course, we can tell that one is a modified EUI-64 format, and the other one is randomly generated. An IPv6 address with ff:fe in the middle indicates the EUI-48 to EUI-64 transform. On Mac OS X, no random identifier is used. The global unicast address is the product of the modified EUI-64 format, as shown in Figure 8-13.

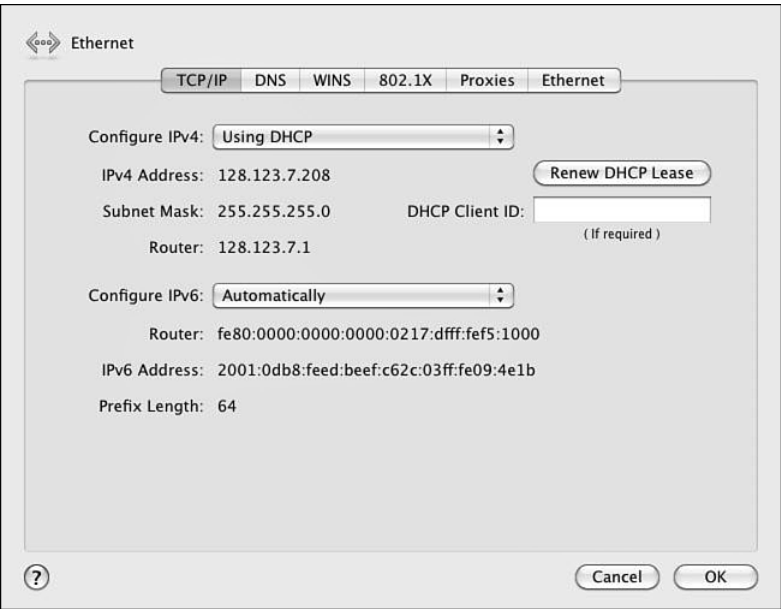


FIGURE 8-13 Mac OS X—**ipconfig** result with an IPv6 global unicast address

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 IPv6 addresses in examples, books, documentation, or even in test environments.

Throughout this chapter, the IPv6 prefix used is **2001:DB8::/32**. This is a special range designated by the IANA to be used for any testing or documentation. This IPv6 prefix cannot be used nor can it be routed on the Internet.

With the global unicast address, the machine is now reachable from anywhere on the IPv6 network. However, it is a daunting task to remember the IPv6 global unicast address. It is not practical to use the long 128-bits address. This required a DNS server that can translate a host name to an IPv6 address. The DNS record for IPv6 is called AAAA (Quad A) record.

8-5 IPV6 ROUTING

When interconnecting IPv6 networks together, a routing protocol is required. IPv6 supports static, RIP, OSPF, EIGRP, and IS-IS routing. Most of these protocols had to be revised to be able to deal with IPv6 addresses. However, the routing protocols for IPv6 work the same way as they do with IPv4. In fact, they still maintain the same routing principles. The following material demonstrates how to configure IPv6 routing for static, RIP, OSPF, EIGRP, and ISIS.

IPv6: Static

Configuring a static route for IPv6 is almost the same as it is in IPv4. In IPv4, one can specify the next hop IP address or/and the exit interface. In IPv6, there is an extra feature. The next hop IP address in IPv6 can either be the link local address or the global address. The following examples show how to configure an IPv6 static route using these three different methods:

```
Router# conf t
Router(config)# ipv6 route 2001:0db8:BEEF::/32 FA1/0
Router(config)# ipv6 route 2001:0db8:BEEF::/32 FA1/0 fe80::2
Router(config)# ipv6 route 2001:0db8:BEEF::/32 2001:0db8:FEED::1
```

The first static route shows the route to the network 2001:0db8:BEEF::/32 is configured via interface FastEthernet1/0. The second static route gives an option of the link-local next hop address, which is specified with the fe80 prefix. The third static entry shows a route to the network that points to the global IPv6 address of 2001:0db8:FEED::1.

IPv6: RIP

RIPng

Routing Information Protocol next generation, which is required to support IPv6 routing.

RIP routing using IPv6 requires the use of a RIP version called Routing Information Protocol next generation or **RIPng**. The basic features of RIPng are the same as RIPv2. For example, this is still a distance vector protocol, there is a maximum hop limitation; however, RIPng is updated to use IPv6 for transport. Also, RIPng uses the IPv6 multicast address of FF02::9 for all RIP updates.

Configuring RIPng on Cisco routers is simple. The biggest difference between configuring RIPv2 and RIPng on Cisco routers is now RIPng must be configured on a per network link or per-interface basis rather than per-network basis as in RIPv2.

The following examples demonstrate how to enable RIPng and how to configure RIPng on a Cisco router interface:

```
Router# conf t
Router(config)#
Router(config)# ipv6 router rip RIP100
Router(config)#
Router(config)# int Gig3/1
Router(config-if)# ipv6 rip RIP100 enable
```

The command **ipv6 router rip *rip_tag*** is used to enable RIPng on Cisco routers. The ***rip_tag*** is a tag to identify the RIP process. The RIPng is enabled on the Gigabit interface 3/1 with the command **ipv6 rip *rip_tag* enable**. The same command will be used to enable other RIP interfaces. This is different than configuring RIPv2 where the network statement needs to be issued for every RIP network.

rip_tag
Used to identify the RIP process.

IPv6: OSPF

The current OSPF version used in IPv4 is OSPFv2. Most of OSPF information relies heavily on the IP number (for example the router ID <area ID> and the link-state ID). To support IPv6, the OSPF routing protocol has been significantly re-vamped. The new OSPF version for IPv6 is **OSPFv3**. The basic foundation of OSPF still remains intact—for example, OSPFv3 is still a link state routing protocol. However, OSPFv3 uses the IPv6 link-local multicast addresses of FF02::5 for all OSPF routers and FF02::6 for OSPF designated routers.

OSPFv3
The OSPF version that supports IPv6.

OSPFv3 is now enabled on a per-link basis, not on a per-network basis on Cisco routers. This is similar to the changes in RIPng. OSPFv3 identifies which networks are attached to the link and propagates them into the OSPF area. The following example demonstrates how to enable OSPFv3 and how to configure OSPFv3 on a Cisco router interface:

```
Router# conf t
Router(config)#
Router(config)# ipv6 router ospf 99
Router(config)#
Router(config)# int Gig3/1
Router(config-if)# ipv6 ospf 99 area 0.0.0.0
```

The command **ipv6 router ospf *process_id*** is used to enable OSPFv3 on Cisco routers. OSPFv3 is enabled on the Gigabit interface 3/1 with the command **ipv6 ospf *process_id* area *area_id***. The same command is used to enable other OSPF interfaces. The router in this example is configured to be area 0 which is the backbone (area 0.0.0.0).

IPv6: EIGRP

EIGRP is inherently a multiprotocol routing protocol. It was designed to support non-IP protocols, such as IPX and Appletalk, and it supports the IP protocols IPv4 and now IPv6. IPv6 EIGRP uses the IPv6 link-local multicast addresses of FF02::A for all EIGRP Hello packets and updates.

IPv6 EIGRP is now configured over a network link, so there is no need to configure a network statement as in IPv4 EIGRP. The following example demonstrates how to enable IPv6 EIGRP and how to configure it on a Cisco router interface:

```
Router# conf t
Router(config)#
Router(config)# ipv6 router eigrp 999
Router(config-rtr)# no shut
Router(config)# int Gig3/1
Router(config-if)# ipv6 eigrp 999
```

The command **ipv6 router eigrp** *as_number* is used to enable EIGRP on Cisco routers. The IPv6 EIGRP protocol is created in a shutdown mode by default. The **no shutdown** is issued to ensure that the protocol is enabled. Next, the IPv6 EIGRP is enabled on the Gigabit interface 3/1 with the command **ipv6 eigrp** *as_number*. The network link is now part of the EIGRP routing network.

IPv6: IS-IS

As mentioned in Chapter 3, IS-IS is designed to work on the same network layer just like IP. Therefore, it does not require an IP protocol for it to function. Later, IS-IS was adapted to work with IP. Because of its IP independence, IS-IS is much easier than most protocols to incorporate with IPv6. Only a few adjustments to IS-IS have been made to better support IPv6.

Configuring IPv6 IS-IS is very similar to the method used in IPv4. In IPv6, IS-IS is always enabled on a per network link basis. This is the same for the IPv4 configuration. The same global command (**clns routing**) is used to enable the IS-IS routing protocol. The same NET address is used in the IPv6 configuration as in the IPv4 configuration. The only big difference is the use of keyword **ipv6** when enabling the IPv6 IS-IS interface. The following example demonstrates how to enable IPv6 IS-IS and how to configure it on an interface of a Cisco router:

```
Router# conf t
Router(config)# clns routing
Router(config)# router isis
Router(config-rtr)# net 49.0001.c202.00e8.0202.00
Router(config)#
Router(config)# int Gig3/1
Router(config-if)# ipv6 router isis
```

The command **clns routing** is used to enable the connectionless network service. The command **router isis** will allow the IS-IS protocol to be configured. The **net** *NET Address* assigns the NET address to IS-IS. Then, the IPv6 IS-IS is enabled on the Gigabit interface 3/1 with the command **ipv6 router isis**.

This section demonstrated the steps for configuring IPv6 routing for static, RIP, OSPF, EIGRP, and IS-IS. As was demonstrated, the steps are similar to configuring routing for IPv4; however, there are some distinct differences required to enable an IPv6 interface.

8-6 TROUBLESHOOTING IPV6 CONNECTION

One big question that needs to be answered before troubleshooting IPv6 connectivity is: Does the network environment support IPv6? If the answer is yes, the same network troubleshooting techniques and approaches still apply on IPv6 as on IPv4. Remember what has changed is only the network layer on the OSI model. Other layers are still intact and stay the same. You will still need to troubleshoot the physical connections to make sure the physical layer is working properly. The data link layer still needs to be inspected to see if the packets are being forwarded, MAC addresses are still being seen, and hosts are still in the correct VLANs.

The commands such as **ipconfig** in Windows and **ifconfig** for Linux or Mac OS X can be used to view the TCP/IP configuration information of a host. This is always a good start in network troubleshooting. First, you have to see what is configured and whether it is configured correctly before you can move on to the next step. The examples of these commands are shown throughout this chapter.

Many basic network tools that are available in IPv4 are available in IPv6 as well. Ping is one of the most commonly used tools to test the connectivity between two hosts. Ping is implemented using ICMP echo and Echo reply for a very simple hello network test. In IPv6, the ICMP version 6 is being used instead; therefore the tool has changed slightly to accommodate the change in the ICMP protocol fields. The command **ping6** can be used to explicitly specify the IPv6 address, even though most operating systems have modified the **ping** command to understand both the IPv4 and IPv6 addresses. An issue of using the **ping** command in IPv6 is the lengthy address and the time required for entering the destination address. For example, the following is an example. The first part shows the IPv6 address that is assigned to the router's R1 interface.

```
R2(config-if)# ipv6 address 2001:C16C:0000:0001:0000:0000:0000:0001/64
```

The IPv6 address can be simplified using double colon notation, as shown:

```
R2# ping ipv6 2001:C16C:0:1::1
```

The IPv6 address is still complicated even with the reduced address length. A solution to this is to assign a hostname to the specified IPv6 address. In this case, the hostname R1-WAN will be assigned to the specified IPv6 address using the command **ipv6 host R1-WAN 2001:C16C:0:1::1/64**, as shown:

```
R2(config)# ipv6 host R1-WAN 2001:C16C:0:1::1
```

Now, the **ping** command, using the newly assigned hostnames for R1 and R2, can be used. An example is provided:

```
R2(config)# ipv6 host R1-WAN 2001:C16C:0:1::1
```

```
R2# ping R1-WAN
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 2001:C16C:0:1::1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

```
R2#
```

ping6

Command used to explicitly specify the IPv6 address.

tracert6

The router tool that enables the user to see the routing information between the two hosts.

tracert6

The Windows tool that enables the user to see the routing information between the two hosts.

Another useful network tool is **tracert** or **tracert** in Windows world. This tool enables the user to see the routing information between the two hosts. The IPv6 version of this tool is **tracert6** or **tracert6** in Windows. Like **ping**, the IPv6 version of **tracert** has to understand the ICMP version 6 messages as well. The structure for the **tracert6** command is shown. The Host name and web addresses assume the DNS entries have been made:

```
tracert6 <destination address, Host name, or web address>
```

For example, the following could be entered to run a **tracert**:

```
tracert6 2001:C16C:0:2::2
```

```
tracert6 www.6bone.net
```

```
tracert6 R1-WAN
```

When will the Internet switch to IPv6? The answer is not clear, but the networking community recognizes that something must be done to address the limited availability of current IP address space. Manufacturers have already incorporated IPv6 capabilities in their routers and operating systems. What about IPv4? The bottom line is that the switch to IPv6 will not come without providing some way for IPv4 networks to still function. Additionally, techniques such as NAT have made it possible for intranets to use the private address space and still be able to connect to the Internet. This has significantly reduced the number of IPv4 addresses required for each network and have delayed the need to immediately switch to IPv6.

SUMMARY

This chapter presented an overview of the fundamentals of the IP version 6. IPv6 is proposed to replace IPv4 to carry the data traffic over the Internet. The student should understand the following:

- The basic differences between IPv6 and IPv4
- The basic structure of a 128-bit IPv6 hexadecimal address
- The addresses that IPv6 uses
- How to setup IPv6 on the computers
- The purpose of link-local addresses
- How to setup IPv6 on the routers

QUESTIONS AND PROBLEMS

Section 8-1

1. What is the size of the IPv6 address?
2. What is a datagram?
3. How many bits are used to define the IPv4 source and destination address?
4. How many bits are used to define the IPv6 source and destination address?
5. Why is IPv6 faster than IPv4 for transferring packets?
6. At what layer is error detection performed in IPv6?
7. What is IPsec?
8. How is IPsec enabled with IPv6?
9. How are broadcasts handled in IPv6?
10. Why is DHCP not required in IPv6?

Section 8-2

11. How many bits are in an IPv6 address?
12. IPv6 numbers are written in what format?
13. Express the following IPv6 numbers using double-colon notation:
 - a. 5355:4821:0000:0000:0000:1234:5678:FEDC
 - b. 0000:0000:0000:1234:5678:FEDC:BA98:7654
 - c. 1234:5678:ABCD:EF12:0000:0000:1122:3344
14. Express the IPv4 IP address 192.168.12.5 in IPv6 form using dotted decimal.
15. Recover the following IPv6 address from the following double-colon notation:
1234:5678::AFBC

16. Define the structure of the 6to4 prefix.
17. What is the purpose of the 6to4 relay router?
18. What does it mean to have a full IPv6 address?
19. What is the network prefix for the following IPv6 address and how big is the network prefix?
2001:1234:ABCD:5678::10/64
20. What is the length of the interface identifier in IPv6?
21. These types of addresses started with FF00::/8:
 - a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct
22. This address is only deliverable to the nearest node.
 - a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct
23. The range of these addresses starts with 2000::/3.
 - a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct
24. The network prefix for this address is FE80::/10.
 - a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct

25. The IPv6 addresses are equivalent to public addresses in IPv4.
- a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct
26. This type of address can be thought of as a cross between unicast and multicast addresses.
- a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct
27. Every IPv6 interface will have at least one of these addresses.
- a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct
28. These types of IPv6 addresses can be thought of as private addresses in IPv4.
- a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct
29. The 001 of this address indicates it is what type of address?
- a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct

30. These types of IDs are administered by IANA.
- a. FP ID
 - b. SLA ID
 - c. TLA ID
 - d. Interface ID
 - e. None of these answers are correct
31. This type of ID is used to indicate an interface on a specific subnet.
- a. FP ID
 - b. SLA ID
 - c. TLA ID
 - d. Interface ID
 - e. None of these answers are correct
32. This ID is used to identify subnet within the site.
- a. FP ID
 - b. SLA ID
 - c. TLA ID
 - d. Interface ID
 - e. None of these answers are correct

Section 8-3

33. This type of operating system has no manual configuration mode for assigning the IPv6 address.
34. In regard to subnet address length in IPv6, the default value for unicast addresses is
- a. 32
 - b. 64
 - c. 128
 - d. None of these answers are correct
35. All the machines in a network are running IPv6 enabled in the automatic configuration mode. What mode is this, and what does this mean?
36. Which of the following types of IPv6 address is self-configured?
- a. Anycast
 - b. Multicast
 - c. Global unicast
 - d. Link-local
 - e. None of these answers are correct

37. How many DNS root servers are there in the world?
38. Why does a computer issue a neighbor solicitation message?
 - a. To discover the unicast address of another IPv6 node
 - b. To discover the anycast address of another IPv6 node
 - c. To discover the link-layer address of another IPv6 node
 - d. To discover the global unicast address of another IPv6 node
39. The process of detecting another machine with the same IPv6 address is called which of the following?
 - a. Duplicate Address Detection
 - b. Redundant Address Detection
 - c. Stateless Address Detection
 - d. Global Address Detection
40. What is the benefit of the “Privacy Extensions for Stateless Address Autoconfiguration in IPv6?”

Section 8-4

41. For multicast group management, IPv6 uses which of the following?
 - a. Unicast Listener Discovery
 - b. Stateless Listener Discovery
 - c. Unicast Listener Discovery
 - d. Multicast Listener Discovery
42. What global command is used to enable IPv6 unicast packet forwarding on Cisco routers?
43. To enable IPv6 on an interface, which of the following commands must be entered?
 - a. **ipv6 enable**
 - b. **ipv6 configure**
 - c. **ipv6 interface**
 - d. **ipv6 routing**

44. The following information is displayed after entering the **show running-config** command:

```
!  
interface GigabitEthernet1/1  
  no ip address  
  ipv6 enable
```

This information verifies which of the following? (Select all that apply.)

- a. IPv4 is configured.
 - b. Interface ge1/1 is configured.
 - c. IPv6 is enabled.
 - d. Interface status is ip.
45. The **show ipv6 interface gigabitEthernet 3/1** command is entered on a router. The address GigabitEthernet3/1 FE80::217:DFFF:FEF5:1000 is listed. What type of address is this?
46. The command **ipv6 address 2001:DC21:2244:3311::1/64** is entered on a router. What is the network prefix of this address and what is its length? What is the command doing?
47. What is the EUI option?
48. What is the purpose of the network discovery protocol in IPv6?
49. What is the purpose of the router solicitation message in IPv6?

Section 8-5

50. What is the following command showing?

```
Router(config)# ipv6 route 2001:0db8:ABCD::/32 FA0/0
```

51. List the command to create a static route for 2001:0db8:1234::/32 that points to the global network 2001:0db8:ABCD::1.
52. Create a static route for 2001:0db8:1234::/32 off the FA0/0 interface that gives the link-local next hop address, which is specified with the fe80::1 prefix.
53. What is RIPng and what is it used for?
54. What is the multicast address for RIPng?
55. List the command that is used to enable RIPng on Cisco routers.
56. What is the purpose of the rip tag?
57. What version of OSPF is used with IPv6?
58. What are the IPv6 link-local multicast addresses for routers and the link-local addresses for designated routers?
59. What command is used to configure OSPF routing for IPv6, using a process ID of 50?
60. What does the following command do?

```
Router(config-if)# ipv6 ospf 50 area 0.0.0.0
```

61. What is the IPv6 link-local multicast addresses for EIGRP? What is the link-local address used for in IPv6?
62. What is the command for enabling EIGRP for IPv6 with a specified AS of 100?
63. List the configuration for enabling ISIS for IPv6. List the router prompts and all commands required for enabling IS-IS on the Gig1/1 interface. Use a net address of 49.0002.b123.a456.0012.00.

Section 8-6

64. What command is used to view the /TCP/IP setting in Windows?
65. What command is used to view the /TCP/IP setting in Linux?
66. What is the purpose of the **ping6** command?
67. What is the purpose of the **tracert6** or **tracert6** command in IPv6?
68. List three things that should be answered before troubleshooting IPv6 connectivity?

Critical Thinking

69. Your boss read about IPv6 and wants to know if the network you oversee is ready for the transition. Prepare a response based on the networking and computer operating systems used in your facility.
70. The **show ipv6 interface** command is issued to examine a router's R1 interface. The interface has been configured with an IPv6 address. Where is the MAC address of the interface found?

```
R1# sh ipv6 interface
Serial0/0/0 is up, line protocol is up
IPv6 is enabled, link-local address is
FE80::213:19FF:FE7B:1101/64
No Virtual link-local address(es):
Global unicast address(es):
2001:C16C:0:1::1, subnet is 2001:C16C:0:1::/64
Joined group address(es):
FF02::1
FF02::2
FF02::0001:FF00:0001
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
Hosts use stateless autoconfig for addresses.
```

71. What is the purpose of the command **ipv6 address 2001:C16C:0:2:213:19FF:FE7B:1101/64 eui-64**?
72. Answer the following for the given IPv6 address: 2001:C15C:0000:0001:0000:0000:0001/64
 - a. Write this address using double colon notation
 - b. Identify the network prefixes

INDEX

Numbers

3DES (Triple Data Encryption Standard), ESP, 301

6to4 prefix (IPv6 addresses), 314

802.1Q, 18, 24-26

2001, DB8::/32 prefix and IPv6 router configuration, 324

Symbols

? (question mark), JUNOS operating system, 161

A

AAA (Authentication, Authorization, and Accounting), 281

ABR (area border routers), 112

access layer, 6

access-list 100 deny udp any any eq 161 command, ACL configuration, 273

access-list 100 deny udp any any eq snmp command, ACL configuration, 274

access-list permit ip any any command, ACL configuration, 274

accounting (security), 281

ACK (Acknowledgment) packets, TCP three-way handshakes, 230

ACL (Access Lists), 270-272. See also filter lists

access-list 100 deny udp any any eq 161 command, 273

access-list 100 deny udp any any eq snmp command, 274

access-list permit ip any any command, 274

configure terminal command, 273

edge routers, 273-275

extended ACL, 273

false TCP headers, 278

hosts, 277

ip access-group 100 out command, 274

IP addresses, stopping data traffic from, 277-278

permit ip any any command, 274-276

placement of, 274

remote data hosts, stopping data traffic from, 277

router logging, 283-285

show access-list 100 command, 274

show access-list command, 275-276

SMB, 273-275

standard ACL, 273

UDP, 276

AD (Administrative Distance), 71

address family ipv6 command, IPv6 Internet routing via BGP4+, 413

Address field (show ip eigrp neighbors command), 125

administration (Linux), 389

Is system-config- * command, 385

security, 387

system-config- [tool-name] command, 385

system-config-date command, 386

system-config-network command, 388

administration commands (Linux)

df command, 363

df -kh command, 364

history command, 364

kill [PID] command, 361

kill -9 [PID] command, 361

man command, 358-359

mount command, 358, 362

ps command, 358-361

shutdown command, 358, 364

shutdown -h now command, 364

su command, 358, 362

Tab key shortcut, 364

umount command, 364

up arrow shortcut, 364

advertise_connected policies, Juniper router route redistribution, 179

advertise_isis policies, Juniper router route redistribution, 179

advertise_rip policies, Juniper router route redistribution, 179

advertise_static policies, Juniper router route redistribution, 180

advertising networks, 75

AES (Advance Encryption Standard)

ESP, 301

WPA2, 291

AF33 (Assured Forwarding class 3), VoIP class maps, 441

AH (Authentication Headers), troubleshooting VPN tunnels, 300

allow-snmp term (filter lists), 279

AMI (alternate mark inversion), 38

anycast IPv6 addresses, 314

AP (access points), NSEL and IS-IS, 113

APIPA (Automatic Private IP Addressing), 196

Area ID, IS-IS, 112

areas (OSPF), 102, 105

A records (Address records), DNS, 214, 218-219

ARIN (American Registry for Internet Numbers), IP address assignments, 191

ARP (Address Resolution Protocol)

- broadcasts, IP address management, 200
- forensics, 236
 - arp-a command*, 237
 - ARP replies*, 241
 - ARP requests*, 241
 - show-arp command*, 237

AS (Autonomous Systems), 191, 401

ASN (Autonomous Systems Numbers), AS and BGP Internet routing, 401

at (ATM), 164

ATM (Asynchronous Transfer Mode), 41-44, 164

atm framing chitplcp command, 43

ATM ports, configuring, 38-44

atm scrambling cell-payload command, 43

authentication

- AAA, 281
- AH, troubleshooting VPN tunnels, 300
- CCMP, 291
- CHAP, troubleshooting VPN tunnels, 299
- data packets, 247
- EAP, troubleshooting VPN tunnels, 299
- LEAP, wireless network security, 291
- open authentication, 290
- PAP, troubleshooting VPN tunnels, 299
- RADIUS, 281
 - VPN tunnels, troubleshooting*, 299
 - wireless network security*, 292
- sharekey authentication, 290
- TACACS+, 281

authoritative name servers, DNS, 212

authorization, 281

B

B8ZS (bipolar 8 zero substitution), 38

backbones (OSPF), 102

backups

- BDR, OSPF configuration, 108
- router configuration files, 54, 85-88

bandwidth command, EIGRP load balancing/redundancy, 126-127

bandwidth route metric (dynamic routing), 72

Bash (Bourne again shell) files, Linux, 346

BDR (Backup Designated Routers), OSPF configuration, 108

beacons, wireless network security, 290

BGP (Border Gateway Protocol), 400

- address family ipv6 command, 413
- AS, 401
- autonomous-system [AS_Number] command, 416
- BGP Best Path Selection Algorithm, 410-412
- BGP4+, IPv6 Internet routing, 413
- configuring, 401-409
- eBGP, 401
- EGP, 401
- family inet6 command, 419
- iBGP, 401
- IPv6 Internet routing
 - BGP4+, 413*
 - troubleshooting, 413-415*
- ISP connections, 402-409
- Juniper router configuration, 415-420
- neighbor [ip address] remote [as number] command, 402-403
- neighbor IPv6_address activate command, 413
- neighbor IPv6_address remote as AS_Number command, 413
- Networking Challenge scenarios, 409-410
- network IPv6_network command, 413
- no bgp default ipv4 unicast command, 413
- peering, 401
- router bgp AS command, 402
- set group [BGP-group_name] neighbor [next_hop_address] command, 416
- set group [BGP-group_name] type [external/internal] command, 417
- set router-id [ip_address] command, 416
- sh ip bgp neighbor command, 406-408
- sh ip bgp sum command, 404-405
- sh ip int brief command, 403
- sh ip route command, 408
- show bgp ipv6 unicast ? command, 415
- show bgp ipv6 unicast summary command, 413
- show bgp neighbor command, 418
- show ip bgp commnd, 411-412
- show ip bgp sum command, 417
- show route protocol bgp command, 418-419
- sh show running-configuration (sh run) command, 408

binding, DHCP IP address deployments, 202

block-snmp term (filter lists), 279

boot services (Linux), enabling/disabling, 382-384

BOOTP (Bootstrap Protocol), IP address management, 195

BPDU filter, 288

BPDU guard, switch security, 288

broadcast domains, 16

buffer, VoIP QoS, 439

C

C (routing table code), 59

cable. See also wireless networks

fiber-optic, 7

twisted-pair, 7

campus networks, 4

access layer, 6

cable, 7

core layer, 5

data flow, 6

distribution layer, 5

gateways, 15

IP address ranges, 8

IP assignments, 15

IP host addresses, 11-14

IP subnet design, 7-15

media, selecting, 6, 7

physical network design, 4-7

redundancy, 5

routed networks, 28-44

routers

configuration file backups, 54, 85-88

three-router networks, 56

two-router networks, 57-58

routing protocols

distance vector protocols, 73-85

dynamic routing, 54, 70-74, 101-129

hybrid routing protocols, 101, 119-129

ip route command, 58-60

link state protocols, 74, 101-118

netstat -r command, 55

OSPF, 134-137

RIP, 75-85, 130-133, 137

RIPv2, 82-83

route print command, 55

routing loops, 75

routing redistribution, 129-143

routing table code C, 59

routing table code S, 59

show ip route (sh ip route) command, 58-61

static routing, 54-55, 58-70

TFTP, 54, 85-88

subnetworks, 9-11

supernets, 11

VLAN, 16-28

wireless networks, 7

cat command

Linux networking, 375

printing file contents in Linux, 346

CBWFQ (class-based weighted fair queuing), VoIP data traffic, 440

CCMP (Cipher Block Chaining Message Authentication Code Protocol), WPA2, 291

ccTLDs (country-code top-level domains), 190

cd command, changing directories in Linux, 348-349

cd files command, changing working directories to files in Linux, 352

CDP (Cisco Discovery Protocol)

router security, 283

switch security, 289

CHAP (Challenge Handshake Authentication Protocol), troubleshooting VPN tunnels, 299

chgrp command, changing file group ownership in Linux, 357

chkconfig command, enabling/disabling boot services, 382-384

chmod command, changing file/directory permissions in Linux, 353-355

chown command, changing file ownership in Linux, 356

CIDR (classless interdomain routing), 8-14

Class A IP addresses, 8

Class B IP addresses, 8

Class C IP addresses, 8

classful addressing, 75

class maps, VoIP QoS configuration, 440-441

class network addresses, 75

CLNS (Connectionless Network Service), 112, 115-118

clns routing command, IS-IS IPv6 routing, 326

CLOSE-WAIT TCP connection state, 233

CLOSED TCP connection state, 233

CNAME records (Canonical Name records), DNS, 215-216

cnls routing command, 114

CODEC (coders/decoders), VoIP and, 432

collectors (flow), protocol analysis/forensics, 250

command line (Linux), 343

commit and- quit command

IS-IS configuration on Juniper routers, 177

Juniper router route redistribution, 179

OSPF configuration on Juniper routers, 174

RIP configuration on Juniper routers, 172

commit command, Juniper routers

hostname configuration, 167

RIP configuration, 172

- confidentiality (data packets), 247**
- configuration hardening, routers, 280-283**
- configure command, Juniper routers**
 - IS-IS configuration, 175
 - OSPF configuration, 173
- conf t (configure terminal) command, 62**
 - ACL router configuration, 273
 - BGP, ISP connections, 402-403
 - EIGRP configuration, 121
 - OSPF configuration, 106
 - SNMP configuration, 244
- connection-oriented protocols, 230**
- contiguous networks, 76**
- convergence, dynamic routing, 72**
- copy run start command, RIP configuration, 81**
- copy running-configuration startup-configuration (copy run start) command, 66**
- copying files in Linux, 352**
- core layer, 5**
- cost paths, 68**
- cost route metric (dynamic routing), 73**
- country domains, DNS, 210**
- cp command, copying files in Linux, 352**
- CQ (custom queuing), VoIP data traffic, 440**
- crypto key generate rsa command, router security, 281**
- CSU/DSU (channel service unit/data service unit), 38**

D

- DAD (Duplicate Address Detection), IPv6, 318**
- data encapsulation**
 - encapsulation (encap) command, 39
 - s hint s0/0 command, 40
- data filtering**
 - DHCP filtering, 260-261
 - FTP filtering, 256-258
 - Wireshark protocol analyzer, 251-261
- data flow, campus networks, 6**
- data packets**
 - ACK packets, TCP three-way handshakes, 230
 - authentication, 247
 - captures via Wireshark, 243-244
 - confidentiality, 247
 - DHCP, 198-199
 - FIN packets, 232
 - integrity, 247
 - packet filtering, 270
 - pps, storm control, 287

- SYN packets, TCP three-way handshakes, 230
- SYN-ACK packets, firewall analysis of, 271
- SYN+ACK packets, TCP three-way handshakes, 230
- VoIP packets, 442, 445-449
 - buffer, 439*
 - jitter, 438, 451*
 - network equipment MAC addresses table, 443*
 - network latency, 439, 451*
 - packet sequence numbers, 432*
 - queuing, 439, 440*
 - RTCP, 432*
 - RTP headers, 432*
 - telephone call packet codes for call processors table, 443*
 - timestamps, 432*
 - WRED, 439*

data speeds, 7

data traffic analysis

- collectors (flow), 250
- Jflow, 250
- NetFlow, 250-251
- Sflow, 250
- SNMP
 - configuring, 244-250*
 - MIB, 244*
 - snmp community [community string], 245*
 - SNMPv2, 247*
 - SNMPv3, 247-250*

datagrams, 66-67, 309

DDoS (Distributed Denial of Service) attacks, 270

dead time (routers), OSPF configuration, 108

default gateways, 54-55

default metric bandwidth delay reliability load MTU command, route redistribution, 140

default version control, RIPv2 configuration, 83

delay command, EIGRP load balancing/redundancy, 127

delay route metric (dynamic routing), 73

deleting files from Linux, 351

DES (Data Encryption Standard), ESP, 301

description command, BGP and ISP connections, 402

destination unreachable error messages, 68

df command (Linux), 363

df -kh command (Linux), 364

DHCP (Dynamic Host Configuration Protocol)

- filtering, Wireshark protocol analyzer, 260-261
- IP address management
 - ARP broadcasts, 200*
 - binding, 202*
 - DHCP ACK messages, 196*

- DHCP Discover messages*, 195
- DHCP Offer messages*, 196
- DHCP Request messages*, 196
- ipconfig/release command*, 196
- ipconfig/renew*, 196
- ip helper command*, 197
- MT ACK data packets*, 199
- MT Discover data packets*, 198
- MT Offer data packets*, 198
- MT Request data packets*, 198
- show ip dhcp binding command*, 202
- show ip dhcp pool command*, 202
- SOHO deployments*, 201-203
- unicast packages*, 197
- Diffie-Hellman key exchange algorithm (IKE), troubleshooting VPN tunnels**, 301
- Dig (Domain Information Groper), DNS**, 211-214
- Dijkstra, E.W.**, 74, 102
- directed broadcasts, smurf attacks**, 269
- discontiguous networks**, 76
- displaying Juniper router interfaces**, 166-167
- distance vector protocols**, 73-74
 - IS-IS route redistribution, 137
 - RIP, 76
 - classful addressing*, 75
 - class network addresses*, 75
 - configuring*, 77-81
 - copy run start command*, 81
 - ip address command*, 77
 - limitations of*, 82
 - Network Challenge example*, 84-85
 - network command*, 75, 79
 - no shut command*, 77
 - route redistribution*, 130-133, 137
 - router rip command*, 75-79
 - routing loops*, 75
 - show ip interface brief (sh ip int brief) command*, 78
 - show ip protocol (sh ip protocol) command*, 78
 - show ip route (sh ip route) command*, 79, 82
 - show running-configuration (sh run) command*, 79-81
 - RIPv2, configuring, 82-83
- distribution layer, campus networks**, 5
- dmesg command, troubleshooting Linux boot processes**, 378
- DMZ (demilitarized zones), firewalls**, 272
- DNS (Domain Name Services)**
 - authoritative name servers, 212
 - country domains, 210
 - Dig, 211-214
 - forward DNS, 209
 - FQDN, 213
 - Linux and, 376
 - local server administration example, 218
 - lookup utilities, 211-213
 - networks, adding clients to, 218-219
 - nslookup command, 211-213
 - A records*, 214
 - CNAME records*, 215
 - MX records*, 216
 - NS records*, 216
 - PTR records*, 215
 - SoA*, 214
 - SRV records*, 218
 - TXT records*, 217
 - PQDN, 213
 - reverse DNS, 209
 - Root Hints file (root hints), 209
 - root servers, 209
 - RR
 - A records*, 214, 218-219
 - CNAME records*, 215-216
 - MX records*, 216-217
 - NS records*, 216
 - PTR records*, 215
 - SoA*, 214
 - SRV records*, 217-218
 - TXT records*, 217
 - TLD, 210
 - tree hierarchy, 210-213
 - whois command, 212
- domain names**
 - ccTLDs, 190
 - DNS, 209
 - A records*, 214, 218-219
 - authoritative name servers*, 212
 - CNAME records*, 215-216
 - country domains*, 210
 - Dig*, 211-214
 - dynamically adding clients to networks*, 219
 - forward DNS*, 209
 - FQDN*, 213
 - local server administration example*, 218
 - lookup utilities*, 211-213
 - manually adding clients to networks*, 218
 - MX records*, 216-217
 - nslookup command*, 211-218
 - NS records*, 216

- PQDN*, 213
- PTR records*, 215
- reverse DNS*, 209
- Root Hints file (root hints)*, 209
- root servers*, 209
- RR*, 214-219
- SoA*, 214
- TLD*, 210
- tree hierarchy*, 210-213
- TXT records*, 217-218
- whois command*, 212

domain registrars, 192

FQDN, 213

gTLDs, 190

IANA, 190

IDN language table registry, 191

in-addr.arpa, 190

int, 190

managing, 190

PQDN, 213

TLD, 192

whois protocol, 192-195

DoS (Denial of Service) attacks, 268

double-colon notation (IPv6), 312

DR (Designated Routers), 108

DS (digital signal), 37

DSCP (Differentiated Services Code Point) values, VoIP class maps, 441

DTP (Dynamic Trunking Protocol), switch security, 289

DUAL Finite State Machine (EIGRP), 120

dynamic NAT (Network Address Translation), 206

dynamic routing protocols, 54, 70

AD, 71

convergence, 72

distance vector protocols, 73-74

hybrid routing protocols, 101, 119-129

link state protocols

EIGRP, 101

hello packets, 74, 101-102, 143-146

IS-IS, 101, 112-119

OSPF, 74, 101-112, 132-137

load balancing, 72

metrics

bandwidth, 72

cost, 73

delay, 73

hop count, 72-73

load, 73

reliability, 72

ticks, 73

path determination, 72

prefix length, 71

Dynamic VLAN (Virtual Local Area Networks), 18

dynamic/private ports, 228

E

E2 network routes, OSPF route redistribution, 134

E911 (Enhanced 911), VoIP and, 442

EAP (Extensible Authentication Protocol)

VPN tunnels, troubleshooting, 299

wireless network security, 291

eBGP (external Border Gateway Protocol), BGP Internet routing, 401

echo requests, ICMP forensics, 241

edge routers, ACL configuration, 273-275

edit interfaces ge-0/0/0 command, Juniper router IP address assignments, 168

edit policy options command, Juniper router route redistribution, 179

edit protocols rip command, RIP configuration on Juniper routers, 171

edit routing-options static command, STATIC route configuration on Juniper routers, 169

Educause, TLD registration, 192

EF (Expedited Forwarding), VoIP class maps, 441

EGP (Exterior Gateway Protocol), BGP Internet routing, 401

EIGRP (Enhanced Interior Gateway Routing Protocol), 101, 119

bandwidth command, 126-127

configuring, 121-125

conf t command, 121

delay command, 127

DUAL Finite State Machine, 120

EX, 138

hello packets, 120

IP addresses, 121

IPv6 routing, 325-326

load balancing, 125-128

Neighbor Discovery Recovery, 120

network command, 121-124

Networking Challenge examples, 128-129

Protocol Dependent Modules, 120

redundancy, 125-128

Reliable Transport Protocol, 120

route redistribution, 133-141

router eigrp [AS-number] command, 121-124

- sh ip eigrp neighbors command, 125
- sh ip int brief command, 122
- sh ip protocol command, 121-123
- sh ip route command, 122-125
- show ip eigrp topology command, 126-128
- show ip route command, 136
- show ip route eigrp topology command, 127
- sh run command, 122
- subnet masks, 121
- enable secret command, EXEC level passwords and router security, 280**
- encapsulation (encap) command, 39**
- encryption**
 - 3DES, 301
 - AES, 291, 301
 - CHAP, troubleshooting VPN tunnels, 299
 - DES, 301
 - HTTP, 282-283
 - HTTPS, 282-283
 - SNMP, 282
 - Type 5, router security, 280
 - Type 7, router security, 280
- equal-cost load balancing, 68. See also load balancing**
- ERRDISABLE state, switchport security, 286-287**
- error messages, destination unreachable errors, 68**
- ESP (Encapsulating Security Payload), troubleshooting VPN tunnels, 300**
- ESTABLISHED TCP connection state, 233**
- Ethernet cards, 371**
- eui-64, IPv6 addresses, 321**
- everything-else term (filter lists), 279**
- EXEC level passwords, 280**
- executable (x) permissions in Linux, 355**
- EX (external EIGRP type), 138**
- exit interfaces, static routing, 63-64**
- export advertise_static policies, Juniper router route redistribution, 180**
- export command, Juniper router route redistribution, 180**
- extended ACL (Access Lists), 273**

F

- failing threshold (storm control), 287**
- FEE80::/64 subnet prefix (IPv6), 318**
- fiber-optic cable, 7**
- FIFO (First in, First out) status, VoIP data traffic, 439**

- filtering data**
 - DHCP filtering, 260-261
 - FTP filtering, 256-258
 - Wireshark protocol analyzer, 251-261
- filter lists, 278-279. See also ACL (Access Lists)**
- FIN packets, 232**
- FIN-WAIT-1 TCP connection state, 233**
- FIN-WAIT-2 TCP connection state, 233**
- Firefox, 368**
- firewalls, 270**
 - DMZ, 272
 - open networks and, 272
 - placement of, 272
 - show firewall command, filter lists, 279
 - spoofs and, 271
 - stateful firewalls, 271
 - SYN-ACK packets, 271
 - web servers and, 271
- first queued position (VoIP data traffic), 439**
- flat networks, 17**
- floating static routes, 68-69**
- forensics/protocol analysis**
 - ARP forensics, 236-237, 241
 - collectors (flow), 250
 - ICMP forensics, 237-242
 - Jflow, 250
 - NetFlow, 250
 - ping command, 238, 241
 - Sflow, 250
 - SNMP, 244-250
 - TCP forensics, netstat command, 234-235
 - TCP three-way handshakes, 230-233
 - TCP/UDP ports, 228-229
 - UDP forensics, 233-235
 - Wireshark protocol analyzer, 239-241
 - data filtering, 251-261*
 - data packet captures, 243-244*
 - DHCP filtering, 260-261*
 - FTP filtering, 256-258*
 - right-click filtering logic rules, 258-259*
- forward DNS (Domain Name Services), 209**
- FP (Format Prefix), IPv6 addresses, 314**
- FQDN (Fully Qualified Domain Names), 213**
- fstab files (Linux), 362**

FTP (File Transfer Protocol)

filtering, Wireshark protocol analyzer, 256-258

Linux FTP client, 376-377

ncftp, Linux and, 376-377

full IPv6 addresses, 311

G-H

gateway addresses, routed networks, 30

gateways, 15

default gateways, 54-55

gateway of last resort, 61

loopbacks, 55

VoIP gateways, 434

global addresses (IP addresses), 205

global unicast addresses, 313

GRE (Generic Routing Encapsulation), VPN, 293-294

gTLDs (generic top-level domains), 190

H.323 signaling technique, PSTN and, 431

hacked (security), defining, 270

HDLC (high-level data link control), 38-40

hello packets

hello intervals, 143

IGP, 145

link state protocols, 74, 101-102, 143-146

Neighbor Discovery Recovery (EIGRP), 120

network masks, 143

OSPF, 145

RID, 144

router dead intervals, 143

help, JUNOS operating system, 161

hexadecimal IPv6 addresses, converting IPv4 addresses to, 312

H field (show ip eigrp neighbors command), 125

hidden files, viewing in Linux, 346

high-end routers, core layer, 5

history command (Linux), 364

Hold field (show ip eigrp neighbors command), 125

hop count route metric (dynamic routing), 72-73

hostnames

Juniper routers, configuring in, 167

Linux, changing in, 377

hosts, defining, 277

HP Procurve switches, configuring, 27-28

HTTP (Hyper-text Transfer Protocol), encryption, 282-283

HTTP ports, 228

httpd

httpd.conf files, 370

yum install httpd command, 368

HTTPS ports, 228

HTTPS, encryption, 282-283

hubs, 6

hybrid routing protocols

EIGRP, 101, 119

bandwidth command, 126-127

configuring, 121-125

conf t command, 121

delay command, 127

DUAL Finite State Machine, 120

EX, 138

IP addresses, 121

load balancing, 125-128

Neighbor Discovery Recovery, 120

network command, 121-124

Networking Challenge examples, 128-129

Protocol Dependent Modules, 120

redundancy, 125-128

Reliable Transport Protocol, 120

route redistribution, 133-141

router eigrp [AS-number] command, 121-124

sh ip eigrp neighbors command, 125

sh ip int brief command, 122

sh ip protocol command, 121-123

sh ip route command, 122-125

show ip eigrp topology command, 126-128

show ip route eigrp topology command, 127

sh run command, 122

subnet masks, 121

IS-IS

redistribute connected command, 142

redistribute static command, 142

route redistribution, 133, 141-143

show ip route command, 142

show ip route isis command, 142-143

I

IANA (Internet Assigned Numbers Authority), 190-191

iBGP (internal Border Gateway Protocol), BGP Internet routing, 401

ICANN (Internet Corporation of Assigned Names and Numbers)

IANA and, 191

well known/reserved ports, 228

ICMP (Internet Control Message Protocol), forensics, 237-238, 241-242

IDN (Internationalized Domain Name) language table registry, 191

IETF (Internet Engineering Task Force), OSPF development, 101

ifconfig command

IPv6 connections, troubleshooting, 327

Linux networking, 371

ifdown command, Linux networking, 372

ifup command, Linux networking, 372

IGP (Interior Gateway Protocol)

hello packets, 145

OSPF development, 101

IKE (Internet Key Exchange), troubleshooting VPN tunnels, 301

in-addr.arpa, 190

inet, 167

integrity (data packets), 247

integrated IS-IS. See IS-IS

interface cost, OSPF load balancing, 110

Interface field (show ip eigrp neighbors command), 125

Interface ID, IPv6 addresses, 315

interface identifier (IPv6 addresses), 313

interface VLAN 1, 21

Internal Ethernet Interface (Juniper routers, permanent interfaces), 166

Internet Protocol Version 6 (TCP/IPv6) Properties window (Windows 7), 316-317

Internet routing

BGP, 400

address family ipv6 command, 413

AS, 401

ASN, 401

autonomous-system [AS_Number] command, 416

BGP4+, 413

BGP Best Path Selection Algorithm, 410-412

configuring, 401-409

eBGP, 401

EGP, 401

iBGP, 401

IPv6 Internet routing, 413-415

ISP connections, 402-409

Juniper router configuration, 415-420

neighbor [ip address] remote [as number] command, 402-403

neighbor IPv6_address activate command, 413

neighbor IPv6_address remote as AS_Number command, 413

Networking Challenge scenarios, 409-410

network IPv6_network command, 413

no bgp default ipv4 unicast command, 413

peering, 401

router bgp AS command, 402

set group [BGP-group_name] neighbor [next_hop_address] command, 416

set group [BGP-group_name] type [external/internal] command, 417

set router-id [ip_address] command, 416

sh ip bgp neighbor command, 406-408

sh ip bgp sum command, 404-405

sh ip int brief command, 403

sh ip route command, 408

show bgp ipv6 unicast ? command, 415

show bgp ipv6 unicast summary command, 413

show ip bgp command, 411-412

show running-configuration (sh run) command, 408

Internet connections, configuring, 400-409

IPv6, troubleshooting, 413-415

stubby areas, 400

totally stubby areas, 400

WAN connections, 398-400

Internet sockets, 228

InterVLAN routing, configuring, 35-37

int (intergovernmental) domain registries, 190

int Gig3/1 command, IPv6 router configuration, 320

intranets, 8

int tunnel0 command, VPN virtual interface configuration (router to router), 295

ip access-group 100 out command, ACL configuration, 274

ip address command, RIP configuration, 77

IP addresses

APIPA, 196

ARIN, 191

BOOTP, 195

campus networks, 8

CIDR, 8-14

Class A IP addresses, 8

Class B IP addresses, 8

Class C IP addresses, 8

DHCP

ARP broadcasts, 200

binding, 202

DHCP ACK messages, 196

DHCP Discover messages, 195

DHCP Offer messages, 196

DHCP Request messages, 196

ipconfig/release command, 196

ipconfig/renew command, 196

ip helper command, 197

MT ACK data packets, 199

MT Discover data packets, 198

MT Offer data packets, 198

MT Request data packets, 198

show ip dhcp binding command, 202

show ip dhcp pool command, 202

SOHO deployments, 201-203

unicast packages, 197

DNS

authoritative name servers, 212

country domains, 210

Dig, 211-214

forward DNS, 209

lookup utilities, 211-213

nslookup command, 211-218

reverse DNS, 209

Root Hints file (root hints), 209

root servers, 209

TLD, 210

tree hierarchy, 210-213

whois command, 212

EIGRP configuration, 121

global addresses, 205

hosts, 277

IANA, 191

Juniper routers, assigning addresses in, 168

lease time, 195

local addresses, 205

NAT, 8, 204-208

number resource management, 191

PAT, 8, 204, 207

preferred keyword, 168

primary IP addresses, 35

private IP addresses, translating, 8

secondary IP addresses, 35

stopping data traffic from, ACL configuration, 277-278

UDP, 198

VLAN, assigning to, 21

whois protocol, 192-195

ip address [ip address] [subnet mask] command, BGP and ISP connections, 402

ip address [ip_address] [subnet_mask] secondary command, 35

IP assignments, campus networks, 15

ipconfig command, troubleshooting IPv6 connections, 327

ipconfig/release command, IP address management, 196

ipconfig/renew command, IP address management, 196

ip flow ingress command, NetFlow configuration, 251

ip helper command, IP address management, 197

IP host addresses, campus networks, 11-14

IPng. See IPv6

ip ospf cost command, OSPF load balancing, 110

ip route-cache flow command, NetFlow configuration, 251

ip route command, 58-62

ip router isis command, IS-IS configuration, 114

ip routing command, 37, 114

IPSec (IP security), 300, 310

IP subnet design, campus networks, 7-15

IP telephony. See VoIP

IP tunnels, 293, 299

IPv4 (Internet Protocol version 4)

address conversion to IPv6 hexadecimal addresses, 312

datagrams, 309

IPv6 comparisons to, 308, 311

V4ADDR, 315

IPv6 (Internet Protocol version 6)

6to4 prefix, 314

anycast IPv6 addresses, 314

connections, troubleshooting, 327-328

DAD, 318

datagrams, 309

double-colon notation, 312

EIGRP routing, 325-326

FE80::/64 subnet prefix, 318

FP, 314

full IPv6 addresses, 311

global unicast addresses, 313

Interface ID, 315

interface identifier, 313

Internet Protocol Version 6 (TCP/IPv6) Properties window settings (Windows 7), 316-317

Internet routing, 413-415

IPSec, 310

IPv4 address conversion to IPv6 hexadecimal address example, 312

IPv4 comparisons to, 308, 311

IPv6 stateless autoconfiguration, 318

IS-IS routing, 326

link local addresses, 318

Local Area Connections Properties window settings (Windows 7/Windows XP), 315

multicast IPv6 addresses, 314

Neighbor Solicitation messages, 318

- network prefix, 313
- OSPFv3 routing, 325
- prefix length, 313
- Privacy Extensions for Stateless Address
Autoconfiguration (RFC 4941), 319
- RIP routing, 324
- router configuration, 2001 and DB8::/32 prefix, 320-324
- SLAAC, 311
- SLA ID, 315
- static routing, 324
- TLA ID (0x2002), 314
- unicast IPv6 addresses, 313
- ipv6 address ipv6 interfaced address command, IPv6
router configuration, 321**
- ipv6 eigrp as_number command, EIGRP IPv6 routing,
326**
- ipv6 enable command, IPv6 router configuration, 320**
- ipv6 ospf process_id area area_id command, OPFv3 IPv6
routing, 325**
- ipv6 router eigrp as_number command, EIGRP IPv6
routing, 326**
- ipv6 router isis command, IS-IS IPv6 routing, 326**
- ipv6 router ospf process_id command, OPFv3 IPv6 rout-
ing, 325**
- ipv6 unicast-routing command, IPv6 router configura-
tion, 320**
- ISAKMP (Internet Security Association and Key Manage-
ment Protocol), troubleshooting VPN tunnels, 301**
- IS-IS (Intermediate System-Intermediate System), 101**
 - ABR, 112
 - Area ID, 112
 - CLNS, 112, 115-116
 - configuring, 114-118
 - IPv6 routing, 326
 - Juniper routers, 175-180
 - L1 routers, 112
 - L2 routers, 112
 - load balancing, 117-118
 - NET, 112
 - Networking Challenge example, 118-119
 - NSEL, 113
 - redistribute connected command, 142
 - redistribute isis IS-IS_Level command, 141
 - redistribute static command, 142
 - redundancy, 117-118
 - route redistribution, 133, 137, 141-143
 - show ip route command, 142
 - show ip route isis command, 142-143
 - System ID, 113

- ISL (Inter-Switch Link), VLAN tagging, 24**
- ISP (Internet Service Providers), 8, 402-409**
- Is system-config- * command, Linux system administra-
tion, 385**

J

- Jflow, 250**
- jitter, VoIP QoS, 438, 451**
- Juniper routers**
 - at (ATM), 164
 - BGP configuration, 415-420
 - inet, 167
 - IS-IS configurations, 175-178
 - JUNOS operating system, 160-169
 - multi-services cards, 164
 - oc-3 connections, 164
 - oc-12 connections, 164
 - OSPF configurations, 173-175
 - permanent interfaces, 166
 - PIC, 164
 - ping command, 165
 - RIP configurations, 171-172
 - route redistribution, 178-181
 - show interfaces brief command, 166-167
 - STATIC route configurations, 169-170
 - t2/ds3 cards, 164
 - transient interfaces, 166
- JUNOS operating system**
 - family inet6 command, 419
 - filter lists, 278-279
 - help, 161
 - operational mode, 160-165
 - Out of Band Management statements, 164
 - re0 {and re1}, 164
 - router configuration mode, 166-169
 - show ? command, 162
 - <show c spacebar> command, 162
 - show configuration command, 163
 - <show in spacebar> command, 162
 - show version command, 163

K-L

- kill [PID] command (Linux), 361**
- kill -9 [PID] command (Linux), 361**
- L1 routers, 112**
- L2 routers, 112**

- L2F (Layer 2 Forwarding) protocol, troubleshooting VPN tunnels, 300**
- L2TP (Layer 2 Tunneling Protocol), troubleshooting VPN tunnels, 300**
- language table registry (domain names), 191**
- LAN (Local Area Networks), 6, 16. See also campus networks**
- LAST_ACK TCP connection state, 233**
- last command, Linux security, 380-381**
- latency (networks), VoIP QoS, 439, 451**
- Layer 2 switches**
 - access layer, 6
 - broadcast domains, 16
 - core layer, 5
 - flat networks, 17
 - VLAN, IP address assignments, 21
- Layer 3 addressing. See network addresses**
- Layer 3 networks. See routed networks**
- Layer 3 switches, core layer, 5**
- LEAP (Lightweight Extensible Authentication Protocol), wireless network security, 291**
- lease time, IP addresses, 195**
- line passwords, router security, 280**
- link local addresses (IPv6), 318**
- link state protocols, 74**
 - EIGRP, 101, 136
 - hello packets, 74, 101-102, 143-146
 - IS-IS, 101
 - ABR, 112
 - Area ID, 112
 - CLNS, 112, 115-118
 - cnls routing command, 114
 - configuring, 113-117
 - ip router isis command, 114
 - ip routing command, 114
 - L1/L2 routers, 112
 - L1 routers, 112
 - L2 routers, 112
 - load balancing, 117, 118
 - NET, 112
 - Network Challenge example, 118-119
 - NSEL, 113
 - redistribute isis IS-IS_Level command, 141
 - redundancy, 117-118
 - router isis command, 114
 - sh ip protocol command, 114
 - show cnls is neighbors command, 115-116
 - show ip int brief command, 113
 - show ip route (sh ip route) command, 114

- show ip route isis (sh ip route isis) command, 115*
- show ip route isis command, 117-118*
- show isis neighbor command, 116*
- sh run command, 116*
- System ID, 113*
- OSPF, 74**
 - advantages/disadvantages of, 103
 - areas, 102, 105
 - backbones, 102
 - BDR, 108
 - configuring, 103-108
 - conf t command, 106
 - dead time, 108
 - DR, 108
 - E2 network routes, 134
 - hello packets, 102, 143-146
 - ip ospf cost command, 110
 - load balancing, 109-110
 - LSA, 101
 - neighbor ID, 108
 - network command, 105
 - Networking Challenge exercises, 111-112
 - network numbers, 105
 - redistribute connected command, 134
 - redistribute connected subnets command, 134
 - redistribute ospf command, 141
 - redistribute static command, 135
 - redistribute static subnets command, 135
 - redundancy, 109-110
 - route flapping, 103
 - router ospf [process id] command, 104-106
 - routing redistribution, 132-137
 - sh ip int brief command, 104-106
 - sh ip ospf interface command, 109
 - sh ip ospf neighbor command, 108
 - sh ip protocol command, 108
 - sh ip route command, 107
 - sh ip route ospf command, 107
 - show ip ospf neighbor command, 134
 - show ip route command, 134-135
 - show ip route interface command, 109
 - show ip route ospf command, 134, 137
 - state of FULL, 108
 - VLSM, 102
 - wild card bits, 105

Linux

- administration commands
 - df command, 363
 - df -kh command, 364

- history command*, 364
- kill [PID] command*, 361
- kill -9 [PID] command*, 361
- man command*, 358-359
- mount command*, 358, 362
- ps command*, 358-361
- shutdown command*, 358, 364
- shutdown -h now command*, 364
- su command*, 358, 362
- Tab key shortcut*, 364
- umount command*, 364
- up arrow shortcut*, 364
- applications, installing/uninstalling, 365-371
- cat command, 346
- cd command, 348-349, 352
- chgrp command, 357
- chkconfig command, 382-384
- chmod command, 353-355
- chown command, 356
- command line, 343
- cp command, 352
- df command, 363-364
- directories
 - changing*, 348-349
 - changing permissions of*, 353-355
 - changing working directories to files*, 352
 - executable (x) permissions*, 355
 - httpd.conf files*, 370
 - making directories*, 350
 - permission attribute settings table*, 353-354
 - printing working (current) directory*, 349-352
 - removing directories*, 350
 - resolv.conf directory*, 376
- dmesg command, 378
- DNS service, 376
- executable (x) permissions, 355
- files
 - attributes of*, 345
 - Bash files*, 346
 - changing directories*, 348-349
 - changing group ownership of*, 357
 - changing ownership of*, 356
 - changing permissions of*, 353-355
 - changing working directories to files*, 352
 - copying*, 352
 - deleting*, 351
 - displaying contents of*, 346
 - executable (x) permissions*, 355
 - fstab files*, 362
 - httpd.conf files*, 370
 - listing*, 344-346, 352
 - making directories*, 350
 - moving*, 351
 - password files*, 348
 - permission attribute settings table*, 353-354
 - printing contents to screen*, 346
 - printing working (current) directory*, 349-352
 - removing directories*, 350
 - renaming*, 351
 - viewing hidden files*, 346
- Firefox, 368
- FTP client, 376-377
- history command, 364
- httpd, 368-370
- ifconfig command, 371
- ifdown command, 372
- ifup command, 372
- Is system-config- * command, 385
- kill [PID] command, 361
- kill -9 [PID] command, 361
- last command, 380-381
- lo, 371
- logging onto, 339
- ls command, 344-346, 352
- ls -l command, 344
- ls -la command, 346, 352
- man command, 358-359
- mkdir command, 350
- more command, 346
- mount command, 358, 362
- mv command, 351
- netstat -ap command, 384
- networking
 - cat command*, 375
 - changing hostnames*, 377
 - DNS service*, 376
 - Ethernet cards*, 371
 - FTP client*, 376-377
 - ifconfig command*, 371
 - ifdown command*, 372
 - ifup command*, 372
 - lo*, 371
 - network start command*, 373-374
 - network stop command*, 373
 - route add default gw command*, 373
 - SSH installations*, 375-376

- network start command, 373-374
- network stop command, 373
- nmap command, 382
- ps command, 358-361
- pwd command, 349-352
- reboot command, 379-380
- rm command, 351
- rmdir command, 350
- root access, 339
- route add default gw command, 373
- route cat command, 375
- security
 - last command*, 380-381
 - nmap command*, 382
 - password files*, 348
 - system administration*, 387
 - w command*, 381
 - who command*, 381
- shutdown command, 358, 364
- shutdown -h now command, 364
- SSH installations, 375-376
- su command, 358, 362
- system administration, 389
 - Is system-config- * command*, 385
 - security*, 387
 - system-config- [tool-name] command*, 385
 - system-config-date command*, 386
 - system-config-network command*, 388
- Tab key shortcut, 364
- telnet, 366
- troubleshooting
 - boot processes*, 378-379
 - boot services*, 382-384
 - network connections*, 384
- umount command, 364
- UNIX versus, 338
- up arrow shortcut, 364
- user accounts, adding, 340-341
- w command, 381
- who command, 381
- YUM, installing/uninstalling applications via, 365-371

LISTEN TCP connection state, 233

lo (loopbacks), Linux, 371

load balancing, 68. See also equal-cost load balancing

- dynamic routing, 72
- EIGRP, 125-128
- IS-IS, 117-118
- OSPF, 109-110

- load route metric (dynamic routing), 73
- local addresses (IP addresses), 205
- Local Area Connections Properties window (Windows XP/Windows 7), IPv6 network settings, 315
- local user accounts, router security, 280
- logging (security), routers, 283-285
- logical addresses, 29
- logical networks, DMZ, 272
- lookup utilities, DNS, 211-213
- loopbacks, 55, 371
- loops (routing), 75
- LSA (link state advertisements), 101
- ls command, listing files in Linux, 344-346, 352
- ls -l command, listing files in Linux, 344
- ls -la command, listing files in Linux, 346, 352

M

- MAC addresses, switchport security, 286
- man (manual) command (Linux), 358-359
- man yum command (Linux, YUM), 365
- Management Ethernet Interface (Juniper routers, permanent interfaces), 166
- {master} mode (routers), 161
- MD5 hashing algorithm (CHAP), troubleshooting VPN tunnels, 299
- media, selecting for campus networks, 6-7
- metrics, dynamic routing, 72-73
- MIB (Management Information Base), SNMP, 244
- minimum ones density, 38
- mkdir command, making directories in Linux, 350
- MLD (Multicast Listener Discovery), IPv6 router configuration, 320
- MLS (multilayer switches), 32-33
- more command, displaying file contents in Linux, 346
- mount command (Linux), 358, 362
- moving files in Linux, 351
- MT ACK data packets, IP address management, 199
- MT Discover data packets, IP address management, 198
- MT Offer data packets, IP address management, 198
- MT Request data packets, IP address management, 198
- multicast IPv6 addresses, 314
- multi-homed Internet connections, 400
- multiple LAN (Local Area Networks), 16
- multiple VLAN (Virtual Local Area Networks), trunk ports, 24-26
- multiplexing, TDM and VoIP, 433
- multi-services cards, 164

mv command, moving/renaming files in Linux, 351
MX records (Mail Exchange records), DNS, 216-217

N

name-Sales command, 27
name servers (authoritative), DNS, 212
naming files in Linux, 351
NAT (Network Address Translation), 8, 204-205
 dynamic NAT, 206
 NAT overload. See PAT
 show ip nat translation, 207-208
 static NAT, 206
ncftp and Linux, 376-377
ND (neighbor discovery) protocol, IPv6 router configuration, 322
Neighbor Discovery Recovery (EIGRP), 120
neighbor ID, OSPF configuration, 108
neighbor [ip address] remote [as number] command, 402-403
neighbor IPv6_address activate command, 413
neighbor IPv6_address remote as AS_Number command, 413
Neighbor Solicitation messages (IPv6), 318
NET (Network Entity Title), IS-IS, 112
NetFlow, 250-251
net masks (Linux), 371
netstat -ap command, troubleshooting Linux network connections, 384
netstat command, TCP/UDP forensics, 234-235
netstat -r command, 55
network addresses, 29
network command, 75
 EIGRP configuration, 121-124
 OSPF configuration, 105
 RIP configuration, 79
network IPv6_network command, 413
network latency, VoIP QoS, 439, 451
network masks, 143
network numbers, OSPF configuration, 105. See also subnets
network prefix (IPv6 addresses), 313
network start command, Linux networking, 373-374
network stop command, Linux networking, 373
Networking Challenge exercises
 BGP, 409-410
 EIGRP, 128-129
 IS-IS, 118-119
 OSPF, 111-112

RIP, 84-85
static routing, 70

networks

advertising, 75
campus networks, 4
 access layer, 6
 core layer, 5
 data flow, 6
 designing, 4-15
 distance vector protocols, 73-85
 distribution layer, 5
 dynamic routing protocols, 54, 70-74, 101-129
 fiber-optic cable, 7
 gateways, 15
 hybrid routing protocols, 101, 119-129
 IP address ranges, 8
 IP subnet design, 7-15
 link state protocols, 74, 101-119
 media selection, 6-7
 OSPF, 134-137
 physical network design, 4-7
 redundancy, 5
 RIP, 75-85, 130-133, 137
 RIPv2, 82-83
 routed networks, 28-44
 router configuration file backups, 54, 85-88
 routing protocols, 54
 routing redistribution, 129-143
 static routing protocols, 54-55, 58-70
 subnetworks, 9-11
 supernets, 11
 TFTP, 54, 85-88
 three-router networks, 56
 twisted-pair cable, 7
 two-router networks, 57-58
 VLAN, 16-28
 wireless networks, 7
contiguous networks, 76
discontiguous networks, 76
domain names
 ccTLDs, 190
 DNS, 209-219
 domain registrars, 192
 FQDN, 213
 gTLDs, 190
 IANA, 190
 IDN language table registry, 191
 in-addr.arpa, 190

- int*, 190
- managing*, 190
- PQDN*, 213
- TLD*, 192
- whois protocol*, 192-195
- flat networks, 17
- forensics/protocol analysis, 228
 - ARP forensics*, 236-237, 241
 - ARP replies*, 241
 - collectors (flow)*, 250
 - data filtering*, 251-261
 - DHCP filtering*, 260-261
 - FTP filtering*, 256-258
 - ICMP forensics*, 237-242
 - Jflow*, 250
 - NetFlow*, 250-251
 - ping command*, 238, 241
 - Sflow*, 250
 - SNMP*, 244-250
 - TCP forensics*, 234-235
 - TCP three-way handshakes*, 230-233
 - TCP/UDP ports*, 228-229
 - UDP*, 233-235
 - Wireshark protocol analyzer*, 239-244, 251-261
- IP addresses
 - APIPA*, 196
 - ARIN*, 191
 - ARP broadcasts*, 200
 - binding*, 202
 - BOOTP*, 195
 - DHCP*, 195-203
 - DNS*, 209-218
 - dynamic NAT*, 206
 - global addresses*, 205
 - IANA*, 191
 - ipconfig/release command*, 196
 - ipconfig/renew command*, 196
 - ip helper command*, 197
 - lease time*, 195
 - local addresses*, 205
 - MT ACK data packets*, 199
 - MT Discover data packets*, 198
 - MT Offer data packets*, 198
 - MT Request data packets*, 198
 - NAT*, 204-208
 - number resource management*, 191
 - PAT*, 204, 207
 - SOHO DHCP deployments*, 201-203
 - static NAT*, 206
 - UDP*, 198
 - unicast packages*, 197
 - whois protocol*, 192-194
- IP assignments, campus networks, 15
- IP host addresses, campus networks, 11-14
- LAN
 - access layer*, 6
 - campus networks*, 4
 - multiple LAN*, 16
 - sizes of*, 16
- Linux
 - adding user accounts*, 340-341
 - Bash files*, 346
 - cat command*, 375
 - cd command*, 348-349, 352
 - changing file directories*, 348-349
 - changing file/directory permissions*, 353-355
 - changing file group ownership*, 357
 - changing file ownership*, 356
 - changing hostnames*, 377
 - changing working directories to files*, 352
 - chgrp command*, 357
 - chkconfig command*, 382-384
 - chmod command*, 353-355
 - chown command*, 356
 - command line*, 343
 - copying*, 352
 - cp command*, 352
 - deleting*, 351
 - df command*, 363
 - df -kh command*, 364
 - displaying file contents*, 346
 - dmesg command*, 378
 - DNS service*, 376
 - Ethernet cards*, 371
 - executable (x) permissions*, 355
 - file attributes tables*, 345
 - file/directory attribute settings table*, 353-354
 - Firefox*, 368
 - fstab files*, 362
 - FTP client*, 376-377
 - history command*, 364
 - httpd*, 368
 - httpd.conf files*, 370
 - ifconfig command*, 371
 - ifdown command*, 372
 - ifup command*, 372

- installing/uninstalling applications*, 365-371
- Is system-config- * command*, 385
- kill [PID] command*, 361
- kill -9 [PID] command*, 361
- last command*, 380-381
- listing files*, 344-346, 352
- lo*, 371
- logging onto*, 339
- ls command*, 344-346, 352
- ls -la command*, 346, 352
- ls -l command*, 344
- making directories*, 350
- man command*, 358-359
- mkdir command*, 350
- more command*, 346
- mount command*, 358, 362
- moving*, 351
- mv command*, 351
- netstat -ap command*, 384
- network start command*, 373-374
- network stop command*, 373
- networking*, 371-377
- nmap command*, 382
- password files*, 348
- print command*, 346
- printing file contents to screen*, 346
- printing working (current) directories*, 349-352
- ps command*, 358-361
- pwd command*, 349-352
- reboot command*, 379-380
- removing directories*, 350
- renaming*, 351
- resolv.conf directory*, 376
- rm command*, 351
- rmdir command*, 350
- root access*, 339
- route add default gw command*, 373
- security*, 380-382, 387
- shutdown command*, 358, 364
- shutdown -h now command*, 364
- SSH installations*, 375-376
- su command*, 358, 362
- system administration*, 385-389
- system-config- [tool-name] command*, 385
- system-config-date command*, 386
- system-config-network command*, 388
- Tab key shortcut*, 364
- telnet*, 366
- troubleshooting boot process*, 378-380
- troubleshooting boot services*, 382-384
- troubleshooting network connections*, 384
- umount command*, 364
- UNIX versus*, 338
- up arrow shortcut*, 364
- viewing hidden files*, 346
- w command*, 381
- who command*, 381
- YUM*, 365-371
- logical networks, DMZ, 272
- open networks and firewalls, 272
- physical networks
 - campus networks*, 4-7
 - DMZ*, 272
- protocol assignments, 191
- PSTN, 430-431
- routed networks, 28
 - ATM*, 41-44
 - atm framing cbitplcp command*, 43
 - ATM port configuration*, 37-44
 - atm scrambling cell-payload command*, 43
 - encapsulation (encap) command*, 39
 - gateway addresses*, 30
 - InterVLAN routing configuration*, 35-37
 - ip routing command*, 37
 - logical addresses*, 29
 - MLS*, 32-33
 - network addresses*, 29
 - network segments*, 31
 - no shut command*, 39
 - port configuration*, 33-35
 - router interfaces*, 29
 - router on a stick*, 35
 - routers*, 29-30
 - routing tables*, 30
 - serial port configuration*, 37-44
 - service-module tl command*, 40
 - show atm vc command*, 43
 - show atm vc interface atml/0.33 command*, 44
 - show controller atm slot/port command*, 44
 - show controller Tl slot/port command*, 41
 - SONET*, 33
 - SVC*, 42
 - SVI*, 37
 - VCC*, 42
 - VCI*, 42
 - VPC*, 42

- VPI, 42
- VWIC, 40, 41
- WAN, 33
- WIC, 40
- wire speed routing, 32
- security
 - ACL, 270-278, 283-285
 - DDoS attacks, 270
 - directed broadcasts, smurf attacks, 269
 - DoS attacks, 268
 - edge routers, 273-275
 - filter lists, 278-279
 - firewalls, 270-272
 - hacked, definition of, 270
 - HTTP, 282-283
 - HTTPS, 282-283
 - IP addresses, stopping data traffic from, 277-278
 - logging, 283-285
 - packet filtering, 270
 - proxy servers, 270
 - remote data hosts, stopping data traffic from, 277
 - routers, 279-285
 - SMB, 273-275
 - smurf attacks, 268-269
 - SNMP, 282
 - spoofs, 268, 271
 - stateful firewalls, 271
 - switches, 285-289
 - SYN attacks, 268
 - TCP headers, 278
 - UDP, 276
- subnet masks, 32
- Subnet, NET, 31
- TCP/IP, telnet, 366
- UNIX versus Linux, 338
- VLAN, 16-17
 - 802.1Q, 18, 24-26
 - configuring, 18-23
 - Dynamic VLAN, 18
 - HP Procurve switches, 27-28
 - interface VLAN I, 21
 - IP address assignments, 21
 - name-Sales command, 27
 - no shutdown command, 21
 - port-based VLAN, 17
 - protocol-based VLAN, 17
 - show interface command, 22
 - show interface status command, 22
 - show running-config (sh run) command, 22-23
 - show vlan 2 command, 28
 - show vlan brief command, 20
 - show vlan command, 18-20, 27
 - show vlan name vlan-name command, 21
 - show vlan vlan-id command, 21
 - Static VLAN, 18, 26
 - switchport access vlan vlan-id command, 20
 - switchport mode access command, 20
 - tag-based VLAN, 17
 - tagged Port_number command, 28
 - tagging, 23-26
 - trunk ports, 24-25
 - vlan 2 command, 27
 - vlan database command, 19
 - VLAN ID, 18-19
 - VLAN tagging, 18
 - VoIP, 440
 - VTP, 289
- VoIP, 430
 - buffer, 439
 - class maps, 440-441
 - CODEC, 432
 - complete IP telephony solutions, 436-437
 - configuration example, 440-442
 - data packets, 442-449
 - E911, 442
 - gateways, 434
 - H.323 signaling technique, 431
 - jitter, 438, 451
 - network latency, 439, 451
 - packet sequence numbers, 432
 - PBX, 430, 433-437
 - PCM digital signals, 431
 - policy maps, 440
 - PSTN, 430
 - QoS, 438-442, 451
 - queuing, 439-440
 - RTCP, 432
 - RTP headers, 432
 - security, 440, 449-451
 - signaling, 430
 - SIP signaling technique, 431
 - SS7 signaling technique, 431
 - SSIP signaling technique, 431
 - TDM, 433
 - tie line replacements (PBX), 433-435
 - timestamps, 432

- upgrading PBX, 435-436*
 - VLAN, 440*
 - WRED, 439*
 - VPN
 - GRE, 293-294*
 - IP tunnels, 293, 299*
 - remote-access VPN, 293*
 - security, 292-301*
 - site-to-site VPN, 293*
 - tunnels, troubleshooting, 299-301*
 - virtual interface configuration (router to router), 294-298*
 - WAN, 33
 - wireless networks
 - campus networks, 7*
 - data speeds, 7*
 - security, 289-292*
 - nmap command, Linux security, 382**
 - no auto-summary command, RIPv2 configuration, 83**
 - no bgp default ipv4-unicast command, 413**
 - no ip directed broadcast command, directed broadcasts in smurf attacks, 269**
 - nonauthoritative answers, DNS lookup utilities, 213**
 - no service config command, router security, 283**
 - no service tcp-small-servers command, router security, 282**
 - no service udp-small-servers command, router security, 282**
 - no shut command, 39, 62, 77**
 - no shutdown command, 21**
 - no switchport command, 35**
 - NSEL (Network Service Access Point Selector), IS-IS, 113**
 - nslookup command, DNS, 211, 213**
 - A records, 214*
 - CNAME records, 215*
 - MX records, 216*
 - NS records, 216*
 - PTR records, 215*
 - SoA, 214*
 - SRV records, 218*
 - TXT records, 217*
 - NS records (Name Server records), DNS, 216**
 - NTP (Network Time Protocol), 284**
 - null0 interfaces, static routing, 64-65**
- ## O
-
- oc-3 connections, Juniper routers, 164**
 - oc-12 connections, Juniper routers, 164**
 - open authentication, wireless network security, 290**
 - open networks and firewalls, 272**
 - openssh, Linux SSH installations, 375**
 - operational mode (JUNOS), 160-165**
 - OSPF (Open Shortest Path First), 74, 101**
 - advantages/disadvantages of, 103*
 - areas, 102, 105*
 - backbones, 102*
 - configuring, 103*
 - areas, 105*
 - BDR, 108*
 - conf t command, 106*
 - dead time, 108*
 - DR, 108*
 - neighbor ID, 108*
 - network command, 105*
 - network numbers, 105*
 - router ospf [process id] command, 104-106*
 - sh ip int brief command, 104-106*
 - sh ip ospf interface command, 109*
 - sh ip ospf neighbor command, 108*
 - sh ip protocol command, 108*
 - sh ip route command, 107*
 - sh ip route ospf command, 107*
 - state of FULL, 108*
 - wild card bits, 105*
 - E2 network routes, 134*
 - export advertise_static command, 180*
 - Juniper router configurations, 173-175*
 - hello packets, 101-102, 143-146*
 - load balancing, 109-110*
 - LSA, 101*
 - Networking Challenge exercises, 111-112*
 - redistribute connected command, 134*
 - redistribute connected subnets command, 134*
 - redistribute ospf command, 141*
 - redistribute static command, 135*
 - redistribute static subnets command, 135*
 - redundancy, 109-110*
 - route flapping, 103*
 - routing redistribution, 132-137*
 - set ospf export advertise_static command, 180*
 - show ip ospf neighbor command, 134*
 - show ip route command, 134-135*
 - show ip route ospf command, 134, 137*
 - VLSM, 102*
- OSPFv3 (Open Shortest Path First Interior Gateway Protocol), hello packets, 145**
- OSPFv3 routing, IPv6, 325**

Out of Band Management statements, JUNOS operating system, 164
overloading routers, 8
ownership (Linux files), changing, 356-357

P

packets (data)

- ACK packets, TCP three-way handshakes, 230
- authentication, 247
- captures via Wireshark, 243-244
- confidentiality, 247
- DHCP, 198-199
- FIN packets, 232
- integrity, 247
- packet filtering, 270
- pps, storm control, 287
- SYN packets, TCP three-way handshakes, 230
- SYN-ACK packets, firewall analysis of, 271
- SYN+ACK packets, TCP three-way handshakes, 230
- VoIP packets, 442, 445-449
 - buffer, 439*
 - jitter, 438, 451*
 - network equipment MAC addresses table, 443*
 - network latency, 439, 451*
 - packet sequence numbers, 432*
 - queuing, 439-440*
 - RTCP, 432*
 - RTP headers, 432*
 - telephone call packet codes for call processors table, 443*
 - timestamps, 432*
 - WRED, 439*

PAP (Password Authentication Protocol), troubleshooting VPN tunnels, 299

passwords

- Linux password files, 348
- PAP, troubleshooting VPN tunnels, 299
- router security, 280

path determination, dynamic routing, 72

PAT (Port Address Translation), 8, 204, 207

PBX (Private Branch Exchanges) and VoIP, 430

- complete IP telephony solutions, switching to, 436-437
- PBX upgrades, 435-436
- tie lines, replacing, 433-435

PCM (Pulse Code Modulation) digital signals and VoIP, 431

peering, BGP Internet routing, 401

permanent interfaces (Juniper routers), 166

permissions (Linux files/directories), changing, 353-355
permit ip any any command, ACL configuration, 274-276
physical networks

- DMZ, 272
- campus networks, 4-7

PIC (Physical Interface Cards), 164

PID (Process ID) field, ps (processes) command (Linux), 360

ping command, 241

- ICMP forensics, 238-239, 242
- Juniper routers, 165
- VPN virtual interface configuration (router to router), 297

ping6 command, troubleshooting IPv6 connections, 327

policy maps, VoIP QoS configuration, 440

ports

- ATM ports, configuring, 37-44
- routed ports, configuring, 33-35
- security, 286-287
- serial ports, configuring, 37-44
- STP, 288
- TCP/UDP ports, 228-229
- VLAN, 17

PPP (Point-to-Point Protocol), 38, 299

pps (packets per second), storm control, 287

PPTP (Point to Point Tunneling Protocol), troubleshooting VPN tunnels, 299

PQ (priority queuing), VoIP data traffic, 440

PQDN (Partial Qualified Domain Names), 213

preferred keyword (IP address statements), 168

prefix length

- dynamic routing, 71
- IPv6 addresses, 313

primary IP addresses, 35

Privacy Extensions for Stateless Address

- Autoconfiguration (RFC 4941), IPv6, 319

private IP addresses, translating, 8

private/dynamic ports, 228

protected violation action (switchport security), 286

protocol analysis/forensics, 228

- ARP forensics, 236
 - arp-a command, 237*
 - ARP replies, 241*
 - ARP requests, 241*
 - show-arp command, 237*

- collectors (flow), 250

- ICMP forensics, 237

- echo requests, 241*

- ping command, 238-239, 242*

- Jflow, 250
- NetFlow, 250-251
- ping command, 238, 241
- Sflow, 250
- SNMP
 - configuring*, 244-250
 - MIB*, 244
 - snmp community [community string]*, 245
 - SNMPv2*, 247
 - SNMPv3*, 247-250
- TCP forensics, netstat command, 234-235
- TCP three-way handshakes, 230-233
- TCP/UDP ports, 228-229
- UDP, 233-235
- Wireshark protocol analyzer, 239-241
 - data filtering*, 251-261
 - data packet captures*, 243-244
 - DHCP filtering*, 260-261
 - FTP filtering*, 256-258
 - right-click filtering logic rules*, 258-259
- protocol-based VLAN (Virtual Local Area Networks), 17
- Protocol Dependent Modules (EIGRP), 120
- protocols, assigning, 191
- proxy servers, 270
- ps (processes) command (Linux), 358-361
- PSTN (Public Switched Telephone Networks), VoIP and, 430-431
- PTR records (Pointer records), DNS, 215
- pwd command, printing working (current) directory in Linux, 349-352

Q-R

- Q Cnt (Queue Count) field (show ip eigrp neighbors command), 125
- QoS (Quality of Service), VoIP and, 438
 - buffer, 439
 - class maps, 440-441
 - configuration example, 440-442
 - jitter, 438, 451
 - network latency, 439, 451
 - policy maps, 440
 - queuing, 439-440
 - WRED, 439
- question mark (?), JUNOS operating system, 161
- queuing, VoIP QoS, 439-440
- RA (Router Advertisement) messages, IPv6 router configuration, 322

- RADIUS (Remote Authentication Dial-In User Service), 281
 - VPN tunnels, troubleshooting, 299
 - wireless network security, 292
- re0 {and re1}, JUNOS operating system, 164
- reboot command, troubleshooting Linux boot processes, 379-380
- redistribute connected command, 132-134, 138, 142
- redistribute connected subnets command, 134
- redistribute eigrp AS_id [metric 0-16777214] command, 137
- redistribute eigrp AS_number metric 0-16 command, 133
- redistribute isis IS-IS_Level command, 137, 141
- redistribute isis IS-IS_number metric 0-16 command, 133
- redistribute ospf command, 141
- redistribute ospf process_id 0-16 command, 133
- redistribute rip command, 137
- redistribute rip metric bandwidth delay reliability load MTU command, 140
- redistribute static command, 132, 135, 138, 142
- redistribute static subnets command, 135
- redistribution connected command, 131
- redistribution protocol command, 131
- redundancy
 - campus networks, 5
 - core layer, 5
 - EIGRP, 125-128
 - IS-IS, 117-118
 - OSPF, 109-110
- registered ports, 228
- relays (VoIP). See gateways; VoIP, gateways
- reliability route metric (dynamic routing), 72
- Reliable Transport Protocol (EIGRP), 120
- remote-access VPN (Virtual Private Networks), 293
- remote data hosts, stopping data traffic from, 277
- renaming files in Linux, 351
- reserved/well known ports, 228
- resolv.conf directory (Linux), 376
- restrict violation action (switchport security), 286
- reverse DNS (Domain Name Services), 209
- RID (Router ID), hello packets, 144
- RIP (Routing Information Protocol)
 - classful addressing, 75
 - class network addresses, 75
 - configuring, 77-81
 - copy run start command, 81
 - ip address command, 77
 - IPv6, 324

- Juniper routers
 - route configuration, 171-172*
 - route redistribution, 179*
- limitations of, 82
- Network Challenge example, 84-85
- network command, 75, 79
- no shut command, 77
- route redistribution, 130-133, 137
- router rip command, 75-79
- routing loops, 75
- show ip interface brief (sh ip int brief) command, 78
- show ip protocol (sh ip protocol) command, 78
- show ip route (sh ip route) command, 79, 82
- show running-configuration (sh run) command, 79-81
- RIPng (Routing Information Protocol next generation), IPv6 RIP routing, 324**
- rip-tag, IPv6 RIP routing, 325**
- RIPv2 (Routing Information Protocol version 2)**
 - configuring, 82-83
 - default version control, 83
 - no auto-summary command, 83
 - router rip command, 82-83
 - show ip protocol (sh ip protocol) command, 83
 - version 2 command, 83
- RIR (Regional Internet Registries), 191**
- rising threshold (storm control), 287**
- rm command, deleting files from Linux, 351**
- rmdir command, removing directories from Linux, 350**
- root access (Linux), 339**
- Root Hints file (root hints), DNS, 209**
- root servers (DNS), 209**
- route add default gw command, Linux networking, 373**
- routed networks, 28, 33**
 - ATM, 41-44
 - atm framing cbitplcp command, 43
 - ATM ports, configuring, 37-44
 - atm scrambling cell-payload command, 43
 - encapsulation (encap) command, 39
 - gateway addresses, 30
 - InterVLAN routing, configuring, 35-37
 - ip routing command, 37
 - logical addresses, 29
 - MLS, 32-33
 - network addresses, 29
 - network segments, 31
 - no shut command, 39
 - ports, configuring, 33-35
 - router interfaces, 29
 - router on a stick, 35
 - routers, 29-30
 - routing tables, 30
 - serial ports, configuring, 37-44
 - service-module tl command, 40
 - show atm vc command, 43
 - show atm vc interface atml/0.33 command, 44
 - show controller atm slot/port command, 44
 - show controller Tl slot/port command, 41
 - SONET, 33
 - SVC, 42
 - SVI, 37
 - VCC, 42
 - VCI, 42
 - VPC, 42
 - VPI, 42
 - VWIC, 40-41
 - WAN, 33
 - WIC, 40
 - wire speed routing, 32
- route flapping, 103**
- route print command, 55**
- router bgp AS command, BGP and ISP connections, 402**
- router configuration mode (JUNOS)**
 - command/prompt summary table, 169
 - commit command, 167
 - hostname configuration, 167
 - IP address assignments, 168
 - router interfaces, displaying, 166-167
- router dead intervals, hello packets, 143**
- router eigrp [AS-number] command, EIGRP configuration, 121-124**
- router isis command, 114, 326**
- router ospf [process id] command, OSPF configuration, 104-106**
- router rip command, 75**
 - RIP configuration, 77-79
 - RIPv2 configuration, 82-83
- routers, 29-30**
 - ABR, 112
 - BDR, OSPF configuration, 108
 - BGP, 400
 - address family ipv6 command, 413*
 - AS, 401*
 - ASN, 401*
 - autonomous-system [AS_Number] command, 416*
 - BGP4+, 413*
 - BGP Best Path Selection Algorithm, 410-412*

- configuring*, 401-409
- eBGP*, 401
- EGP*, 401
- family inet6 command*, 419
- iBGP*, 401
- IPv6 Internet routing*, 413-415
- ISP connections*, 402-409
- Juniper router configuration*, 415-420
- neighbor [ip address] remote [as number] command*, 402-403
- neighbor IPv6_address activate command*, 413
- neighbor IPv6_address remote as AS_Number command*, 413
- Networking Challenge scenarios*, 409-410
- network IPv6_network command*, 413
- no bgp default ipv4 unicast command*, 413
- peering*, 401
- router bgp AS command*, 402
- set group [BGP-group_name] neighbor [next_hop_address] command*, 416
- set group [BGP-group_name] type [external/internal] command*, 417
- set router-id [ip_address] command*, 416
- sh ip bgp neighbor command*, 406-408
- sh ip bgp sum command*, 404-405
- sh ip int brief command*, 403
- sh ip route command*, 408
- show bgp ipv6 unicast ? command*, 415
- show bgp ipv6 unicast summary command*, 413
- show bgp neighbor command*, 418
- show ip bgp command*, 411-412
- show ip bgp sum command*, 417
- show route protocol bgp command*, 418-419
- show running-configuration (sh run) command*, 408
- configuration file backups*, 54, 85-88
- dead time*, OSPF configuration, 108
- DR*, 108
- edge routers*, ACL, 273-275
- high-end routers*, 5
- Internet routing*
 - BGP*, 400-409
 - Internet connections*, 400-401
 - IPv6 Internet routing*, 413-415
 - multi-homed connections*, 400
 - stubby areas*, 400
 - totally stubby areas*, 400
 - WAN connections*, 398-400
- IPv6 router configuration*
 - 2001, DB8::/32 prefix*, 324
 - eui-64*, 321
 - int Gig3/1 commnd*, 320
 - ipv6 address ipv6 interface address command*, 321
 - ipv6 enable command*, 320
 - ipv6 unicast-routing*, 320
 - MLD*, 320
 - ND protocol*, 322
 - RA messages*, 322
 - Router Solicitation messages*, 322
 - show ipv6 interface command*, 321
 - show ipv6 interface gigabitEthernet 3/1 command*, 322
- IPv6 routing*
 - EIGRP routing*, 325-326
 - IS-IS routing*, 326
 - OSPFv3 routing*, 325
 - RIP routing*, 324
 - static routing*, 324
- Juniper routers*, 160
 - at (ATM)*, 164
 - BGP configuration*, 415-420
 - commit command*, 167
 - inet*, 167
 - IS-IS configurations*, 175-178
 - JUNOS operating system*, 160
 - multi-services cards*, 164
 - oc-3 connections*, 164
 - oc-12 connections*, 164
 - operational mode (JUNOS operating system)*, 160-165
 - OSPF configurations*, 173-175
 - permanent interfaces*, 166
 - PIC*, 164
 - ping command*, 165
 - RIP configurations*, 171-172
 - router configuration mode (JUNOS operating system)*, 166-169
 - route redistribution*, 178-181
 - show interfaces brief command*, 166-167
 - STATIC route configurations*, 169-170
 - t3/ds3 cards*, 164
 - transient interfaces*, 166
- L1 routers*, 112
- L2 routers*, 112
- logical addresses*, 29
- {master} mode*, 161
- NAT*, 8
- network addresses*, 29
- NTP*, 284

- overloading, 8
- route distribution, Juniper routers, 178-181
- router interfaces, 29
- router on a stick, 35
- routing protocols, 54
 - AD summary table*, 71
 - distance vector protocols*, 73-85
 - dynamic routing*, 54, 70-74, 101-129
 - hybrid routing protocols*, 101, 119-129
 - ip route command*, 58-60
 - link state protocols*, 74, 101-119
 - netstat -r command*, 55
 - OSPF*, 134-137
 - RIP*, 75-85, 130-133, 137
 - route print command*, 55
 - routing loops*, 75
 - routing redistribution*, 129-143
 - routing table code C*, 59
 - routing table code S*, 59
 - show ip route (sh ip route) command*, 58-61
 - static routing*, 54-70
 - TFTP*, 54, 85-88
- security, 279
 - AAA*, 281
 - access*, 280-282
 - CDP*, 283
 - configuration hardening*, 280-283
 - crypto key generate rsa command*, 281
 - enable security command*, 280
 - encryption*, 280
 - EXEC level passwords*, 280
 - line passwords*, 280
 - local user accounts*, 280
 - logging*, 283-285
 - no service config command*, 283
 - no service tcp-small-servers command*, 282
 - no service udp-small-servers command*, 282
 - RADIUS*, 281
 - router services*, 282-283
 - RXA keys*, 281
 - service-password encryption command*, 280
 - TACACS+*, 281
 - transport input none command*, 281
 - transport input ssh command*, 281
 - username admin privilege 10 password @
dmlnp@\$swd command*, 281
 - username [name] privilege [level] password
[password_string] command*, 280
- state of FULL, OSPF configuration, 108

- three-router campus networks, 56
- two-router campus networks, 57-58
- VPN, virtual interface configuration, 294-298
- WRED, 439

Router Solicitation messages, IPv6 router configuration, 322

routing loops, 75

routing protocols, 54

- AD summary table*, 71
- distance vector protocols*
 - IS-IS*, 137
 - RIP*, 75-85, 130-133, 137
 - RIPv2*, 82-83
- dynamic routing*, 54, 70
 - AD*, 71
 - bandwidth metric*, 72
 - convergence*, 72
 - cost metric*, 73
 - delay metric*, 73
 - distance vector protocols*, 73-74
 - hop count metric*, 72-73
 - hybrid routing protocols*, 101, 119-129
 - link state protocols*, 74, 101-119
 - load balancing*, 72
 - load metric*, 73
 - metrics*, 72
 - path determination*, 72
 - prefix length*, 71
 - reliability metric*, 72
 - ticks metric*, 73
- hybrid routing protocols*, 101, 119-129
- ip route command*, 58-60
- link state protocols*
 - EIGRP*, 101
 - IS-IS*, 101, 112-119
 - OSPF*, 74, 101-112, 132-137
- netstat -r command*, 55
- route print command*, 55
- route redistribution*, 129
 - default metric bandwidth delay reliability load MTU
command*, 140
 - EIGRP*, 133-141
 - IS-IS*, 133, 141-143
 - Juniper routers*, 178-181
 - OSPF*, 132-137
 - rdistribute connected command*, 134
 - rdistribute connected subnets command*, 134
 - reasons for*, 129-130
 - redistribute connected command*, 132, 138

- redistribute isis IS-IS_Level command, 141*
- redistribute ospf command, 141*
- redistribute ospf process_id 0-16 command, 133*
- redistribute rip metric bandwidth delay reliability load MTU command, 140*
- redistribute static command, 132, 135, 138*
- redistribute static subnets command, 135*
- redistribution connected command, 131*
- redistribution protocol command, 131*
- RIP, 130-133, 137*
- sh ip route command, 136*
- sh ip route rip command, 132-133*
- show ip ospf neighbor command, 134*
- show ip route command, 131-135*
- show ip route ospf command, 134, 137*
- show ip route rip command, 131*
- routing loops, 75
- routing tables, 59
- show ip route (sh ip route) command, 58-61
- static routing, 54, 58-60
 - configuration command summary table, 69*
 - configure terminal (conf t) command, 62*
 - configuring, 61-69*
 - copy running-configuration startup-configuration (copy run start) command, 66*
 - cost paths, 68*
 - datagrams, 66-67*
 - default gateways, 54-55*
 - equal-cost load balancing, 68*
 - exit interfaces, 63-64*
 - floating static routes, 68-69*
 - gateway of last resort, 61*
 - ip route command, 62*
 - load balancing, 68*
 - loopbacks, 55*
 - Network Challenge example, 70*
 - no shut command, 62*
 - null0 interfaces, 64-65*
 - show ip interface brief (sh ip int brief) command, 62*
 - show ip route command, 64*
 - show ip route (sh ip route) command, 69*
 - show ip route static (sh ip route static) command, 62-63*
 - show running-config (sh run) command, 65*
 - show startup-config (sh run) command, 65*
 - traceroute destination-ip-address command, 66-67*
 - tracert destination-ip-address command, 67-68*
 - variable length subnet masking, 58*
 - write memory (wr m) command, 66*
- TFTP, 54, 85-88

routing tables, 30

RR (Resource Records), DNS

- A records, 214, 218-219
- CNAME records, 215-216
- MX records, 216-217
- NS records, 216
- PTR records, 215
- SoA, 214
- SRV records, 217-218
- TXT records, 217

RSA keys, router security, 281

RTCP (Real Time Control Protocol), VoIP and, 432

RTO (Retransmission Timeout) field (show ip eigrp neighbors command), 125

RTP (Real Time Protocol) headers, VoIP and, 432

S

S (routing table code), 59

secondary IP addresses, 35

security

- AAA, 281
- accounting, 281
- ACL, 270-272
 - access-list 100 deny udp any any ee snmp command, 274*
 - access-list 100 deny udp any any eq 161 command, 273*
 - access-list permit ip any any command, 274*
 - configure terminal command, 273*
 - edge routers, 273-275*
 - extended ACL, 273*
 - false TCP headers, 278*
 - hosts, 277*
 - ip access-group 100 out command, 274*
 - IP addresses, stopping data traffic from, 277-278*
 - permit ip any any command, 274-276*
 - placement of, 274*
 - remote data hosts, stopping data traffic from, 277*
 - router logging, 283-285*
 - show access-list 100 command, 274*
 - show access-list command, 275-276*
 - SMB, 273-275*
 - standard ACL, 273*
 - UDP, 276*
- AH, troubleshooting VPN tunnels, 300
- authentication
 - AAA, 281
 - CCMP, 291
 - LEAP, 291

- open authentication*, 290
- RADIUS*, 292
- sharekey authentication*, 290
- authorization, 281
- DDoS attacks, 270
- DoS attacks, 268
- encryption
 - 3DES*, 301
 - AES*, 291, 301
 - CHAP*, 299
 - DES*, 301
 - HTTP*, 282-283
 - HTTPS*, 282-283
 - SNMP*, 282
 - Type 5 encryption*, 280
 - Type 7 encryption*, 280
- ESP, troubleshooting VPN tunnels, 300
- filter lists, 278-279
- firewalls, 270
 - DMZ*, 272
 - open networks and*, 272
 - placement of*, 272
 - SN-ACK packets*, 271
 - spoofs and*, 271
 - stateful firewalls*, 271
 - web servers and*, 271
- hacked, defining, 270
- HTTP, 282-283
- HTTPS, 282-283
- IPSec, 300, 310
- Linux
 - last command*, 380-381
 - nmap command*, 382
 - password files*, 348
 - system administration*, 387
 - w command*, 381
 - who command*, 381
- logging, routers, 283-285
- packet filtering, 270
- passwords, Linux password files, 348
- ports (switches), 286-288
- proxy servers, 270
- routers, 279
 - AAA*, 281
 - access*, 280-282
 - CDP*, 283
 - configuration hardening*, 280-283
 - crypto key generate rsa command*, 281
 - enable secret command*, 280
 - encryption*, 280
 - EXEC level passwords*, 280
 - line passwords*, 280
 - local user accounts*, 280
 - logging*, 283-285
 - no service config command*, 283
 - no service tcp-small-servers command*, 282
 - no service udp-small-servers command*, 282
 - RADIUS*, 281
 - router services*, 282-283
 - RSA keys*, 281
 - service-password encryption command*, 280
 - TACACS+*, 281
 - transport input non command*, 281
 - transport input ssh command*, 281
 - username admin privilege 10 password @ dmlnp@\$swd command*, 281
 - username [name] privilege [level] password [password_string] command*, 280
- smurf attacks, 268-269
- SNMP, 282
- spoofs, 268, 271
- switches, 285-289
- SYN attacks, 268
- TCP headers, 278
- TKIP, 291
- VoIP, 440, 449-451
- VPN, 292-294
 - troubleshooting tunnels*, 299-301
 - virtual interface configuration*, 295-298
- WEP, 290
- wireless networks, 289-292
- WPA, 291
- WPA2, 291
- Seq Num (Sequence Number) field (show ip eigrp neighbors command), 125**
- serial ports, configuring, 37-44**
- servers**
 - authoritative name servers, DNS, 212
 - proxy servers, 270
 - root servers (DNS), 209
 - web servers and firewalls, 271
- service-module tl command, 40**
- service-password encryption command, 280**
- set address command, Juniper router IP address assignments, 168**
- set metric value command, OSPF configuration on Juniper routers, 175**

set ospf export advertise_static command, Juniper router route redistribution, 180
set policy statement command, Juniper router route redistribution, 179
set protocols command, OSPF configuration on Juniper routers, 173
set protocols isis interface command, IS-IS configuration on Juniper routers, 175
set protocols ospf area area interface interface hello-interval seconds dead-interval seconds command, 173
Sflow (Sampled Flow), 250
SHA-1 (Secure Hash Algorithm-1), ESP, 301
sharekey authentication, wireless network security, 290
sh int s0/0 command, 40
sh int tunnel 0 command, VPN virtual interface configuration (router to router), 296-297
sh ip bgp neighbor command, BGP and ISP connections, 406-408
sh ip bgp sum command, BGP and ISP connections, 404-405
sh ip eigrp neighbors command, EIGRP configuration, 125
sh ip int brief command
 BGP, ISP connections, 403
 EIGRP configuration, 122
 OSPF configuration, 104-106
 VPN virtual interface configuration (router to router), 296-297
sh ip ospf interface command, OSPF configuration, 109
sh ip ospf neighbor command, OSPF configuration, 108
sh ip protocol command
 EIGRP configuration, 121-123
 IS-IS configuration, 114
 OSPF configuration, 108
sh ip route command
 BGP, ISP connections, 408
 EIGRP configuration, 122-125
 OSPF configuration, 107
 route redistribution, 136
sh ip route ospf command, 107
sh ip route rip command, 132-133
show access-list 100 command, 274
show access-list command, 275-276
show-arp command, ARP forensics, 237
show atm vc command, 43
show atm vc interface atml/0.33 command, 44
show bgp ipv6 unicast ? command, IPv6 Internet routing, 415
show bgp ipv6 unicast summary command, IPv6 Internet routing, 413
show cns interface command, IS-IS load balancing, 118
show cns is neighbors command, IS-IS configuration, 115-116
show ? command, JUNOS operating system, 162
show command, Juniper router route redistribution, 180
show configuration command, JUNOS operating system, 163
show controller atm slot/port command, 44
show controller T1 slot/port command, 41
<show c spacebar> command, JUNOS operating system, 162
show firewall command, filter lists, 279
<show in spacebar> command, JUNOS operating system, 162
show interface command, 22
show interfaces brief command, Juniper routers, 166-167
show interfaces Io0 command, IS-IS configuration on Juniper routers, 176
show interface status command, 22
show interfaces trunk command, 26
show ip bgp command, displaying contents of BGP routing tables, 411-412
show ip dhcp binding command, 202
show ip dhcp pool command, 202
show ip eigrp neighbor command, EIGRP route redistribution, 137
show ip eigrp topology command, EIGRP load balancing/redundancy, 126-128
show ip flow export command, NetFlow configuration, 251
show ip int brief command, IS-IS configuration, 113
show ip interface brief (sh ip int br) command, 34, 39
show ip interface brief (sh ip int brief) command, 62, 78
show ip nat translation command, NAT configuration, 207-208
show ip ospf neighbor command, route redistribution, 134
show ip protocol (sh ip protocol) command
 RIP configuration, 78
 RIPv2 configuration, 83
show ip route command, 64
 EIGRP route redistribution, 138
 OSPF load balancing, 109
 route redistribution, 131-135, 142
show ip route eigrp command, 137, 141
show ip route eigrp topology command, 127
show ip route isis command
 IS-IS
 configuring, 115
 load balancing, 117
 route redistribution, 142-143
show ip route ospf command, 134, 137

show ip route rip command, 131
show ip route (sh ip route) command, 58-61, 69
 IS-IS configuration, 114
 RIP configuration, 79, 82
show ip route static (sh ip route static) command, 62-63
show ipv6 interface command, IPv6 router configuration, 321
show ipv6 interface gigabitEthernet 3/1 command, IPv6 router configuration, 322
show isis adjacency command, IS-IS configuration on Juniper routers, 177
show isis neighbor command, IS-IS configuratuon, 116
show ospf interface command, 174
show ospf neighbor command, 174
show rip neighbor command, 171
show route command, 172
show route protocol isis command, 177
show route protocol ospf command, 174
show route protocol rip command, 172
show route protocol static command, STATIC route configuration on Juniper routers, 170
show run command, VPN virtual interface configuration (router to router), 298
show running-config command, IPv6 router configuration, 321
show running-config (sh run) command, 22-23, 65
show running-configuration (sh run) command
 BGP, ISP connections, 408
 RIP configuration, 79-81
show startup-config (sh run) command, 65
show version command, JUNOS operating system, 163
show vlan 2 command, 28
show vlan brief command, 20
show vlan command, 18-20, 27
show vlan id vlan-id command, 21
show vlan name vlan-name command, 21
sh run command
 EIGRP configuration, 122
 IS-IS configuration, 116
shutdown command (Linux), 358, 364
shutdown -h now command (Linux), 364
shutdown violation action (switchport security), 286
signaling
 H.323 signaling technique, 431
 PSTN and VoIP, 430
 SIP signaling technique, 431
 SS7 signaling technique, 431
 SSIP signaling technique, 431
SIP (Session Initiation Protocol) signaling technique, PSTN and, 431
site-to-site VPN (Virtual Private Networks), 293
SLAAC (Stateless Address Autoconfiguration), 311
SLA ID (Site Level Aggregation Identifier), IPv6 addresses, 315
SMB (Server Message Block), 273-275
smurf attacks, 268-269
SNMP (Simple Network Management Protocol)
 access-list 100 deny udp any any eq snmp command, 274
 allow-snmp term, filter lists, 279
 configuring, 244-250
 encryption, 282
 MIB, 244
 snmp community [community string], 245
 SNMPv2, 247
 SNMPv3, 247-250
SoA (Start of Authority), DNS, 214
SOHO (small office/home office) DHCP deployments, IP address management, 201-203
SONET (Synchronous Optical Networks), 33
spanning-tree bpdupfilter enable command, 288
spanning-tree portfast bpdupfilter default command, 288
SPF (Sender Policy Framework), TXT records, 217
SPIT (Spam over Internet Telephony), 440
spoofs, 268, 271
SRTP (Secure Real Time Protocol), VoIP security, 450
SRTT (Smooth Round Trip Time) field (show ip eigrp neighbors command), 125
SRV records (Service records), DNS, 217-218
SS7 signaling technique, PSTN and, 431
ssh [destination] command, Linux SSH installations, 376
SSH (Secure Shell), Linux installations, 375-376
SSID (Service Set Identifiers), wireless network security, 290
SSIP (Secure Session Initiation Protocol) signaling technique, PSTN and, 431
standard ACL (Access Lists), 273
stateful firewalls, 271
stateless autoconfiguration (IPv6 addresses), 318
state of FULL, OSPF configuration, 108
static NAT (Network Address Translation), 206
STATIC routes, Juniper routers
 configuring, 169-170
 route redistribution, 180
static routing protocols, 54, 60
 configuring, 61
 commands summary table, 69
 configure terminal (conf t) command, 62

- copy running-configuration startup-configuration (copy run start) command, 66*
- datagrams, 66-67*
- destination unreachable error messages, 68*
- exit interfaces, 63-64*
- ip route command, 62*
- no shut command, 62*
- null0 interfaces, 64-65*
- show ip interface brief (sh ip int brief) command, 62*
- show ip route command, 64*
- show ip route (sh ip route) command, 69*
- show ip route static (sh ip route static) command, 62-63*
- show running-config (sh run) command, 65*
- show startup-config (sh run) command, 65*
- traceroute destination-ip-address command, 66-67*
- tracert destination-ip-address command, 67*
- write memory (wr m) command, 66*
- cost paths, 68
- default gateways, 54-55
- equal-cost load balancing, 68
- floating static routes, 68-69
- gateway of last resort, 61
- ip route command, 58-60
- IPv6, 324
- load balancing, 68
- loopbacks, 55
- Network Challenge example, 70
- show ip route (sh ip route) command, 58-61
- variable length subnet masking, 58
- Static VLAN (Virtual Local Area Networks), 18, 26**
- storm control (switchport security), 287**
- STP (Spanning Tree Protocol), switch security, 288**
- stubby areas, Internet routing, 400**
- su (substitute user) command (Linux), 358, 362**
- subnet masks**
 - CIDR – subnet mask IPs conversions, 10-14
 - EIGRP configuration, 121
 - net masks (Linux), 371
 - network segments, 32
 - variable length subnet masking, 58
 - VLSM, OSPF, 102
- subnets. See also network numbers**
 - campus networks, 9-11
 - hop counts, 73
 - IP addresses, SOHO DHCP deployments, 203
 - NET, 31
 - redistribute connected subnets command, route redistribution, 134
 - redistribute static subnets command, OSPF route redistribution, 135
- supernets, 11**
- SVC (Switched Virtual Circuits), 42**
- SVI (switched virtual interfaces), 37**
- switch ports, tagged port_number command, 28**
- switches**
 - HP Procurve switches, configuring, 27-28
 - Layer 2 switches
 - access layer, 6
 - assigning IP addresses to VLAN, 21
 - broadcast domains, 16
 - core layer, 5
 - flat networks, 17
 - Layer 3 switches, 5
 - MLS, 32-33
 - ports
 - security, 286-287
 - STP, 288
 - security, 285
 - CDP, 289
 - DTP, 289
 - ports, 286-288
 - VTP, 289
 - WRED, 439
- switchport access vlan vlan-id command, 20**
- switchport mode access command, 20**
- switchport mode trunk command, 25**
- switchport port-security command, 286**
- switchport port-security maximum 2 command, 286**
- switchport trunk allowed vlan vlan_id command, 25**
- switchport trunk encapsulation dot1q command, 25**
- switchport trunk encapsulation isl command, 25**
- SYN (Synchronizing) attacks, 268**
- SYN (Synchronizing) packets, TCP three-way handshakes, 230**
- SYN-RECEIVED TCP connection state, 233**
- SYN-SENT TCP connection state, 233**
- SYN+ACK (Synchronizing Acknowledgment) packets**
 - firewall analysis of, 271
 - TCP three-way handshakes, 230
- system-config- [tool-name] command, Linux system administration, 385**
- system-config-date command, Linux system administration, 386**
- system-config-network command, Linux system administration, 388**
- System ID, IS-IS, 113**

T

t3/ds3 cards, 164

Tab key shortcut (Linux), 364

TACACS+ (Terminal Access Controller Access-Control System Plus), 281

tag-based VLAN (Virtual Local Area Networks), 17

tagged port_number command, 28

TCP (Transport Control Protocol), 230

- CLOSED connection state, 233

- CLOSE-WAIT connection state, 233

- connection state table, 232-233

- ESTABLISHED connection state, 233

- FIN-WAIT-1 connection state, 233

- FIN-WAIT-2 connection state, 233

- forensics, netstat command, 234-235

- headers, security, 278

- LAST_ACK connection state, 233

- LISTEN connection state, 233

- no service tcp-small-servers command, router security, 282

- SYN-RECEIVED connection state, 233

- SYN-SENT connection state, 233

- three-way handshakes, 230-232

- TIME-WAIT connection state, 233

TCP/IP

- Internet sockets, 228

- telnet, 366

- transport layer protocols, 230

TCP/UDP ports, 228-229

TDM (Time Division Multiplexing), VoIP and, 433

telephony (IP). See VoIP

telnet, 366

terminal monitor (term mon) command, 34

terminal no monitor (term no mon) command, 34

TFTP (Trivial File Transfer Protocol), router configuration file backups, 54, 85-88

three-router campus networks, 56

three-way handshakes (TCP), 230-232

ticks route metric (dynamic routing), 73

tie lines (PBX), replacing, 433-435

time, NTP routers, 284

timestamps, VoIP packets, 432

TIME-WAIT TCP connection state, 233

TKIP (Temporal Key Integrity Protocol), wireless network security, 291

TLA ID (0x2002), IPv6 addresses, 314

TLD (Top Level Domains), 192, 210

Tl status, verifying, 41

top command, Juniper router route redistribution, 180

totally stubby areas, Internet routing, 400

traceroute command, VPN virtual interface configuration (router to router), 298

traceroute destination-ip-address command, 66-67

tracert destination-ip-address command, 67

tracert6 command, troubleshooting IPv6 connections, 328

traffic analysis (data)

- collectors (flow), 250

- Jflow, 250

- NetFlow, 250-251

- Sflow, 250

- SNMP

 - configuring, 244-250

 - MIB, 244

 - snmp community [community string], 245

 - SNMPv2, 247

 - SNMPv3, 247-250

transient interfaces (Juniper routers), 166

transport input none command, router security, 281

transport input ssh command, router security, 281

transport layer protocols, 230

troubleshooting

- BGP, IPv6 Internet routing, 413-415

- IPv6 Internet routing, 413-415

- Linux

 - boot processes, 378-380

 - boot services, 382-384

 - network connections, 384

- VoIP

 - buffer, 439

 - jitter, 438, 451

 - network latency, 439, 451

 - queuing, 439-440

 - WRED, 439

- VPN tunnels, 299

trunk ports, 24-26

twisted-pair cable, 7

two-router campus networks, 57-58

TXT records (Text records), DNS, 217

Type 5 encryption, router security, 280

Type 7 encryption, router security, 280

U

UDP (User Datagram Protocol), 233

- ACL configuration, 276

- forensics, 234-235

- IP address management, 198
- no service udp-small-servers command, 282
- router security, 282
- UDP/TCP ports, 228-229**
- umount command (Linux), 364**
- unicast IPv6 addresses, 313**
- unicast packages, IP address management, 197**
- unicast routing (IPv6), 320**
- UNIX versus Linux, 338**
- up arrow shortcut (Linux), 364**
- upgrading PBX in VoIP networks, 435-436**
- Uptime field (show ip eigrp neighbors command), 125**
- user accounts**
 - Linux, adding in, 340-341
 - local user accounts, router security, 280
- username admin privilege 10 password @dmlnp@\$swd command, router security, 281**
- username [name] privilege [level] password [password_string] command, router security, 280**

V

- V4ADDR, IPv4 addresses, 315**
- variable length subnet masking, 58**
- VCC (Virtual Channel Connection), 42**
- VCI (virtual channel identifiers), 42**
- Verisign, TLD registration, 192**
- version 2 command, RIPv2 configuration, 83**
- violation actions (switchport security), 286**
- virtual interfaces, configuring (VPN), 294-298**
- VLAN (Virtual Local Area Networks), 16-18**
 - 802.1Q, VLAN tagging, 24-26
 - configuring, 18-23
 - Dynamic VLAN, 18
 - HP Procurve switches, configuring, 27-28
 - interface VLAN 1, 21
 - InterVLAN routing, configuring, 35-37
 - IP addresses, assigning, 21
 - multiple VLAN, trunk ports, 24-25
 - name-Sales command, 27
 - no shutdown command, 21
 - port-based VLAN, 17
 - protocol-based VLAN, 17
 - show interface command, 22
 - show interface status command, 22
 - show running-config (sh run) command, 22-23
 - show vlan 2 command, 28
 - show vlan brief command, 20

- show vlan command, 18-20, 27
- show vlan id vlan-id command, 21
- show vlan name vlan-name command, 21
- Static VLAN, 18, 26
- switchport access vlan vlan-id command, 20
- switchport mode access command, 20
- tag-based VLAN, 17
- tagged port_number command, 28
- tagging, 23-26
- trunk ports, 24-26
- vlan 2 command, 27
- vlan database command, 19
- VLAN ID, 18
- VLAN tagging, 18
- vlan [vlan_id] command, 19
- VoIP, 440
- VTP, 289
- VLSM (variable length subnet masks), OSPF, 102**
- VoIP (Voice over IP)**
 - class maps, 440-441
 - CODEC, 432
 - data packets, 442-449
 - E911, 442
 - gateways, 434
 - H.323 signaling technique, 431
 - packet sequence numbers, 432
 - PBX, 430
 - PBX upgrades, 435-436*
 - switching to complete IP telephony solutions, 436-437*
 - tie line replacements, 433-435*
 - PCM digital signals, 431
 - policy maps, 440
 - PSTN, 430
 - QoS, 438
 - buffer, 439*
 - class maps, 440-441*
 - configuration example, 440-442*
 - jitter, 438, 451*
 - network latency, 439, 451*
 - policy maps, 440*
 - queuing, 439-440*
 - WRED, 439*
 - queuing, 439-440
 - relays. See gateways
 - RTCP, 432
 - RTP headers, 432
 - security, 440, 449-451
 - signaling, 430

- SIP signaling technique, 431
- SPIT, 440
- SRTP, 450
- SS7 signaling technique, 431
- SSIP signaling technique, 431
- TDM, 433
- timestamps, 432
- troubleshooting
 - buffer*, 439
 - jitter*, 438, 451
 - network latency*, 439, 451
 - queuing*, 439-440
 - WRED*, 439
- VLAN, 440
- VPC (Virtual Path Connection), 42**
- VPI (Virtual Path Identifiers), 42**
- VPN (Virtual Private Networks)**
 - GRE, 293-294
 - IP tunnels, 293, 299
 - remote-access VPN, 293
 - security, 292-293
 - troubleshooting VPN tunnels*, 299-301
 - virtual interface configuration*, 294-298
 - site-to-site VPN, 293
 - tunnels, troubleshooting, 299-301
 - virtual interface configuration (router to router), 294-298
- VTP (Virtual Trunking Protocol), switch security, 289**
- VWIC (Voice/WAN interface cards), 40-41**

W

- w command, Linux security, 381**
- WAN (Wide-Area Networks), 33, 398-400**
- web servers and firewalls, 271**
- well known/reserved ports, 228**
- WEP (Wired Equivalent Privacy), wireless network security, 290**
- WFQ (Weighted Fair Queuing), VoIP data traffic, 440**
- who command, Linux security, 381**
- whois command, DNS, 212**
- whois protocol, 192-195**
- WIC (WAN Interface Cards), 40**
- wild card bits, OSPF configuration, 105**
- Windows 7, IPv6 network settings, 315-317**
- Windows XP, IPv6 network settings, 315**

wireless networks. See also cable

- campus networks, 7
- data speeds, 7
- security, 289
 - authentication*, 291-292
 - beacons*, 290
 - open authentication*, 290
 - sharekey authentication*, 290
 - SSID*, 290
 - TKIP*, 291
 - WEP*, 290
 - WPA*, 291
 - WPA2*, 291

Wireshark protocol analyzer, 239-241

- data filtering, 251-254
 - DHCP filtering*, 260-261
 - FTP filtering*, 256-258
 - right-click filtering logic rules*, 258-259
- data packet captures, 243-244

wire speed routing, 32

WLAN, 290

WPA2 (Wi-Fi Protected Access version 2), wireless network security, 291

WPA (Wi-Fi Protected Access), wireless network security, 291

WRED (Weighted Random Early Discard), VoIP QoS, 439

write memory (wr m) command, 66

X-Y-Z

yum install httpd command (Linux, YUM), 368

yum install openssh-server command, Linux SSH installations, 376

yum list command (Linux, YUM), 365

yum list installed command (Linux, YUM), 366

yum list telnet command (Linux, YUM), 366

yum provides [filename] command (Linux, YUM), 366

yum remove telnet command (Linux, YUM), 366

YUM (Yellowdog Updater, Modified), installing/uninstalling Linux applications, 365-371