Networking Essentials v3

Companion Guide

Cisco Certified Support Technician (CCST) Networking 100-150

Networking Academy

FREE SAMPLE CHAPTER

Networking Essentials Companion Guide Version 3: Cisco Certified Support Technician (CCST) Networking 100-150

Cisco Press

Networking Essentials Companion Guide Version 3: Cisco Certified Support Technician (CCST) Networking 100-150

Copyright© 2024 Cisco Systems, Inc.

Published by:
Cisco Press

Hoboken, New Jersey

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

$PrintCode

Library of Congress Control Number: 2023948264

ISBN-13: 978-0-13-832133-8

ISBN-10: 0-13-832133-7

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Networking Essentials course. 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 is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. 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 discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, Please visit www.netacad.com

Vice President, IT Professional
Mark Taub

Alliances Manager, Cisco Press
Caroline Antonio

Director, ITP Product Management
Brett Bartow

Executive Editor
James Manly

Managing Editor
Sandra Schroeder

Development Editor
Eleanor Bru

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Technical Editor
Dave Holzinger

Editorial Assistant
Cindy Teeters

Cover Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Timothy Wright

Proofreader
Donna E. Mulder

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., 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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Please contact us with concerns about any potential bias at www.pearson.com/report-bias.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

About the Contributing Authors

Rick Graziani teaches computer science and computer networking at Cabrillo College and the University of California, Santa Cruz. Rick is best known for authoring the Cisco Press book *IPv6 Fundamentals*. Prior to teaching, Rick worked in the information technology field for Santa Cruz Operation, Tandem Computers, and Lockheed Missiles and Space Company, and served in the U.S. Coast Guard. He holds an MA in Computer Science and Systems Theory from California State University, Monterey Bay. Rick also works as a curriculum developer for the Cisco Networking Academy Curriculum Engineering team. When Rick is not working, he is most likely surfing at one of his favorite Santa Cruz surf breaks.

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an MEd in training and development. He taught CCNA courses at the high school level for seven years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team providing services to Networking Academy instructors worldwide and creating training materials. He now splits his time between working as a Curriculum Lead for Cisco Networking Academy and as Account Lead for Unicon (unicon.net) supporting Cisco's educational efforts.

Contents at a Glance

Introduction xlii

Chapter 1 Communications in a Connected World 1

Chapter 2 Network Components, Types, and Connections 25

Chapter 3 Wireless and Mobile Networks 41

Chapter 4 Build a Home Network 57

Chapter 5 Communication Principles 75

Chapter 6 Network Media 91

Chapter 7 The Access Layer 101

Chapter 8 The Internet Protocol 117

Chapter 9 IPv4 and Network Segmentation 125

Chapter 10 IPv6 Addressing Formats and Rules 147

Chapter 11 Dynamic Addressing with DHCP 163

Chapter 12 Gateways to Other Networks 175

Chapter 13 The ARP Process 185

Chapter 14 Routing Between Networks 199

Chapter 15 TCP and UDP 215

Chapter 16 Application Layer Services 229

Chapter 17 Network Testing Utilities 253

Chapter 18 Network Design 265

Chapter 19 Cloud and Virtualization 281

Chapter 20 Number Systems 293

Chapter 21 Ethernet Switching 315

Chapter 22 Network Layer 343

Chapter 23 IPv4 Address Structure 363

Chapter 24 Address Resolution 375

Chapter 25 IP Addressing Services 391

Chapter 26 Transport Layer 407

Chapter 27 The Cisco IOS Command Line 455

Chapter 28 Build a Small Cisco Network 475

Chapter 29 ICMP 499

Chapter 30 Physical Layer 519

Chapter 31 Data Link Layer 555

Chapter 32 Routing at the Network Layer 571

Chapter 33 IPv6 Addressing 587

Chapter 34 IPv6 Neighbor Discovery 621

Chapter 35 Cisco Switches and Routers 629

Chapter 36 Troubleshoot Common Network Problems 659

Chapter 37 Network Support 697

Chapter 38 Cybersecurity Threats, Vulnerabilities, and Attacks 775

Chapter 39 Network Security 813

Appendix A Answers to the “Check Your Understanding” Questions 875

Index 905

Online Element

Glossary

Contents

Introduction xlii

Chapter 1 Communications in a Connected World 1

Objectives 1

Key Terms 1

Introduction (1.0) 2

Network Types (1.1) 2

Everything Is Online (1.1.2) 2

Who Owns "The Internet"? (1.1.3) 2

Local Networks (1.1.4) 3

Small Home Networks 4
Small Office and Home Office Networks 4
Medium to Large Networks 4
Worldwide Networks 6

Mobile Devices (1.1.5) 6

Smartphone 6
Tablet 7
Smartwatch 8
Smart Glasses 8

Connected Home Devices (1.1.6) 8

Security System 8
Appliances 9
Smart TV 10
Gaming Console 11

Other Connected Devices (1.1.7) 11

Smart Cars 11
RFID Tags 12
Sensors and Actuators 13
Medical Devices 13

Data Transmission (1.2) 14

The Bit (1.2.2) 14

Common Methods of Data Transmission (1.2.3) 15

Bandwidth and Throughput (1.3) 17

Bandwidth (1.3.1) 17

Throughput (1.3.2) 18

Communications in a Connected World Summary (1.4) 18

What Did I Learn in This Chapter? (1.4.1) 19

Reflection Questions (1.4.2) 20

Practice 21

Check Your Understanding Questions 21

Chapter 2 Network Components, Types, and Connections 25

Objectives 25

Key Terms 25

Introduction (2.0) 26

Clients and Servers (2.1) 26

Client and Server Roles (2.1.2) 26

Peer-to-Peer Networks (2.1.3) 27

Peer-to-Peer Applications (2.1.4) 28

Multiple Roles in the Network (2.1.5) 29

Network Components (2.2) 30

Network Infrastructure (2.2.2) 30

End Devices (2.2.3) 32

ISP Connectivity Options (2.3) 33

ISP Services (2.3.1) 33

ISP Connections (2.3.2) 34

Cable and DSL Connections (2.3.3) 35

Additional Connectivity Options (2.3.4) 36

Network Components, Types, and Connections Summary (2.4) 37

What Did I Learn in This Chapter? (2.4.1) 37

Reflection Questions (2.4.2) 38

Practice 39

Check Your Understanding Questions 39

Chapter 3 Wireless and Mobile Networks 41

Objectives 41

Key Terms 41

Introduction (3.0) 42

Wireless Networks (3.1) 42

Other Wireless Networks (3.1.3) 43

Global Positioning System 43

Wi-Fi 43

Bluetooth 43

NFC 43

Mobile Device Connectivity (3.2) 44

Mobile Devices and Wi-Fi (3.2.1) 44

Wi-Fi Settings (3.2.2) 44

Configure Mobile Wi-Fi Connectivity (3.2.3) 46

Configure Cellular Data Settings (3.2.4) 47

Android Cellular Data 47

iOS Cellular Data 48

Simple Connectivity with Bluetooth (3.2.6) 49

Bluetooth Pairing (3.2.7) 50

Explore Your Network Settings on Your Mobile Device (3.2.8) 51

Wireless and Mobile Networks Summary (3.3) 52

What Did I Learn in This Chapter? (3.3.1) 52

Reflection Questions (3.3.2) 53

Practice 54

Check Your Understanding Questions 54

Chapter 4 Build a Home Network 57

Objectives 57

Key Terms 57

Introduction (4.0) 58

Home Network Basics (4.1) 58

Components of a Home Network (4.1.2) 58

Typical Home Network Routers (4.1.3) 59

Network Technologies in the Home (4.2) 60

LAN Wireless Frequencies (4.2.1) 61

Wired Network Technologies (4.2.2) 62

Category 5e Cable 62

Coaxial Cable 62

Fiber-Optic Cable 63

Wireless Standards (4.3) 63

Wi-Fi Networks (4.3.1) 64

Wireless Settings (4.3.2) 64

Network Mode 65

Set Up a Home Router (4.4) 66

First Time Setup (4.4.1) 66

Design Considerations (4.4.2) 67

Build a Home Network Summary (4.5) 69

What Did I Learn in This Chapter? (4.5.1) 69

Reflection Questions (4.5.2) 71

Practice 72

Packet Tracer Activities 72

Check Your Understanding Questions 72

Chapter 5 Communication Principles 75

Objectives 75

Key Terms 75

Introduction (5.0) 76

Networking Protocols (5.1) 76

Communication Protocols (5.1.1) 76

Why Protocols Matter (5.1.2) 78

Communication Standards (5.2) 80

The Internet and Standards (5.2.2) 80

Network Standards Organizations (5.2.3) 80

Network Communication Models (5.3) 81

The TCP/IP Model (5.3.3) 81

The OSI Reference Model (5.3.4) 82

OSI Model and TCP/IP Model Comparison (5.3.5) 83

Communication Principles Summary (5.4) 85

What Did I Learn in This Chapter? (5.4.1) 85

Reflection Questions (5.4.2) 87

Practice 88

Check Your Understanding Questions 88

Chapter 6 Network Media 91

Objectives 91

Key Terms 91

Introduction (6.0) 92

Network Media Types (6.1) 92

Three Media Types (6.1.2) 92

Common Network Cables (6.1.3) 93

Twisted-Pair Cable 93

Coaxial Cable 94
Fiber-Optic Cable 95

Network Media Summary (6.2) 95

What Did I Learn in This Chapter? (6.2.1) 95

Reflection Questions (6.2.2) 96

Practice 97

Check Your Understanding Questions 97

Chapter 7 The Access Layer 101

Objectives 101

Key Terms 101

Introduction (7.0) 102

Encapsulation and the Ethernet Frame (7.1) 102

Encapsulation (7.1.2) 102

The Access Layer (7.2) 104

Ethernet Frame (7.2.1) 104

Access Layer Devices (7.2.2) 105

Ethernet Hubs (7.2.3) 106

Ethernet Switches (7.2.4) 107

The MAC Address Table (7.2.5) 109

The Access Layer Summary (7.3) 111

What Did I Learn in This Chapter? (7.3.1) 111

Reflection Questions (7.3.2) 113

Practice 114

Check Your Understanding Questions 114

Chapter 8 The Internet Protocol 117

Objectives 117

Introduction (8.0) 118

Purpose of an IPv4 Address (8.1) 118

The IPv4 Address (8.1.1) 118

Octets and Dotted-Decimal Notation (8.1.2) 119

The IPv4 Address Structure (8.2) 119

Networks and Hosts (8.2.2) 119

Summary (8.3) 121

What Did I Learn in This Chapter? (8.3.1) 121

Reflection Questions (8.3.2) 121

Practice 122

Packet Tracer Activities 122

Check Your Understanding Questions 122

Chapter 9 IPv4 and Network Segmentation 125

Objectives 125

Key Terms 125

Introduction (9.0) 126

IPv4 Unicast, Broadcast, and Multicast (9.1) 126

Unicast (9.1.2) 126

Broadcast (9.1.4) 127

Multicast (9.1.6) 129

Types of IPv4 Addresses (9.2) 130

Public and Private IPv4 Addresses (9.2.1) 130

Routing to the Internet (9.2.2) 131

Special-Use IPv4 Addresses (9.2.4) 132

Loopback Addresses 132

Link-Local addresses 133

Legacy Classful Addressing (9.2.5) 133

Assignment of IP Addresses (9.2.6) 134

Network Segmentation (9.3) 135

Broadcast Domains and Segmentation (9.3.2) 136

Problems with Large Broadcast Domains (9.3.3) 137

Reasons for Segmenting Networks (9.3.4) 138

IPv4 and Network Segmentation Summary (9.4) 140

What Did I Learn in This Chapter? (9.4.1) 140

Reflection Questions (9.4.2) 143

Practice 144

Check Your Understanding Questions 144

Chapter 10 IPv6 Addressing Formats and Rules 147

Objectives 147

Key Terms 147

Introduction (10.0) 148

IPv4 Issues (10.1) 148

The Need for IPv6 (10.1.1) 148

Internet of Things 149

IPv4 and IPv6 Coexistence (10.1.2) 150

Dual Stack 150

Tunneling 150

Translation 151

IPv6 Addressing (10.2) 152

Hexadecimal Number System (10.2.1) 152

IPv6 Addressing Formats (10.2.2) 152

Preferred Format 153

Rule 1—Omit Leading Zeros (10.2.4) 153

Rule 2—Double Colon (10.2.5) 155

IPv6 Addressing Formats and Rules Summary (10.3) 156

What Did I Learn in This Chapter? (10.3.1) 157

Reflection Questions (10.3.2) 158

Practice 159

Check Your Understanding Questions 159

Chapter 11 Dynamic Addressing with DHCP 163

Objectives 163

Key Term 163

Introduction (11.0) 164

Static and Dynamic Addressing (11.1) 164

Static IPv4 Address Assignment (11.1.1) 164

Dynamic IPv4 Address Assignment (11.1.2) 165

DHCP Servers (11.1.3) 166

DHCPv4 Configuration (11.2) 167

DHCPv4 Operation (11.2.1) 168

DHCP Service Configuration (11.2.3) 169

Dynamic Addressing with DHCP Summary (11.3) 170

What Did I Learn in This Chapter? (11.3.1) 170

Reflection Questions (11.3.2) 171

Practice 172

Packet Tracer Activities 172

Check Your Understanding Questions 172

Chapter 12 Gateways to Other Networks 175

Objectives 175

Key Term 175

Introduction (12.0) 176

Network Boundaries (12.1) 176

Routers as Gateways (12.1.2) 176

Routers as Boundaries Between Networks (12.1.3) 177

Network Address Translation (12.2) 178

NAT Operation (12.2.1) 179

Gateways to Other Networks Summary (12.3) 180

What Did I Learn in This Chapter? (12.3.1) 180

Reflection Questions (12.3.2) 181

Practice 182

Packet Tracer Activities 182

Check Your Understanding Questions 182

Chapter 13 The ARP Process 185

Objectives 185

Key Term 185

Introduction (13.0) 186

MAC and IP (13.1) 186

Destination on Same Network (13.1.1) 186

Destination on Remote Network (13.1.2) 187

Broadcast Containment (13.2) 189

Broadcast Domains (13.2.2) 190

Access Layer Communication (13.2.3) 191

ARP (13.2.5) 192

The ARP Process Summary (13.3) 193

What Did I Learn in This Chapter? (13.3.1) 193

Reflection Questions (13.3.2) 194

Practice 195

Packet Tracer Activities 195

Check Your Understanding Questions 195

Chapter 14 Routing Between Networks 199

Objectives 199

Key Terms 199

Introduction (14.0) 200

The Need for Routing (14.1) 200

Now We Need Routing (14.1.2) 200

The Routing Table (14.2) 201

Routing Table Entries (14.2.4) 202

The Default Gateway (14.2.5) 203

Create a LAN (14.3) 204

Local Area Networks (14.3.1) 205

Local and Remote Network Segments (14.3.2) 205

All Hosts in One Local Segment 206

Hosts on a Remote Segment 206

Routing Between Networks Summary (14.4) 208

What Did I Learn in This Chapter? (14.4.1) 208

Reflection Questions (14.4.2) 210

Practice 211

Packet Tracer Activities 211

Check Your Understanding Questions 211

Chapter 15 TCP and UDP 215

Objectives 215

Key Terms 215

Introduction (15.0) 216

TCP and UDP (15.1) 216

Protocol Operations (15.1.1) 216

TCP and UDP (15.1.2) 217

TCP Reliability (15.1.3) 218

UDP Best Effort Delivery (15.1.4) 218

Port Numbers (15.2) 219

TCP and UDP Port Numbers (15.2.1) 219

Socket Pairs (15.2.2) 222

The **netstat** Command (15.2.3) 223

TCP and UDP Summary (15.3) 224

What Did I Learn in This Chapter? (15.3.1) 224
Reflection Questions (15.3.2) 225
Practice 226
Check Your Understanding Questions 226
Chapter 16 Application Layer Services 229
Objectives 229
Key Terms 229
Introduction (16.0) 230
The Client-Server Relationship (16.1) 230
Client and Server Interaction (16.1.1) 230
Client Requests a Web Page (16.1.2) 231
URI, URN, and URL (16.1.3) 232
Network Application Services (16.2) 233
Common Network Application Services (16.2.1) 233
Domain Name System (16.3) 234
Domain Name Translation (16.3.1) 234
DNS Servers (16.3.2) 235
A Note About Syntax Checker Activities (16.3.3) 236
Web Clients and Servers (16.4) 236
HTTP and HTML (16.4.2) 237
FTP Clients and Servers (16.5) 238
File Transfer Protocol (16.5.1) 238
Virtual Terminals (16.6) 239
Telnet (16.6.2) 240
Security Issues with Telnet (16.6.3) 241
Email and Messaging (16.7) 242
Email Clients and Servers (16.7.1) 242
Email Protocols (16.7.2) 242
Simple Mail Transfer Protocol (SMTP) 243
Post Office Protocol (POP3) 243
Internet Message Access Protocol (IMAP4) 243
Text Messaging (16.7.3) 244
Internet Phone Calls (16.7.4) 245
Application Layer Services Summary (16.8) 245

What Did I Learn in This Chapter? (16.8.1) 245
Reflection Questions (16.8.2) 248
Practice 249
Packet Tracer Activities 249
Check Your Understanding Questions 249

Chapter 17 Network Testing Utilities 253
Objectives 253
Key Terms 253
Introduction (17.0) 254
Troubleshooting Commands (17.1) 254
Overview of Troubleshooting Commands (17.1.1) 254
The **ipconfig** Command (17.1.2) 254
The **ping** Command (17.1.4) 258
Ping Results (17.1.5) 259
Network Testing Utilities Summary (17.2) 260
What Did I Learn in This Chapter? (17.2.1) 260
Reflection Questions (17.2.2) 261
Practice 262
Packet Tracer Activities 262
Check Your Understanding Questions 262

Chapter 18 Network Design 265
Objectives 265
Key Terms 265
Introduction (18.0) 266
Reliable Networks (18.1) 266
Network Architecture (18.1.1) 266
Fault Tolerance (18.1.3) 267
Scalability (18.1.4) 267
Quality of Service (18.1.5) 269
Network Security (18.1.6) 270
Hierarchical Network Design (18.2) 271
Physical and Logical Addresses (18.2.1) 271
Hierarchical Analogy (18.2.4) 272

Access, Distribution, and Core (18.2.6) 273

Access Layer 273
Distribution Layer 274
Core Layer 274

Network Design Summary (18.3) 275

What Did I Learn in This Chapter? (18.3.1) 275

Reflection Questions (18.3.2) 276

Practice 277

Labs 277

Check Your Understanding Questions 277

Chapter 19 Cloud and Virtualization 281

Objectives 281

Key Terms 281

Introduction (19.0) 282

Cloud and Cloud Services (19.1) 282

Types of Clouds (19.1.2) 282

Cloud Services (19.1.3) 283

Cloud Computing and Virtualization (19.1.4) 284

Virtualization (19.2) 285

Advantages of Virtualization (19.2.1) 285

Hypervisors (19.2.2) 286

Type 1 Hypervisor—"Bare Metal" Approach 286
Type 2 Hypervisor—"Hosted" Approach 286

Cloud and Virtualization Summary (19.3) 287

What Did I Learn in This Chapter? (19.3.1) 287

Reflection Questions (19.3.2) 289

Practice 290

Labs 290

Check Your Understanding Questions 290

Chapter 20 Number Systems 293

Objectives 293

Key Terms 293

Introduction (20.0) 294

Binary Number System (20.1) 294

Binary and IPv4 Addresses (20.1.1) 294

Decimal to Binary Conversion (20.1.5) 296

Decimal to Binary Conversion Example (20.1.6) 300

IPv4 Addresses (20.1.9) 307

Hexadecimal Number System (20.2) 308

Hexadecimal and IPv6 Addresses (20.2.1) 308

Number Systems Summary (20.3) 311

What Did I Learn in This Chapter? (20.3.1) 311

Reflection Questions (20.3.2) 311

Practice 312

Check Your Understanding Questions 312

Chapter 21 Ethernet Switching 315

Objectives 315

Key Terms 315

Introduction (21.0) 316

Ethernet (21.1) 316

The Rise of Ethernet (21.1.1) 316

Ethernet Evolution (21.1.2) 317

Ethernet Frames (21.2) 318

Ethernet Encapsulation (21.2.1) 318

Data Link Sublayers (21.2.2) 319

MAC Sublayer (21.2.3) 320

Data Encapsulation 321

Accessing the Media 321

Ethernet Frame Fields (21.2.4) 322

Ethernet MAC Address (21.3) 324

MAC Address and Hexadecimal (21.3.1) 324

Unicast MAC Address (21.3.2) 326

Broadcast MAC Address (21.3.3) 327

Multicast MAC Address (21.3.4) 328

The MAC Address Table (21.4) 330

Switch Fundamentals (21.4.1) 330

Switch Learning and Forwarding (21.4.2) 331

Examine the Source MAC Address 331

Find the Destination MAC Address 332

Filtering Frames (21.4.3) 333

Ethernet Switching Summary (21.5) 336

What Did I Learn in This Chapter? (21.5.1) 336

Reflection Questions (21.5.2) 338

Practice 339

Labs 339

Check Your Understanding Questions 339

Chapter 22 Network Layer 343

Objectives 343

Key Terms 343

Introduction (22.0) 344

Network Layer Characteristics (22.1) 344

The Network Layer (22.1.2) 344

IP Encapsulation (22.1.3) 346

Characteristics of IP (22.1.4) 347

Connectionless (22.1.5) 347

Best Effort (22.1.6) 348

Media Independent (22.1.7) 349

IPv4 Packet (22.2) 350

IPv4 Packet Header (22.2.1) 350

IPv4 Packet Header Fields (22.2.2) 350

IPv6 Packet (22.3) 352

Limitations of IPv4 (22.3.1) 352

IPv6 Overview (22.3.2) 353

IPv4 Packet Header Fields in the IPv6 Packet Header (22.3.3) 354

IPv6 Packet Header (22.3.4) 356

Network Layer Summary (22.4) 357

What Did I Learn in This Chapter? (22.4.1) 357

Reflection Questions (22.4.2) 358

Practice 359

Check Your Understanding Questions 359

Chapter 23 IPv4 Address Structure 363

Objectives 363

Key Terms 363

Introduction (23.0) 364

IPv4 Address Structure (23.1) 364

Network and Host Portions (23.1.1) 364

The Subnet Mask (23.1.2) 365

The Prefix Length (23.1.3) 366

Determining the Network: Logical AND (23.1.4) 367

IPv4 Address Structure Summary (23.2) 369

What Did I Learn in This Chapter? (23.2.1) 369

Reflection Questions (23.2.2) 370

Practice 371

Check Your Understanding Questions 371

Chapter 24 Address Resolution 375

Objectives 375

Key Terms 375

Introduction (24.0) 376

ARP (24.1) 376

ARP Overview (24.1.1) 376

ARP Functions (24.1.2) 377

Removing Entries from an ARP Table (24.1.6) 380

ARP Tables on Devices (24.1.7) 381

ARP Issues—ARP Broadcasts and ARP Spoofing (24.1.8) 382

Address Resolution Summary (24.2) 384

What Did I Learn in This Chapter? (24.2.1) 384

Reflection Questions (24.2.2) 385

Practice 386

Labs 386

Packet Tracer Activities 386

Check Your Understanding Questions 386

Chapter 25 IP Addressing Services 391

Objectives 391

Key Terms 391

Introduction (25.0) 392

DNS Services (25.1) 392

Domain Name System (25.1.2) 392

DNS Message Format (25.1.3) 395

DNS Hierarchy (25.1.4) 395

The **nslookup** Command (25.1.5) 397

DHCP Services (25.2) 398

Dynamic Host Configuration Protocol (25.2.1) 398

DHCP Messages (25.2.3) 399

IP Addressing Services Summary (25.3) 401

What Did I Learn in This Chapter? (25.3.1) 401

Reflection Questions (25.3.2) 402

Practice 403

Labs 403

Check Your Understanding Questions 403

Chapter 26 Transport Layer 407

Objectives 407

Key Terms 407

Introduction (26.0) 408

Transportation of Data (26.1) 408

Role of the Transport Layer (26.1.1) 408

Transport Layer Responsibilities (26.1.2) 409

Transport Layer Protocols (26.1.3) 413

Transmission Control Protocol (TCP) (26.1.4) 413

User Datagram Protocol (UDP) (26.1.5) 414

The Right Transport Layer Protocol for the Right Application (26.1.6) 415

TCP Overview (26.2) 417

TCP Features (26.2.1) 417

TCP Header (26.2.2) 418

TCP Header Fields (26.2.3) 418

Applications That Use TCP (26.2.4) 419

UDP Overview (26.3) 420

UDP Features (26.3.1) 420

UDP Header (26.3.2) 420

UDP Header Fields (26.3.3) 421

Applications That Use UDP (26.3.4) 421

Port Numbers (26.4) 422

Multiple Separate Communications (26.4.1) 422

Socket Pairs (26.4.2) 423

Port Number Groups (26.4.3) 424

The **netstat** Command (26.4.4) 426

TCP Communication Process (26.5) 427

TCP Server Processes (26.5.1) 427

TCP Connection Establishment (26.5.2) 430

Session Termination (26.5.3) 431

TCP Three-Way Handshake Analysis (26.5.4) 432

Reliability and Flow Control (26.6) 433

TCP Reliability—Guaranteed and Ordered Delivery (26.6.1) 433

TCP Reliability—Data Loss and Retransmission (26.6.3) 435

TCP Flow Control—Window Size and Acknowledgments (26.6.5) 437

TCP Flow Control—Maximum Segment Size (MSS) (26.6.6) 439

TCP Flow Control—Congestion Avoidance (26.6.7) 440

UDP Communication (26.7) 441

UDP Low Overhead Versus Reliability (26.7.1) 441

UDP Datagram Reassembly (26.7.2) 441

UDP Server Processes and Requests (26.7.3) 443

UDP Client Processes (26.7.4) 443

Transport Layer Summary (26.8) 447

What Did I Learn in This Chapter? (26.8.2) 447

Reflection Questions (26.8.3) 449

Practice 450

Packet Tracer Activities 450

Check Your Understanding Questions 450

Chapter 27 The Cisco IOS Command Line 455

Objectives 455

Key Terms 455

Introduction (27.0) 456

Navigate the IOS (27.1) 456

The Cisco IOS Command-Line Interface (27.1.1) 456

Primary Command Modes (27.1.2) 457

A Note About Syntax Checker Activities (27.1.5) 458

The Command Structure (27.2) 458

Basic IOS Command Structure (27.2.1) 458

IOS Command Syntax (27.2.2) 459

Hotkeys and Shortcuts (27.2.4) 460

View Device Information (27.3) 462

show Commands (27.3.2) 463

The Cisco IOS Command Line Summary (27.4) 469

What Did I Learn in This Chapter? (27.4.1) 469

Reflection Questions (27.4.2) 471

Practice 472

Packet Tracer Activities 472

Check Your Understanding Questions 472

Chapter 28 Build a Small Cisco Network 475

Objectives 475

Key Term 475

Introduction (28.0) 476

Basic Switch Configuration (28.1) 476

Basic Switch Configuration Steps (28.1.1) 476

Switch Virtual Interface Configuration (28.1.2) 478

Configure Initial Router Settings (28.2) 479

Basic Router Configuration Steps (28.2.1) 479

Basic Router Configuration Example (28.2.2) 480

Secure the Devices (28.3) 482

Password Recommendations (28.3.1) 482

Secure Remote Access (28.3.2) 483

Enable SSH (28.3.3) 485

Verify SSH (28.3.5) 487

Connecting the Switch to the Router (28.4) 488

Default Gateway for a Host (28.4.1) 488

Default Gateway on a Switch (28.4.2) 490

Build a Small Cisco Network Summary (28.5) 492

What Did I Learn in This Chapter? (28.5.1) 492

Reflection Questions (28.5.2) 495

Practice 496

Packet Tracer Activities 496

Check Your Understanding Questions 496

Chapter 29 ICMP 499

Objectives 499

Introduction (29.0) 500

ICMP Messages (29.1) 500

ICMPv4 and ICMPv6 Messages (29.1.1) 500

Host Reachability (29.1.2) 500

Destination or Service Unreachable (29.1.3) 501

Time Exceeded (29.1.4) 502

ICMPv6 Messages (29.1.5) 502

Ping and Traceroute Tests (29.2) 505

Ping—Test Connectivity (29.2.1) 505

Ping the Local Loopback (29.2.2) 506

Ping the Default Gateway (29.2.3) 507

Ping a Remote Host (29.2.4) 508

Traceroute—Test the Path (29.2.5) 509

Round-Trip Time (RTT) 509

IPv4 TTL and IPv6 Hop Limit 509

ICMP Summary (29.3) 511

What Did I Learn in This Chapter? (29.3.2) 511

Reflection Questions (29.3.3) 513

Practice 514

Packet Tracer Activities 514

Check Your Understanding Questions 514

Chapter 30 **Physical Layer 519**

Objectives 519

Key Terms 519

Introduction (30.0) 520

Purpose of the Physical Layer (30.1) 520

The Physical Connection (30.1.1) 520

The Physical Layer Process (30.1.2) 522

Physical Layer Characteristics (30.2) 523

Physical Layer Standards (30.2.1) 523

Physical Components (30.2.2) 525

Encoding (30.2.3) 525

Signaling (30.2.4) 525

Bandwidth (30.2.6) 527

Bandwidth Terminology (30.2.7) 528

Latency 528
Throughput 529
Goodput 529

Copper Cabling (30.3) 529

Characteristics of Copper Cabling (30.3.1) 529

Types of Copper Cabling (30.3.2) 531

Unshielded Twisted-Pair (UTP) (30.3.3) 531

Shielded Twisted-Pair (STP) (30.3.4) 533

Coaxial Cable (30.3.5) 533

UTP Cabling (30.4) 535

Properties of UTP Cabling (30.4.1) 535

UTP Cabling Standards and Connectors (30.4.2) 536

Straight-Through and Crossover UTP Cables (30.4.3) 539

Fiber-Optic Cabling (30.5) 541

Properties of Fiber-Optic Cabling (30.5.1) 541

Types of Fiber Media (30.5.2) 541

Single-Mode Fiber 541
Multimode Fiber 542
Fiber-Optic Cabling Usage (30.5.3) 543

Fiber-Optic Connectors (30.5.4) 543

Fiber Patch Cords (30.5.5) 545

Fiber Versus Copper (30.5.6) 547

Summary (30.6) 548

What Did I Learn in This Chapter? (30.6.1) 548

Reflection Questions (30.6.2) 550

Practice 551

Check Your Understanding Questions 551

Chapter 31 Data Link Layer 555

Objectives 555

Key Terms 555

Introduction (31.0) 556

Topologies (31.1) 556

Physical and Logical Topologies (31.1.1) 556

WAN Topologies (31.1.2) 558

Point-to-Point 558

Hub and Spoke 558

Mesh 559

Point-to-Point WAN Topology (31.1.4) 559

LAN Topologies (31.1.5) 560

Legacy LAN Topologies 560

Media Access Control Methods (31.2) 561

Half- and Full-Duplex Communication (31.2.1) 562

Half-Duplex Communication 562

Full-Duplex Communication 562

Access Control Methods (31.2.2) 563

Contention-Based Access 563

Controlled Access 564

Contention-Based Access—CSMA/CD (31.2.3) 564

Contention-Based Access—CSMA/CA (31.2.4) 566

Summary (31.3) 568

What Did I Learn in This Chapter? (31.3.1) 568

Reflection Questions (31.3.2) 568

Practice 569

Check Your Understanding Questions 569

Chapter 32 Routing at the Network Layer 571

Objectives 571

Key Terms 571

Introduction (32.0) 572

How a Host Routes (32.1) 572
Host Forwarding Decision (32.1.1) 572
Default Gateway (32.1.2) 574
A Host Routes to the Default Gateway (32.1.3) 574
Host Routing Tables (32.1.4) 575
Routing Tables (32.2) 576
Router Packet Forwarding Decision (32.2.1) 576
IP Router Routing Table (32.2.2) 577
Static Routing (32.2.3) 579
Dynamic Routing (32.2.4) 580
Introduction to an IPv4 Routing Table (32.2.6) 582
Summary (32.3) 582
What Did I Learn in This Chapter? (32.3.1) 582
Reflection Questions (32.3.2) 583
Practice 584
Check Your Understanding Questions 584
Chapter 33 IPv6 Addressing 587
Objectives 587
Key Terms 587
Introduction (33.0) 588
IPv6 Address Types (33.1) 588
Unicast, Multicast, Anycast (33.1.1) 588
IPv6 Prefix Length (33.1.2) 588
Types of IPv6 Unicast Addresses (33.1.3) 589
A Note About the Unique Local Address (33.1.4) 590
IPv6 GUA (33.1.5) 591
IPv6 GUA Structure (33.1.6) 592
Global Routing Prefix 592
Subnet ID 592
Interface ID 593
IPv6 LLA (33.1.7) 593
GUA and LLA Static Configuration (33.2) 595
Static GUA Configuration on a Router (33.2.1) 595
Static GUA Configuration on a Windows Host (33.2.2) 596
Static Configuration of a Link-Local Unicast Address (33.2.3) 598

Dynamic Addressing for IPv6 GUAs (33.3) 599

RS and RA Messages (33.3.1) 599

Method 1: SLAAC (33.3.2) 601

Method 2: SLAAC and Stateless DHCPv6 (33.3.3) 602

Method 3: Stateful DHCPv6 (33.3.4) 603

EUI-64 Process vs. Randomly Generated (33.3.5) 604

EUI-64 Process (33.3.6) 605

Randomly Generated Interface IDs (33.3.7) 606

Dynamic Addressing for IPv6 LLAs (33.4) 607

Dynamic LLAs (33.4.1) 607

Dynamic LLAs on Windows (33.4.2) 608

Dynamic LLAs on Cisco Routers (33.4.3) 609

Verify IPv6 Address Configuration (33.4.4) 609

IPv6 Multicast Addresses (33.5) 612

Assigned IPv6 Multicast Addresses (33.5.1) 612

Well-Known IPv6 Multicast Addresses (33.5.2) 613

Solicited-Node IPv6 Multicast Addresses (33.5.3) 614

Summary (33.6) 615

What Did I Learn in This Chapter? (33.6.1) 615

Reflection Questions (33.6.2) 616

Practice 617

Packet Tracer Activities 617

Check Your Understanding Questions 617

Chapter 34 IPv6 Neighbor Discovery 621

Objectives 621

Key Terms 621

Introduction (34.0) 622

Neighbor Discovery Operation (34.1) 622

IPv6 Neighbor Discovery Messages (34.1.2) 622

IPv6 Neighbor Discovery—Address Resolution (34.1.3) 623

Summary (34.2) 625

What Did I Learn in This Chapter? (34.2.1) 625

Practice 626

Packet Tracer Activities 626

Check Your Understanding Questions 626

Chapter 35 Cisco Switches and Routers 629

Objectives 629

Key Terms 629

Introduction (35.0) 630

Cisco Switches (35.1) 630

Connect More Devices (35.1.1) 630

Cisco LAN Switches (35.1.2) 631

Type of Ports 632
Speed Required 632
Expandability 633
Manageability 633

LAN Switch Components (35.1.5) 634

Switch Speeds and Forwarding Methods (35.2) 635

Frame Forwarding Methods on Cisco Switches (35.2.1) 635

Cut-Through Switching (35.2.2) 636

Memory Buffering on Switches (35.2.3) 638

Duplex and Speed Settings (35.2.4) 638

Auto-MDIX (35.2.5) 640

Switch Boot Process (35.3) 641

Power Up the Switch (35.3.1) 642

In-Band and Out-of-Band Management (35.3.3) 644

Out-of-Band Management 644
In-Band Management 644

IOS Startup Files (35.3.4) 645

Cisco Routers (35.4) 646

Router Components (35.4.2) 646

Router Interface Ports (35.4.3) 647

Router Boot Process (35.5) 648

Power Up the Router (35.5.1) 648

Management Ports (35.5.2) 651

Summary (35.6) 653

What Did I Learn in This Chapter? (35.6.1) 653

Reflection Questions (35.6.2) 654

Practice 655

Check Your Understanding Questions 655

Chapter 36 Troubleshoot Common Network Problems 659

Objectives 659

Introduction (36.0) 660

The Troubleshooting Process (36.1) 660

Network Troubleshooting Overview (36.1.2) 660

Gather Information (36.1.3) 660

Structured Troubleshooting Methods (36.1.4) 662

Bottom-Up 662

Top-Down 663

Divide-and-Conquer 664

Follow-the-Path 664

Substitution 665

Comparison 665

Educated Guess 665

Guidelines for Selecting a Troubleshooting Method (36.1.5) 665

Physical Layer Problems (36.2) 667

Common Layer 1 Problems (36.2.1) 667

The Sense of Sight 667

The Senses of Smell and Taste 668

The Sense of Touch 668

The Sense of Hearing 668

Wireless Router LEDs (36.2.2) 668

Cabling Problems (36.2.3) 670

Troubleshoot Wireless Issues (36.3) 671

Causes of Wireless Issues (36.3.1) 671

Authentication and Association Errors (36.3.2) 672

Common Internet Connectivity Issues (36.4) 674

DHCP Server Configuration Errors (36.4.1) 674

Check Internet Configuration (36.4.2) 674

Check Firewall Settings (36.4.3) 677

Divide and Conquer with ping (36.4.5) 678

The **tracert** Command (36.4.6) 678

The **netstat** Command (36.4.7) 680

The **nslookup** Command (36.4.8) 682

Customer Support (36.5) 683

Sources of Help (36.5.1) 683

When to Call for Help (36.5.2) 684

Support Desk Interaction (36.5.3) 685

Issue Resolution (36.5.4) 686

Support Desk Tickets and Work Orders (36.5.5) 686

Troubleshoot Common Network Problems Summary (36.6) 688

What Did I Learn in This Chapter? (36.6.1) 688

Practice 692

Packet Tracer Activities 692

Check Your Understanding Questions 692

Chapter 37 Network Support 697

Objectives 697

Key Terms 697

Introduction (37.0) 698

Diagnostics and Troubleshooting Methodologies (37.1) 698

Troubleshooting Process Review (37.1.1) 698

Seven-Step Troubleshooting Process (37.1.2) 699

Define the Problem 699
Gather Information 700
Analyze Information 700
Eliminate Possible Causes 700
Propose Hypothesis 700
Test Hypothesis 700
Solve the Problem 700

Troubleshooting with Layered Models (37.1.3) 701

Structured Troubleshooting Methods (37.1.4) 701

Guidelines for Selecting a Troubleshooting Method (37.1.5) 702

Document Findings, Actions, and Outcomes (37.1.6) 703

Network Documentation (37.2) 704

Documentation Overview (37.2.1) 704

Network Topologies and Descriptions (37.2.2) 704

PAN 704
LAN 705
VLAN 706
WLAN 706
WMN 707
CAN 708
MAN 708
WAN 709
VPN 710

Enterprise Network Topologies (37.2.4) 710

Network Cloud Services and Applications (37.2.5) 713

SaaS (Software as a Service) 713

PaaS (Platform as a Service) 713

IaaS (Infrastructure as a Service) 714

XaaS (Anything/Everything as a Service) 714

Wireless Standards (37.2.6) 714

Licensed and Unlicensed Bands 716

Network Device Documentation (37.2.8) 717

Router Device Documentation 717

LAN Switch Device Documentation 717

End-System Documentation 718

Establish a Network Baseline (37.2.9) 718

Cisco Discovery Protocol (CDP) Overview (37.2.10) 719

Discover Devices Using CDP (37.2.11) 720

Help Desks (37.3) 723

The Security Policy (37.3.1) 723

Help Desks (37.3.2) 725

Ticketing Systems (37.3.3) 727

Question End Users (37.3.4) 729

Active Listening (37.3.6) 731

Gather Information for Host-Related Tickets (37.3.8) 733

Beep Codes 733

BIOS Information 733

Event Viewer 733

Device Manager 734

Task Manager 735

Diagnostic Tools 736

Gather Information for Cisco Device-Related Tickets (37.3.9) 736

Analyze the Information (37.3.10) 737

Troubleshoot Endpoint Connectivity (37.4) 738

Windows Network Setup (37.4.1) 738

Verify Connectivity in Windows (37.4.2) 740

Linux Network Setup (37.4.3) 741

Verify Connectivity in Linux (37.4.4) 742

macOS Network Setup (37.4.5) 743

Verify Connectivity in macOS (37.4.6) 744

Set Up and Verify Networking in iOS (37.4.7) 746

Set Up and Verify Networking in Android (37.4.8) 747

Troubleshoot a Network (37.5) 750

Network Devices as Sources of Network Information (37.5.1) 750

Packet Capture and Protocol Analysis (37.5.2) 752

Measuring Network Throughput (37.5.5) 754

Troubleshoot Connectivity Remotely (37.6) 755

Supporting Remote Users (37.6.1) 756

Remote Access with Telnet, SSH, and RDP (37.6.2) 757

Understanding VPNs (37.6.4) 760

Site-to-Site VPN 760

Remote-Access VPN 761

Network Management Systems (37.6.5) 763

Network Support Summary (37.7) 765

What Did I Learn in This Chapter? (37.7.1) 765

Reflection Questions (37.7.2) 769

Practice 770

Labs 770

Packet Tracer Activities 770

Check Your Understanding Questions 770

Chapter 38 Cybersecurity Threats, Vulnerabilities, and Attacks 775

Objectives 775

Key Terms 775

Introduction (38.0) 776

Common Threats (38.1) 776

Threat Domains (38.1.1) 776

Types of Cyber Threats (38.1.2) 777

Internal vs. External Threats (38.1.3) 777

User Threats and Vulnerabilities (38.1.5) 778

Threats to Devices (38.1.6) 780

Threats to the Local Area Network (38.1.7) 780

Threats to the Private Cloud (38.1.8) 781

Threats to the Public Cloud (38.1.9) 781

Threats to Applications (38.1.10) 781

Threat Complexity (38.1.12) 782

Backdoors and Rootkits (38.1.13) 782

Backdoors 782
Rootkits 783
Threat Intelligence and Research Sources (38.1.14) 783
The Dark Web 783
Indicator of Compromise (IOC) 783
Automated Indicator Sharing (AIS) 783
Deception (38.2) 784
Social Engineering (38.2.1) 784
Pretexting 784
Something for Something (Quid Pro Quo) 784
Identity Fraud 784
Social Engineering Tactics (38.2.2) 785
Shoulder Surfing and Dumpster Diving (38.2.4) 786
Impersonation and Hoaxes (38.2.5) 786
Impersonation 786
Hoaxes 786
Piggybacking and Tailgating (38.2.6) 787
Other Methods of Deception (38.2.7) 787
Defending Against Deception (38.2.9) 788
Cyber Attacks (38.3) 788
Malware (38.3.1) 788
Viruses 789
Worms 789
Trojan Horse 789
Logic Bombs (38.3.2) 789
Ransomware (38.3.3) 790
Denial of Service Attacks (38.3.4) 790
Overwhelming Quantity of Traffic 790
Maliciously Formatted Packets 791
Domain Name System (38.3.5) 791
Domain Reputation 791
DNS Spoofing 791
Domain Hijacking 791
Uniform Resource Locator (URL) Redirection 792
Layer 2 Attacks (38.3.6) 792
Spoofing 792
MAC Flooding 792
Man-in-the-Middle and Man-in-the-Mobile Attacks (38.3.8) 793
Man-in-the-Middle (MitM) 793
Man-in-the-Mobile (MitMo) 793

Zero-Day Attacks (38.3.9) 793

Keyboard Logging (38.3.10) 793

Defending Against Attacks (38.3.12) 794

Wireless and Mobile Device Attacks (38.4) 794

Grayware and SMiShing (38.4.1) 794

Rogue Access Points (38.4.2) 795

Radio Frequency Jamming (38.4.3) 795

Bluejacking and Bluesnarfing (38.4.4) 796

Bluejacking 796

Bluesnarfing 796

Attacks Against Wi-Fi Protocols (38.4.5) 796

Wi-Fi and Mobile Defense (38.4.6) 797

Application Attacks (38.5) 797

Cross-Site Scripting (38.5.1) 797

Code Injection (38.5.2) 798

XML Injection Attack 798

SQL Injection Attack 798

DLL Injection Attack 798

LDAP Injection Attack 798

Buffer Overflow (38.5.3) 799

Remote Code Executions (38.5.4) 799

Other Application Attacks (38.5.5) 799

Defending Against Application Attacks (38.5.7) 801

Spam (38.5.8) 801

Phishing (38.5.9) 802

Phishing 802

Spear Phishing 802

Vishing, Pharming, and Whaling (38.5.10) 802

Vishing 802

Pharming 803

Whaling 803

Defending Against Email and Browser Attacks (38.5.12) 803

Physical Attacks 804

Adversarial Artificial Intelligence Attacks 804

Supply Chain Attacks 804

Cloud-Based Attacks 804

Cybersecurity Threats, Vulnerabilities, and Attacks Summary (38.6) 805

What Did I Learn in This Chapter? (38.6.1) 805
Reflection Questions (38.6.2) 810

Practice 811

Labs 811

Check Your Understanding Questions 811

Chapter 39 Network Security 813

Objectives 813

Key Terms 813

Introduction (39.0) 814

Security Foundations (39.1) 814

The Cybersecurity Cube (39.1.1) 814
Confidentiality, Integrity, and Availability (39.1.2) 816
CIA Triad—The Principle of Confidentiality (39.1.3) 816
Data Integrity (39.1.5) 817
Ensuring Availability (39.1.7) 819

Access Control (39.2) 820

Physical Access Controls (39.2.1) 820
Logical Access Controls (39.2.2) 821
Administrative Access Controls (39.2.3) 821
Authentication, Authorization, and Accounting (AAA) (39.2.4) 822
Authentication 822
Authorization 822
Accounting 823
What Is Identification? (39.2.5) 823
Federated Identity Management (39.2.6) 823
Authentication Methods (39.2.7) 824
What You Know 824
What You Have 824
Who You Are 825
Passwords (39.2.8) 825
Password Managers 826
Multi-Factor Authentication 827
Multi-Factor Authentication (39.2.9) 827
Authorization (39.2.10) 827
When to Implement Authorization 827
How to Implement Authorization 828

Accounting (39.2.11) 828

Defending Systems and Devices (39.3) 829

Operating System Security (39.3.1) 829

A Good Administrator 829

A Systematic Approach 829

A Baseline 830

Types of Antimalware (39.3.3) 830

Watch Out for Rogue Antivirus Products 830

Fileless Attacks Are Difficult to Detect and Remove 830

Scripts Can also Be Malware 830

Always Remove Unapproved Software 830

Patch Management (39.3.4) 831

What Are Patches? 831

What Do You Need to Do? 831

A Proactive Approach 831

Endpoint Security (39.3.5) 832

Host-Based Firewalls 832

Host Intrusion Detection Systems (HIDSs) 832

Host Intrusion Prevention Systems (HIPSs) 832

Endpoint Detection and Response (EDR) 832

Data Loss Prevention (DLP) 833

Next-Generation Firewall (NGFW) 833

Host Encryption (39.3.6) 833

Boot Integrity (39.3.7) 834

What Is Boot Integrity? 834

How Does Secure Boot Work? 834

What Is Measured Boot? 834

Apple System Security Features (39.3.8) 835

Physical Protection of Devices (39.3.9) 836

Computer Equipment 836

Door Locks 836

Radio Frequency Identification (RFID) Systems 836

Antimalware Protection (39.4) 836

Endpoint Threats (39.4.1) 837

Endpoint Security (39.4.2) 837

Host-Based Malware Protection (39.4.3) 839

Antivirus/Antimalware Software 839

Host-Based Firewall 840

Host-Based Security Suites 840

Network-Based Malware Protection (39.4.4) 841

Firewalls and Host-Based Intrusion Prevention (39.5) 842

Firewalls (39.5.1) 842

Common Firewall Properties 843
Firewall Benefits 843
Firewall Limitations 843

Types of Firewalls (39.5.2) 843

Packet Filtering (Stateless) Firewall 843
Stateful Firewall 844
Application Gateway Firewall 844
Next-Generation Firewall 846

Packet Filtering Firewall Benefits and Limitations (39.5.4) 847

Stateful Firewall Benefits and Limitations (39.5.5) 848

Host-Based Firewalls (39.5.6) 849

Windows Defender Firewall 850
iptables 850
nftables 850
TCP Wrappers 850

Antimalware Programs (39.5.7) 850

Windows Defender Firewall (39.5.8) 851

Secure Wireless Access (39.6) 854

Wireless Security Overview (39.6.2) 854

DoS Attacks (39.6.3) 854

Rogue Access Points (39.6.4) 855

Man-in-the-Middle Attack (39.6.5) 856

SSID Cloaking and MAC Address Filtering (39.6.8) 858

SSID Cloaking 859
MAC Addresses Filtering 859

802.11 Original Authentication Methods (39.6.9) 860

Shared Key Authentication Methods (39.6.10) 860

Authenticating a Home User (39.6.11) 861

Encryption Methods (39.6.12) 862

Authentication in the Enterprise (39.6.13) 863

WPA3 (39.6.14) 864

WPA3-Personal 864
WPA3-Enterprise 864
Open Networks 865
IoT Onboarding 865

Network Security Summary (39.7) 865

What Did I Learn in This Chapter? (39.7.1) 865

Reflection Questions (39.7.2) 870

Practice 871

Packet Tracer Activities 871

Check Your Understanding Questions 871

Appendix A Answers to the "Check Your Understanding" Questions 875

Index 905

Online Element

Glossary

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Networking Essentials Companion Guide Version 3: Cisco Certified Support Technician (CCST) Networking 100-150 is the official supplemental textbook for the Cisco Network Academy Networking Essentials version 3 course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small- to medium-sized businesses as well as enterprise and service provider environments.

As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples as compared with the course. You can use the online curriculum as directed by your instructor and then use this Companion Guide's study tools to help solidify your understanding of all the topics.

This book is a reflection of the Cisco Network Academy Networking Essentials version 3 online course. The format, content, and sequence of topics within this book are meant to mirror the online content for those who want an alternative version to the online course. The online course includes videos, animations, and activities not included in this book. It is recommended that you use this book along with the online course to get the full benefit from the course material.

Who Should Read This Book?

The book, as well as the course, is designed to provide learners with a broad foundational understanding of networking. It is suitable for anyone interested in a career in Information and Communication Technology (ICT), or a related career pathway. Networking Essentials is instructor-led. In this course you will learn how networks operate, including the devices, media, and protocols that enable network communication. You will also develop key skills so you can perform basic troubleshooting, using effective methodologies and help desk best practices.

There is a self-paced version of this course called the Network Technician Career Path. This is a collection of four courses that prepares you for the Cisco Certified Support Technician (CCST) Networking certification. This Career Path includes activities that expand on the course material presented. Upon completion of the online course, the end-of-course survey, and the end-of-course assessment, you will receive a Certificate of Completion. You will also receive a digital badge if the course is taken with an instructor in an instructor-led class.

For those who may wish a more traditional and thorough approach to networking, you may be interested in the Cisco Press CCNAv7 Companion Guide series: Introduction to Networks (ITN), Switching, Routing, and Wireless Essentials (SWRE), and Enterprise Networking, Security, and Automation (ENSA).

Online Course Enrollment

If you are interested in completing this Networking Essentials curriculum through one of our academies (e.g., instructor-led), please visit https://www.netacad.com/portal/netacad_academy_search to find a location near you.

The Network Technician Career Path is the online, self-paced version of this curriculum. You can enroll for free by visiting https://skillsforall.com/career-path/network-technician.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the *Companion Guide* encourages you to think about finding the answers as you read the chapter.
- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of the chapter there is a full list of all the labs, class activities, and Packet Tracer activities to refer back to for study time.

Readability

The following features assist your understanding of the networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in alphabetical order. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary with more than 328 terms.

Practice

Practice makes perfect. This *Companion Guide* offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

Interactive Graphic

- **Check Your Understanding questions and answer key:** Review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "Answers to the 'Check Your Understanding' Questions," provides an answer key to all the questions and includes an explanation of each answer.
- **Labs and activities:** Throughout each chapter, you will be directed back to the online course to take advantage of the activities created to reinforce concepts. In addition, at the end of each chapter, there is a "Practice" section that collects a list of all the labs and activities to provide practice with the topics introduced in this chapter.

Video

- **Page references to online course:** After headings, you will see, for example, (1.1.2). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.

About Packet Tracer Software and Activities

Packet Tracer
□ Activity

Interspersed throughout the chapters you'll find a few Cisco Packet Tracer activities. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in the course. For self-enrolled courses on SkillsForAll.com, Packet Tracer software is available through a link in your course after you enroll. For instructor-led courses on the Cisco Networking Academy website (netacad.com), Packet Tracer software is available from the Resources menu.

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy Switching, Routing, and Wireless Essentials course and is divided into 39 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "Communications in a Connected World":** This chapter explains important concepts in network communication including the concept of a network, network data, and network transmission speeds and capacity.
- **Chapter 2, "Network Components, Types, and Connections":** This chapter explains the role of clients, servers, and networking devices. It also covers the different ISP connectivity options.
- **Chapter 3, "Wireless and Mobile Networks":** This chapter provides a brief overview of the networks used by mobile devices and how you configure basic connectivity in iOS and Android devices.
- **Chapter 4, "Build a Home Network":** This chapter covers how to configure an integrated wireless router and wireless client to connect securely to the Internet including a description of the components required to build a home network, and the wired and wireless network technologies used.
- **Chapter 5, "Communication Principles":** This chapter underscores the importance of standards and protocols in network communications, explains the role of network communication protocols in regulating data exchange, outlines network communication standards for consistent implementation, and compares the OSI and TCP/IP models as frameworks for understanding network layers and protocols.
- **Chapter 6, "Network Media":** This chapter covers the various common types of network cables used for data transmission.
- **Chapter 7, "The Access Layer":** This chapter covers the communication process on Ethernet networks, including the explanation of encapsulation and Ethernet framing, along with insights into how to improve network communication at the access layer.
- **Chapter 8, "The Internet Protocol":** This chapter covers the features of an IP address, the purpose of an IPv4 address, and how IPv4 addresses and subnets are used together for network communication.
- **Chapter 9, "IPv4 and Network Segmentation":** This chapter covers the utilization and segmentation of IPv4 addresses in network communication, including a comparison of unicast, broadcast, and multicast addresses, as well as an explanation of public, private, and reserved IPv4 addresses, and how subnetting enhances network communication through segmentation.

- **Chapter 10, "IPv6 Addressing Formats and Rules":** This chapter discusses the features of IPv6 addressing, the necessity for its implementation, and the methods for representing IPv6 addresses.
- **Chapter 11, "Dynamic Addressing with DHCP":** This chapter explores the comparison between static and dynamic IPv4 addressing, and demonstrates the configuration of a DHCPv4 server for the dynamic assignment of IPv4 addresses.
- **Chapter 12, "Gateways to Other Networks":** This chapter introduces network boundaries and discusses the purpose of Network Address Translation in small networks.
- **Chapter 13, "The ARP Process":** This chapter compares the roles of MAC and IP addresses, discusses the significance of containing broadcasts within a network, and covers how ARP facilitates network communication.
- **Chapter 14, "Routing Between Networks":** This chapter discusses the necessity of routing, explains how routers use routing tables, and demonstrates how to configure a fully connected network.
- **Chapter 15, "TCP and UDP":** This chapter discusses the comparison of TCP and UDP, explains the use of port numbers, and details how clients access Internet services.
- **Chapter 16, "Application Layer Services":** This chapter covers the functions of common application layer services that typically use client/server interactions. It describes various network applications including DNS, HTTP, HTML, FTP, Telnet, SSH, and email protocols.
- **Chapter 17, "Network Testing Utilities":** This chapter describes the use of various tools to test and troubleshoot network connectivity.
- **Chapter 18, "Network Design":** This chapter outlines the four fundamental prerequisites for a dependable network and delves into the operational role of each layer within a three-layer hierarchical network design.
- **Chapter 19, "Cloud and Virtualization":** This chapter covers the characteristics of clouds and cloud services, as well as the purpose and attributes of virtualization.
- **Chapter 20, "Number Systems":** This chapter covers converting numbers between decimal, binary, and hexadecimal systems.
- **Chapter 21, "Ethernet Switching":** This chapter details Ethernet operations within a switched network, covering OSI model Layer 1 and Layer 2 functions, the relationship between Ethernet sublayers and frame fields, various types of Ethernet MAC addresses, and the process by which a switch constructs its MAC address table and forwards frames.

- **Chapter 22, "Network Layer":** This chapter describes how routers use network layer protocols and services to facilitate end-to-end connectivity, including the use of IP protocols for dependable communication, and the significance of key header fields within both IPv4 and IPv6 packets.
- **Chapter 23, "IPv4 Address Structure":** This chapter describes the structure of an IPv4 address, its network portion, host portion, and subnet mask. It then details how to calculate an efficient IPv4 subnetting scheme for network segmentation.
- **Chapter 24, "Address Resolution":** This chapter highlights the purpose of ARP in establishing efficient data transmission. It discusses how ARP facilitates communication within a local area network by resolving IP addresses to MAC addresses.
- **Chapter 25, "IP Addressing Services":** This chapter explains how DNS and DHCP services operate.
- **Chapter 26, "Transport Layer":** This chapter provides an overview of the transport layer's role in end-to-end communications, detailing TCP and UDP characteristics, their use of port numbers, the reliability facilitated by TCP's session establishment and termination, the transmission and acknowledgment of TCP protocol data units for assured delivery, and the UDP client processes involved in establishing communication with a server.
- **Chapter 27, "The Cisco IOS Command Line":** This chapter covers the use of Cisco IOS, including the correct command usage for navigating its modes, guidance on configuring network devices, and the use of **show** commands for monitoring device operations.
- **Chapter 28, "Build a Small Cisco Network":** This chapter covers the process of building a basic computer network using Cisco devices, including initial Cisco switch and router configuration, secure remote management configuration, and default gateway configuration.
- **Chapter 29, "ICMP":** This chapter explains how ICMP works and explores using ICMP diagnostic tools, ping and traceroute, to test network connectivity.
- **Chapter 30, "Physical Layer":** This chapter explores how physical layer protocols, services, and network media facilitate communication within data networks, including topics such as the role and functions of the physical layer, characteristics of copper cabling, the utilization of UTP cable in Ethernet networks, and the distinct advantages of fiber-optic cabling in comparison to other communication media.
- **Chapter 31, "Data Link Layer":** This chapter covers how media access control in the data link layer facilitates communication across physical and logical networks, including a comparison of the attributes of physical and logical topologies, and an explanation of how devices access a LAN to transmit frames.

- **Chapter 32, "Routing at the Network Layer":** This chapter describes the use of routing tables by network devices to effectively route packets to their intended destination networks. It further explains the significance and role of the various fields within a router's routing table.
- **Chapter 33, "IPv6 Addressing":** This chapter covers the implementation of an IPv6 addressing scheme, including a comparison of different types of IPv6 network addresses, explanations of configuring static global unicast and link-local IPv6 addresses, dynamic configuration of global unicast addresses, configuring link-local addresses dynamically, and the identification of IPv6 addresses.
- **Chapter 34, "IPv6 Neighbor Discovery":** This chapter describes how IPv6 neighbor discovery facilitates network communication by explaining its discovery mechanisms and operations.
- **Chapter 35, "Cisco Switches and Routers":** This chapter provides an overview of Cisco routers and switches, including Cisco LAN switches, switch forwarding methods, port settings on Layer 2 switch ports, the Cisco LAN switch boot process, Cisco small business routers, and the Cisco router boot process.
- **Chapter 36, "Troubleshoot Common Network Problems":** This chapter covers troubleshooting basic network connectivity issues, including approaches for network troubleshooting, detecting physical layer problems, addressing wireless network problems, explaining common Internet connectivity issues, and using external sources and Internet resources for effective troubleshooting.
- **Chapter 37, "Network Support":** This chapter covers effective troubleshooting methodologies and help desk best practices, including creating network documentation, explaining help desk best practices, verifying network connectivity on various operating systems, troubleshooting network issues, and explaining remote connectivity troubleshooting.
- **Chapter 38, "Cybersecurity Threats, Vulnerabilities, and Attacks":** This chapter provides an overview of common threats, vulnerabilities, and attacks on endpoints that occur in various domains, the deception methods used by attackers, as well as prevalent types of network, wireless, mobile device, and application attacks.
- **Chapter 39, "Network Security":** This chapter covers foundational security concepts, access control configuration, cybersecurity processes, malware mitigation methods, endpoint security operation, and how to configure basic wireless security on a home router using WPAx.
- **Appendix, "Answers to the 'Check Your Understanding' Questions":** This appendix lists the answers to the "Check Your Understanding" review questions that are included at the end of each chapter.
- **Glossary:** The Glossary provides you with definitions for all the key terms identified in each chapter.

CHAPTER 5

Communication Principles

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What are network communication protocols?
- What are network communication standards?
- What is the difference between the OSI and TCP/IP models?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

International Organization for Standardization (ISO)	*Page 83*
Internet Engineering Task Force (IETF)	*Page 80*
Open Systems Interconnection (OSI)	*Page 83*
protocol	*Page 79*
protocol suite	*Page 82*
reference model	*Page 82*
Request for Comments (RFC)	*Page 80*

Introduction (5.0)

The next day at the hospital, Kishori has a new patient, Srinivas, who has just been admitted to a room. He is from Narayanpet and speaks Telugu. Kishori speaks Marathi. These two Indian languages are very different. Kishori and Srinivas do not speak each other's native language. However, they do both speak English. Therefore, they decide to communicate using English.

Before beginning to communicate with each other, we establish rules or agreements to govern the conversation. Just like Kishori and Srinivas, we decide what method of communication we should use, and what language we should use. We may also need to confirm that our messages are received. For example, Kishori may have Srinivas sign a document verifying that he has understood Kishori's care instructions.

Networks also need rules, or protocols, to ensure successful communication. This chapter will cover the communication principles for networks. Let's get started!

Networking Protocols (5.1)

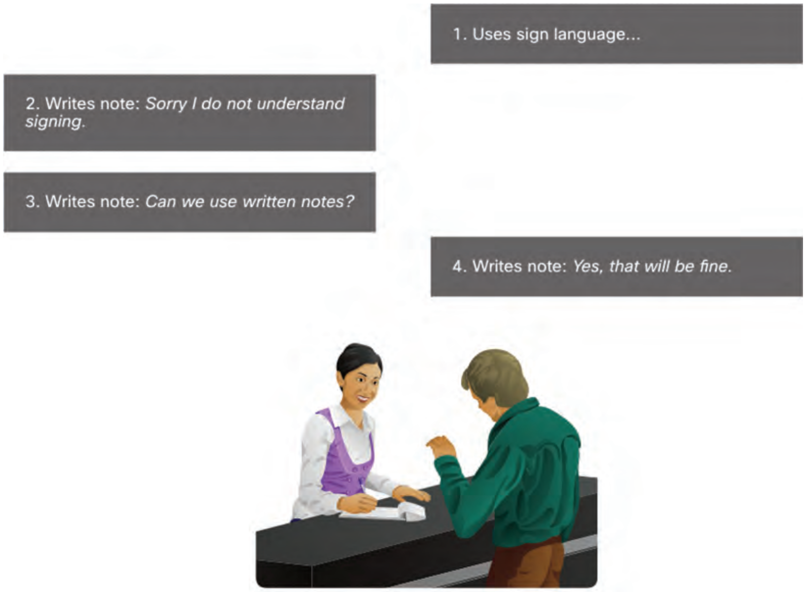
Before communicating with one another, individuals must use established rules or agreements to govern the conversation. Rules are also required for devices on a network to communicate.

Communication Protocols (5.1.1)

Communication in our daily lives takes many forms and occurs in many environments. We have different expectations depending on whether we are chatting via the Internet or participating in a job interview. Each situation has its corresponding expected behaviors and styles.

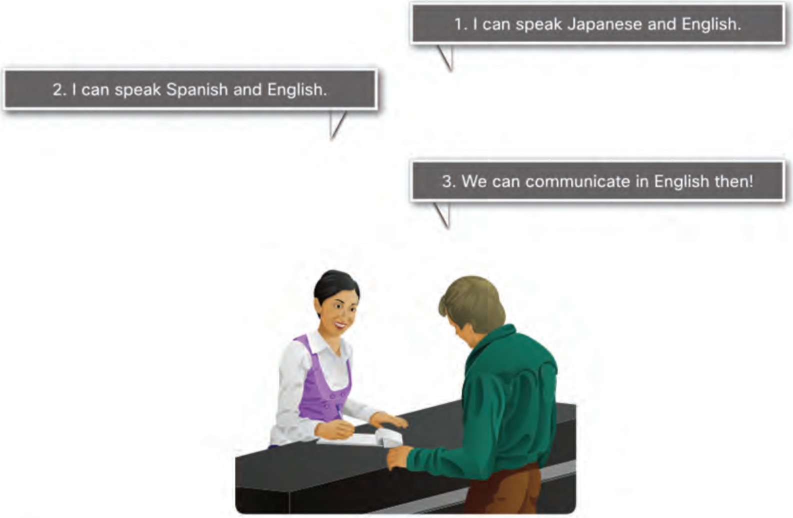
Before beginning to communicate with each other, we establish rules or agreements to govern the conversation. These agreements include the following:

- **Method**—What method of communication should we use? (See Figure 5-1.)
- **Language**—What language should we use? (See Figure 5-2.)
- **Confirmation**—Do we need to confirm that our messages are received? (See Figure 5-3.)


1. Uses sign language...
2. Writes note: *Sorry I do not understand signing.*
3. Writes note: *Can we use written notes?*
4. Writes note: *Yes, that will be fine.*

Before communication can begin, we may have to reach an agreement on the method used.

Figure 5-1 Choosing a Method of Communication


1. I can speak Japanese and English.
2. I can speak Spanish and English.
3. We can communicate in English then!

Before communication can begin, we may have to reach an agreement on the language used.

Figure 5-2 Choosing a Language for Communication

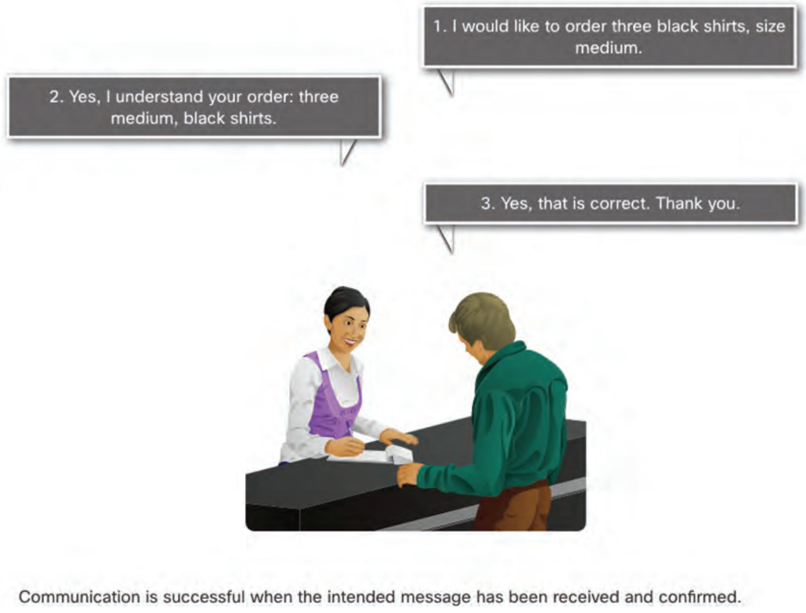

1. I would like to order three black shirts, size medium.
2. Yes, I understand your order: three medium, black shirts.
3. Yes, that is correct. Thank you.
Communication is successful when the intended message has been received and confirmed.

Figure 5-3 Verifying That Communication Was Successful

These rules, or *protocols*, must be followed for the message to be successfully delivered and understood. Among the protocols that govern successful human communication are these:

- An identified sender and receiver
- Agreed-upon method of communicating (face-to-face, telephone, letter, photograph)
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgment requirements

The techniques that are used in network communications share these fundamentals with human conversations.

Think about the commonly accepted protocols for sending text messages to your friends.

Why Protocols Matter (5.1.2)

Just like humans, computers use rules, or protocols, to communicate. Protocols are required for computers to properly communicate across the network. In both a wired and wireless environment, a local network is defined as an area where all hosts must "speak the same language," which in computer terms means they must "share a common protocol."

If everyone in the same room spoke a different language, they would not be able to communicate. Likewise, if devices in a local network did not use the same protocols, they would not be able to communicate.

Networking *protocols* define many aspects of communication over the local network. As shown in Table 5-1, these include message format, message size, timing, encoding, encapsulation, and message pattern.

Table 5-1 Protocol Characteristics

Protocol Characteristic	Description
Message format	When a message is sent, it must use a specific format or structure. Message formats depend on the type of message and the channel that is used to deliver the message.
Message size	The rules that govern the size of the pieces communicated across the network are very strict. They can also be different, depending on the channel used. When a long message is sent from one host to another over a network, it may be necessary to break the message into smaller pieces to ensure that the message can be delivered reliably.
Timing	Many network communication functions are dependent on timing. Timing determines the speed at which the bits are transmitted across the network. It also affects when an individual host can send data and the total amount of data that can be sent in any one transmission.
Encoding	Messages sent across the network are first converted into bits by the sending host. Each bit is encoded into a pattern of sounds, light waves, or electrical pulses depending on the network media over which the bits are transmitted. The destination host receives and decodes the signals to interpret the message.
Encapsulation	Each message transmitted on a network must include a header that contains addressing information that identifies the source and destination hosts; otherwise, it cannot be delivered. Encapsulation is the process of adding this information to the pieces of data that make up the message. In addition to addressing, there may be other information in the header that ensures that the message is delivered to the correct application on the destination host.
Message pattern	Some messages require an acknowledgment before the next message can be sent. This type of request/response pattern is a common aspect of many networking protocols. However, there are other types of messages that may be simply streamed across the network, without concern as to whether they reach their destination.

Communication Standards (5.2)

Communication standards are required in all aspects of human communications. For example, when addressing an envelope, there is a standard regarding the placement of the sender's address, the destination address, and the stamp. Network communication also requires standards to ensure that all the devices in the network are using the same rules to send and receive information.

Video

Video—Devices in a Bubble (5.2.1)

Refer to the online course to view this video.

The Internet and Standards (5.2.2)

With the increasing number of new devices and technologies coming online, how is it possible to manage all the changes and still reliably deliver services such as email? The answer is Internet standards.

A *standard* is a set of rules that determines how something must be done. Networking and Internet standards ensure that all devices connecting to the network implement the same set of rules or protocols in the same manner. Using standards enables different types of devices to send information to each other over the Internet. For example, the way in which an email is formatted, forwarded, and received by all devices is done according to a standard. If one person sends an email via a personal computer, another person can use a mobile phone to receive and read the email as long as the mobile phone uses the same standards as the personal computer.

Network Standards Organizations (5.2.3)

An Internet standard is the end result of a comprehensive cycle of discussion, problem solving, and testing. These different standards are developed, published, and maintained by a variety of organizations. When a new standard is proposed, each stage of the development and approval process is recorded in a numbered ***Request for Comments (RFC)*** document so that the evolution of the standard is tracked. RFCs for Internet standards are published and managed by the ***Internet Engineering Task Force (IETF)***.

The logos of IETF and other standards organizations that support the Internet are shown in Figure 5-4.

IEEE
iana
Internet Assigned Numbers Authority
I E T F
ICANN
The Internet Corporation for Assigned Names and Numbers
ITU
TIA

Figure 5-4 Internet Standards Organizations

Network Communication Models (5.3)

Network communication models help us understand the various components and protocols used in network communications. These models help us see the function of each protocol and their relationship to other protocols.

Video

Video—Network Protocols (5.3.1)

Refer to the online course to view this video.

Video

Video—The Protocol Stack (5.3.2)

Refer to the online course to view this video.

The TCP/IP Model (5.3.3)

Layered models help us visualize how the various protocols work together to enable network communications. A layered model depicts the operation of the protocols occurring within each layer, as well as the interaction with the layers above and below it. The layered model has many benefits:

- Assists in protocol design, because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below.
- Fosters competition because products from different vendors can work together.
- Enables technology changes to occur at one level without affecting the other levels.
- Provides a common language to describe networking functions and capabilities.

The first layered model for internetwork communications was created in the early 1970s and is referred to as the Internet model. It defines four categories of functions that must occur for communications to be successful. The suite of TCP/IP protocols that are used for Internet communications follows the structure of this model, as shown in Table 5-2. Because of this, the Internet model is commonly referred to as the TCP/IP model.

Table 5-2 The Layers of the TCP/IP Model

TCP/IP Model Layer	Description
Application	Represents data to the user, plus encoding and dialog control.
Transport	Supports communication between various devices across diverse networks.
Internet	Determines the best path through the network.
Network Access	Controls the hardware devices and media that make up the network.

The OSI Reference Model (5.3.4)

Two basic types of models are used to describe the functions that must occur for network communications to be successful:

- **Protocol model**—This type of model closely matches the structure of a particular protocol suite. A *protocol suite* includes the set of related protocols that typically provide all the functionality required for people to communicate with the data network. The TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite.
- *Reference model*—This type of model describes the functions that must be completed at a particular layer but does not specify exactly how a function should be accomplished. A reference model is not intended to provide a sufficient

level of detail to define precisely how each protocol should work at each layer. The primary purpose of a reference model is to aid in clearer understanding of the functions and processes necessary for network communications.

The most widely known internetwork reference model was created by the *Open Systems Interconnection (OSI)* project at the *International Organization for Standardization (ISO)*. It is used for data network design, operation specifications, and troubleshooting. This model is commonly referred to as the OSI model. The OSI layers are described in Table 5-3.

Table 5-3 The Layers of the OSI Model

OSI Model Layer	Description
7—Application	The application layer contains protocols used for process-to-process communications.
6—Presentation	The presentation layer provides for common representation of the data transferred between application layer services.
5—Session	The session layer provides services to the presentation layer to organize its dialogue and to manage data exchange.
4—Transport	The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices.
3—Network	The network layer provides services to exchange the individual pieces of data over the network between identified end devices.
2—Data link	The data link layer protocols describe methods for exchanging data frames between devices over a common media.
1—Physical	The physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for a bit transmission to and from a network device.

OSI Model and TCP/IP Model Comparison (5.3.5)

Because TCP/IP is the protocol suite in use for Internet communications, why do you need to learn the OSI model as well?

The TCP/IP model is a method of visualizing the interactions of the various protocols that make up the TCP/IP protocol suite. It does not describe general functions that are necessary for all networking communications. It describes the networking functions specific to those protocols in use in the TCP/IP protocol suite. For example, at the network access layer, the TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium, nor the method of encoding the signals for transmission. OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

The protocols that make up the TCP/IP protocol suite can be described in terms of the OSI reference model. The functions that occur at the Internet layer in the TCP/IP model are contained in the network layer of the OSI model, as shown in Figure 5-5. The transport layer functionality is the same between both models. However, the network access layer and the application layer of the TCP/IP model are further divided in the OSI model to describe discrete functions that must occur at these layers.

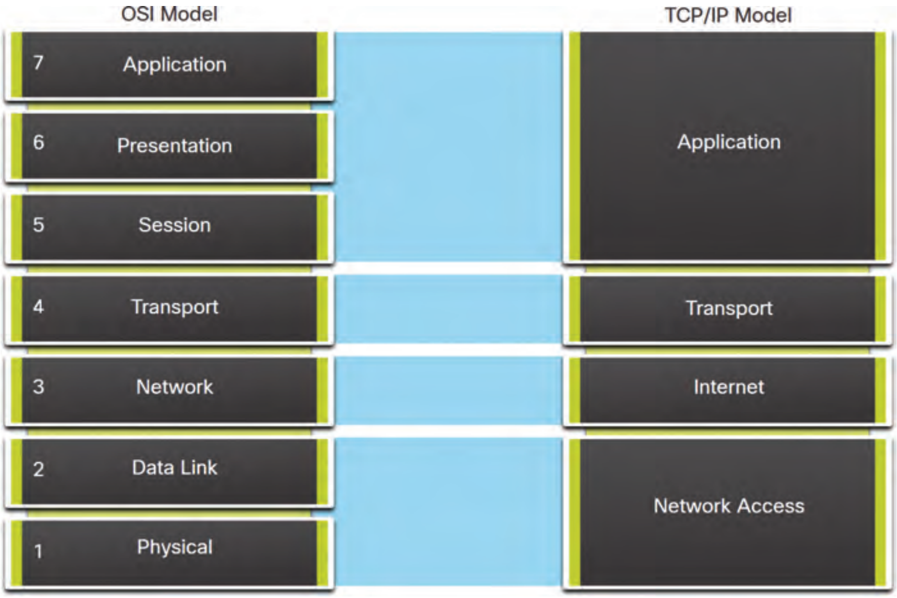


Figure 5-5 The OSI and TCP/IP Models

The key similarities are in the transport and network layers; however, the two models differ in how they relate to the layers above and below each layer:

- OSI Layer 3, the network layer, maps directly to the TCP/IP Internet layer. This layer is used to describe protocols that address and route messages through an internetwork.
- OSI Layer 4, the transport layer, maps directly to the TCP/IP transport layer. This layer describes general services and functions that provide ordered and reliable delivery of data between source and destination hosts.
- The TCP/IP application layer includes several protocols that provide specific functionality to a variety of end-user applications. The OSI model Layers 5, 6,

and 7 are used as references for application software developers and vendors to produce applications that operate on networks.

- Both the TCP/IP and OSI models are commonly used when referring to protocols at various layers. Because the OSI model separates the data link layer from the physical layer, it is commonly used when referring to these lower layers.

Communication Principles Summary (5.4)

The following is a summary of each topic in the chapter and some questions for your reflection.

What Did I Learn in This Chapter? (5.4.1)

- **Communication Protocol**—Protocols are required for computers to properly communicate across the network. Protocols define the following aspects of communication over the local network:
    - **Message format**—When a message is sent, it must use a specific format or structure.
    - **Message size**—The rules that govern the size of the pieces communicated across the network are very strict. They can also be different, depending on the channel used.
    - **Timing**—Timing determines the speed at which the bits are transmitted across the network. It also affects when an individual host can send data and the total amount of data that can be sent in any one transmission.
    - **Encoding**—Messages sent across the network are first converted into bits by the sending host. Each bit is encoded into a pattern of sounds, light waves, or electrical pulses depending on the network media over which the bits are transmitted.
    - **Encapsulation**—Each message transmitted on a network must include a header that contains addressing information that identifies the source and destination hosts. Encapsulation is the process of adding this information to the pieces of data that make up the message.
    - **Message pattern**—Some messages require an acknowledgment before the next message can be sent. This type of request/response pattern is a common aspect of many networking protocols. However, other types of messages may be simply streamed across the network, without concern as to whether they reach their destination.

- **Communication Standards—**Topologies allow us to see the networking using representation of end devices and intermediary devices. How does a device see a network? Think of a device in a bubble. The only thing a device sees is its own addressing information. How does the device know it is on the same network as another device? The answer is network protocols. Most network communications are broken up into smaller data units, or packets.

  A standard is a set of rules that determines how something must be done. Networking and Internet standards ensure that all devices connecting to the network implement the same set of rules or protocols in the same manner. Using standards enables different types of devices to send information to each other over the Internet.

  An Internet standard is the end result of a comprehensive cycle of discussion, problem solving, and testing. Internet standards are developed, published, and maintained by a variety of organizations. When a new standard is proposed, each stage of the development and approval process is recorded in a numbered RFC document so that the evolution of the standard is tracked. RFCs for Internet standards are published and managed by the IETF.

- **Network Communication Models—**Protocols are the rules that govern communications. Successful communication between hosts requires interaction between a number of protocols. Protocols include HTTP, TCP, IP, and Ethernet. These protocols are implemented in software and hardware that are installed on each host and networking device.

  The interaction between the different protocols on a device can be illustrated as a protocol stack. A stack illustrates the protocols as a layered hierarchy, with each higher-level protocol depending on the services of the protocols shown in the lower levels. The separation of functions enables each layer in the stack to operate independently of others.

  The suite of TCP/IP protocols that are used for Internet communications follows the structure of this model:

  - **Application—**Represents data to the user, plus encoding and dialog control
  - **Transport—**Supports communication between various devices across diverse networks
  - **Internet—**Determines the best path through the network
  - **Network Access—**Controls the hardware devices and media that make up the network

  A reference model describes the functions that must be completed at a particular layer but does not specify exactly how a function should be accomplished. The primary purpose of a reference model is to aid in clearer understanding of the functions and processes necessary for network communications.

The most widely known internetwork reference model was created by the OSI project at the ISO. It is used for data network design, operation specifications, and troubleshooting. This model is commonly referred to as the OSI model.

The layers in the OSI model are as follows:

- **7—Application**—Contains protocols used for process-to-process communications
- **6—Presentation**—Provides for common representation of the data transferred between application layer services
- **5—Session**—Provides services to the presentation layer to organize its dialogue and to manage data exchange
- **4—Transport**—Defines services to segment, transfer, and reassemble the data for individual communications between the end devices
- **3—Network**—Provides services to exchange the individual pieces of data over the network between identified end devices
- **2—Data link**—Includes protocols that describe methods for exchanging data frames between devices over a common media
- **1—Physical**—Includes protocols that describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for a bit transmission to and from a network device

Reflection Questions (5.4.2)

Recall that Kishori and Srinivas had to determine a common language. Do you have any friends or relatives whose first language is different than yours? Do you know anyone who uses sign language? How would you communicate with them if you did not know sign language? Did you realize before reading this chapter that you were using a protocol (using a shared language or communicating in writing) to interact with family and friends?

Practice

There are no labs or Packet Tracer activities in this chapter.

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. Appendix A, "Answers to 'Check Your Understanding' Questions," lists the answers.

1. What is the purpose of the OSI physical layer?

   a. To control access to media

   b. To transmit bits across the local media

   c. To perform error detection on received frames

   d. To exchange frames between nodes over physical network media

2. Which statement is correct about network protocols?

   a. They define the type of hardware that is used and how it is mounted in racks.

   b. They define how messages are exchanged between the source and the destination.

   c. They all function in the network access layer of TCP/IP.

   d. They are required only for exchange of messages between devices on remote networks.

3. What networking term describes a particular set of rules at one layer that governs communication at that layer?

   a. Duplex

   b. Encapsulation

   c. Error checking

   d. Protocol

4. Which layer of the OSI model defines services to segment and reassemble data for individual communications between end devices?

   a. Application

   b. Presentation

   c. Session

   d. Transport

   e. Network

5. What is the purpose of protocols in data communications?

   a. To specify the bandwidth of the channel or medium for each type of communication

   b. To specify the device operating systems that will support the communication

   c. To provide the rules required for a specific type of communication to occur

   d. To dictate the content of the message sent during communication

6. Which term refers to a formalized protocol, usually approved by an accepted authority or organization, which can then be implemented by different vendors?

   a. Standard

   b. Protocol

   c. Model

   d. Domain

7. Which three layers of the OSI model make up the application layer of the TCP/IP model? (Choose three.)

   a. Data link

   b. Network

   c. Transport

   d. Session

   e. Presentation

   f. Application

8. Which organization publishes and manages the Request for Comments (RFC) documents?

   a. IEEE

   b. ISO

   c. IETF

   d. TIA/EIA

9. Which two OSI model layers have the same functionality as a single layer of the TCP/IP model? (Choose two.)

   a. Data link

   b. Network

   c. Physical

   d. Session

   e. Transport

This page intentionally left blank

Index

Numerics

2FA (two-factor authentication), 825
802.11, 70

A

AAA (authentication, authorization, and accounting), 822
  accounting, 823, 828
  authentication, 822
    multi-factor, 827
    what you have, 824–825
    what you know, 824
    who you are, 825
  authorization, 822–823
    how to implement, 828
    when to implement, 827–828
access control, 866–867
  administrative, 821–822
  logical, 821
  physical, 820–821
  TCP wrappers, 850
access layer, 104, 112, 273
  communication, 191
  devices, 105–106
  Ethernet
    frame, 104–105
    hub, 106–107
    switch, 107–108, 112
  MAC address table, 109–111
accounting, 823, 828
active listening, 731–732
actuator, 13
administrative access control, 821–822. *See also* **AAA (authentication, authorization, and accounting)**
advanced persistent threat, 782
adversarial artificial intelligence attacks, 804
AES (Advanced Encryption Standard), 862
AfriNIC (African Network Information Centre), 134
AIS (automated indicator sharing), 783–784
algorithm attacks, 782
Android, 53
  cellular data, 47–48
  troubleshooting connectivity, 747–749
  Wi-Fi, settings, 44–46
antimalware/antivirus, 830, 836–837, 839,841–842, 850–851, 868
anycast address, 588
AP (access point), 60, 795, 855–856
APIPA (Automatic Private IP Addressing), 133
APNIC (Asia Pacific Network Information Centre), 134
Apple, security features, 835. *See also* iOS; macOS
appliances, smart, 9–10
application gateway firewall, 844–845
application layer services. *See also* **client/server**
  client-server relationship, 230–231
  email, 242
    IMAP4 (Internet Message Access Protocol), 243–244
    POP3 (Post Office Protocol), 243
    SMTP (Simple Mail Transfer Protocol), 243
  FTP (File Transfer Protocol), 238
  HTML (Hypertext Markup Language), 237–238
  HTTP (Hypertext Transfer Protocol), 237–238
  Internet phone calls, 245
  network application services, 233, 234–236
  protocol, 216
  text messaging, 244
  virtual terminals, 239, 247
    SSH (Secure Shell), 241
    Telnet, 240–241
  web server, 231–233
application/s
  attacks, 799–801, 809
    buffer overflow, 799
    code injection, 798
    cross-site scripting, 797
    remote code execution, 799
  conversion, 409

P2P (peer-to-peer), 28
remote desktop, 756–757
threats, 781–782
well-known, 221
architecture, network, 266–267. *See also* **topology**
ARP (Address Resolution Protocol), 136, 189, 191–192, 193, 203,386
broadcasts, 382
cache timer, 385
functions, 377–378
map, 378, 384
reply, 378, 380
request, 379, 385, 385
role in remote communications, 380
security risks, 385
spoofing, 383
table, 384–385
removing entries, 380
showing contents, 381–382
arp -a command, 381–382, 385
ASCII (American Standard Code for Information Exchange), 15
attacks, 807–808
adversarial artificial intelligence, 804
algorithm, 782
application, 799–801, 809
buffer overflow, 799
code injection, 798
cross-site scripting, 797
remote code execution, 799
bluejacking/bluesnarfing, 796
cloud-based, 804–805
defending against, 794, 801
DoS, 790–791, 854–855
email
defending against, 803
phishing, 802
spear phishing, 802
keylogging, 793–794
Layer 2, spoofing, 792
logic bomb, 789–790
man-in-the-middle, 793, 856–857
man-in-the-mobile, 793
physical, 804
pretexting, 784
quid pro quo, 784
radio frequency jamming, 795
supply chain, 804
Trojan horse, 789
virus, 789
against Wi-Fi protocols, 796
worm, 789
zero-day, 793
attenuation, 530
authentication, 822. *See also* **password/s**
in the enterprise, 863–864
home network, 861–862
multi-factor, 827
passwords, 825–827
two-factor, 825
what you have, 824–825
what you know, 824
who you are, 825
wireless, 860
shared key, 860–861
WPA2/WPA3, 863–865
authorization, 822–823
how to implement, 828
when to implement, 827–828
auto-MDIX, 640–641
autonegotiation, 639
availability, 270, 818–819
AV-TEST, 841

B

back panel, router, 60
backbone, Internet, 34
backdoors, 782–783
in-band management, 644–645
bandwidth, 17, 527–528
Ethernet, 319
goodput, 529
latency, 528–529
throughput, 529, 754–755
banners, router, 481
"bare metal", 286
baseline
network, 718
operating system, 830
beep codes, 733
best effort delivery, 218, 348, 415

binary number system, 311
- converting decimal to, 296–307
- IPv4 and, 294–296

biometrics, 825

BIOS, 733

bit (binary digit), 14
- ASCII (American Standard Code for Information Exchange) code, 15
- discrete states, 15
- prefix length, 366–367

BitLocker/BitLocker To Go, 834

bluejacking/bluesnarfing, 796

Bluetooth, 43, 49–50, 52, 53
- pairing, 50–51, 53
- use cases, 50

boot integrity, 834

bottom-up troubleshooting, 662–663

boundary, network, 176, 180–181

bps (bits per second), 269

broadcast address, 127–128, 327

broadcast domain, 136–137, 189–190, 208
- ARP (Address Resolution Protocol), 191–192, 193
- problems with, 137
- subnetting, 137–140

broadcast transmission, 141

buffer overflow, 799

byte, 15

C

cable
- Category 5e, 62
- coaxial, 62–63, 94, 533–534
- copper, 529, 549
  - *characteristics, 529–531*
  - *STP (shielded twisted-pair), 533*
  - *twisted-pair, 93–94*
  - *UTP (unshielded twisted-pair), 531–532, 535–540, 549*
- fiber-optic, 63, 95, 549
  - *multimode, 542*
  - *patch cords, 545–547*
  - *properties, 541*
  - *single-mode, 541–542*
  - *usage, 543*
- troubleshooting, 670

cable Internet, 35

CAN (campus area network), 708

Category 5e cable, 62

CDP (Cisco Discovery Protocol), 719
- device discovery, 720–723
- mapping the network, 723

cellular Internet, 36. *See also* wireless network

CIA triad, 816–817
- availability, 818–819
- confidentiality, 816–817
- data integrity, 817–818

circuit, 108

Cisco IOS CLI, 456, 457, 469–470
- accessing from a Cisco router, 651–652
- auto-MDIX, 640–641
- command structure, 458–459
- command syntax, 459–460
- configuration mode, 456
- keystroke shortcuts, 460–461
  - *exiting a command mode, 462*
  - *--More-- prompt, 461–462*
- primary command modes, 457–458
- privileged EXEC mode, 751
- show arp command, 466
- show commands, 463, 750–752
- show interfaces command, 464–465
- show ip interface command, 465–466
- show ip route command, 467
- show protocols command, 467
- show running-config command, 463–464, 484
- show version command, 468
- user EXEC mode, 751

Cisco LAN switches, 631–632, 653–654
- cut-through switching, 636–638
- duplex and speed settings, 638–640
- expandability, 633
- IOS startup files, 645
- manageability, 633–634
- memory buffering, 638
- powering up, 642–644
- speed required, 632–633
- store-and-forward switching, 635–636
- type of ports, 632

Cisco routers, 646, 654
- components, 646
- interface ports, 647

management ports, 651–652
powering up, 648–651
classful addressing, 133–134, 141–142
CLI (command-line interface), 240
client/server, 26, 29, 37, 245–246. *See also* **webserver**
clients, 27
DHCP (Dynamic Host Configuration Protocol), 166–167
email, 242
IMAP4 (Internet Message Access Protocol), 243–244
POP3 (Post Office Protocol), 243
SMTP (Simple Mail Transfer Protocol), 243
FTP (File Transfer Protocol), 238, 247
hosts, 26, 32–33
P2P (peer-to-peer) network, 27–28
remote desktop, 756
requests, 231–232
servers, 27
software, 27
UDP (User Datagram Protocol), 443–445
web, 231, 246–247
HTML (Hypertext Markup Language), 237–238
HTTP (Hypertext Transfer Protocol), 237–238
URI (Uniform Resource Identifier), 232–233
URL (Uniform Resource Locator), 232
cloud, 282, 288
-based attacks, 804–805
-based network management, 763–765
community, 283
hybrid, 283
IaaS (Infrastructure as a Service), 283, 714
ITaaS (IT as a Service), 283–284
PaaS (Platform as a Service), 283, 713–714
private, 283
public, 282
SaaS (Software as a Service), 283, 713
threats, 781
virtualization, 284–285
advantages, 285, 288–289
hypervisor, 286–287
XaaS (anything/everything as a service), 714
coaxial cable, 62–63, 94, 533–534
codes, 525
command/s. *See also* **Cisco IOS CLI**
arp -a, 381–382
arp -a command, 385
crypto key generate rsa general keys modulus, 494
displaydns, 395
ifconfig, 742
interface vlan 1, 478
ip address, 595–596, 742
ip default-gateway, 478, 490
ip domain-name, 494
ipconfig, 254–255, 395, 606, 674, 738–740
/all option, 255–256
/release option, 256–257
/renew option, 256–257
iperf, 754–755
ipv6 address, 598
ipv6 unicast-routing, 600
link-local, 598
ncat, 742–743
netstat, 223–224, 426–427, 576, 680–682
nslookup, 236, 397, 401, 682–683
ping, 132, 258–259, 505–506, 512–513,612, 678, 740–741
default gateway, 507–508
local loopback, 506
options, 259–260
remote host, 508–509
results, 259
route print, 576
show, 463, 750–752
show arp, 466
show cdp neighbors, 720–723
show interfaces, 464–465
show ip arp, 381, 385
show ip interface, 465–466
show ip route, 467
show ipv6 interface brief, 610
show ipv6 route, 611
show protocols, 467
show running-config, 463–464, 484
show version, 468
Syntax Checker, 236
traceroute, 509, 513, 678–680, 741
IPv4 TTL and IPv6 hop limit, 509–510
RTT (round-trip time), 509

communication
- broadcast, 127–128, 141
- channels, 92
- client-server relationship, 230–231
- encapsulation, 79, 85, 102–104, 111–112
- full-duplex, 562
- half-duplex, 562
- models, 81, 83–85, 86
  - *OSI, 82–83*
  - *TCP/IP, 81–82*
- multicast, 141
- protocols, 76–79
- standards, 80–81, 86
- timing, 79, 85
- unicast, 126–127

community cloud, 283

confidentiality, 270, 816–817

configuration, DHCP (Dynamic Host Configuration Protocol), 167–168, 171

congestion avoidance, 440

connected home devices, 8
- appliances, 9–10
- encoding, 79
- gaming console, 11
- medical devices, 13–14
- RFID tags, 12
- security system, 8–9
- sensors and actuators, 13
- smart car, 11–12
- smart TV, 10

connectionless protocol, 415

connection-oriented protocol, 414

connections and connectivity. *See also* **ping command**
- dial-up, 36
- ISP (Internet service provider), 34–35
  - *cable, 35*
  - *cellular, 36*
  - *DSL (Digital Subscriber Line), 35*
  - *satellite, 36*
- mobile device
  - *Wi-Fi, 44–47*
- RJ-45 connector, 62
- TCP (Transmission Control Protocol), 430–431
- troubleshooting, 223–224, 689–690, 767–769
  - *on Android, 747–749*
  - *check Internet configuration, 674–677*
  - *DHCP server configuration errors, 674–675*
  - *firewall settings, 677*
  - *on iOS, 746*
  - *ipconfig command, 738–740*
  - *on Linux, 741–743*
  - *on macOS, 740–745*
  - *netstat command, 680–682*
  - *nslookup command, 682–683*
  - *ping command, 678, 740–741*
  - *traceroute command, 678–680, 741*
- vty (virtual terminal), 240

contention-based access, 563
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 566–567
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 564–566

controlled access, 564

conversation, 409

conversion
- decimal-to-binary, 296–307
- decimal-to-binary-to-hexadecimal, 325–326

copper cabling, 529, 549
- characteristics, 529–531
- coaxial, 533–534
- versus fiber-optic, 547–548
- STP (shielded twisted-pair), 533
- UTP (unshielded twisted-pair), 531–532, 549
  - *categories, 536–537*
  - *connectors, 537–539*
  - *properties, 535–536*
  - *standards, 536, 540*
  - *straight-through and crossover, 539–540*

core layer, 274

cross-site scripting, 797

crosstalk, 530

crypto key generate rsa general keys modulus command, 494

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 566–567

CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 564–566

customer support, 690–691
- help desk interaction, 685

issue resolution, 686
sources of help, 683–684
when to call for help, 684–685
cut-through switching, 636–638
CVE (common vulnerabilities and exposures), 783
cyber threats, 777
cybersecurity cube, 814
data states, 815
safeguards, 815–816
security principles, 814–815

D

dark web, 783
data center, 231
data confidentiality, 270, 816–817
data integrity, 270, 817–818
data link layer. ***See also*** **topology**
media access control
full-duplex communication, 562
half-duplex communication, 562
data transmission, 14
bandwidth, 17
bit (binary digit), 14
ASCII (American Standard Code for Information Exchange) code, 15
byte, 15
discrete states, 15
media, 15
signal, 15–16
throughput, 18
wireless, 96
datagram, 409, 441–442
deception, 787, 806–807
defending against, 788
hoaxes, 786
impersonation, 786
pharming, 803
piggybacking and tailgating, 787
shoulder surfing, 786
social engineering, 784–785
vishing, 802–803
whaling, 803
decimal-to-binary conversion, 296–307
de-encapsulation, 345
default gateway, 164, 176, 203–204, 380, 488–490,490–491, 507–508, 574, 574–575
default route, 578
Destination Unreachable message, 501–502
Device Manager, 734–735
DHCP (Dynamic Host Configuration Protocol), 136, 165–166, 170–171, 398,401–402
configuration, 167–168, 171
for IPv6, 399
lease period, 398
messages, 399–400
operation, 168
server, 398
servers, 166–167, 400
service configuration, 169–170
dial-up Internet, 36
directed broadcast, 128
displaydns command, 395
distribution layer, 205, 208, 274
divide-and-conquer troubleshooting, 664
DLL injection, 798
DLP (data loss prevention), 833
DNS (Domain Name System), 234, 246, 401
domain hijacking, 791
domain name translation, 234–235
domain reputation, 791
FQDN (fully qualified domain name), 392
hierarchy, 395–396
message, 392–393, 395
name resolution process, 393–394
resource records, 395
servers, 235–236
spoofing, 791
top-level domains, 396
URL redirection, 792
documentation
end-system, 718
LAN switch, 717
network, 704, 765–766
network device, 717
security policy, 723–725
domain
hijacking, 791
reputation, 791
door locks, 836

DoS (denial of service) attack, 790–791, 854–855
dotted-decimal notation, 119, 307–308, 366–367
double colon, IPv6 address format, 155–156
DRM (digital rights management), 817
DSL (Digital Subscriber Line), 35
dual stack, 150
dumpster diving, 786
duplex connector, 544–545
dynamic address assignment, IPv4, 165–166, 170
dynamic LLA (link-local address), 607–608
  on Cisco routers, 609
  on Windows, 608
dynamic routing, 580–581

E

EDR (endpoint detection and response), 832–833
educated guess, 665
EFS (Windows Encrypting File System), 833
electromagnetic spectrum, 69, 716
email, 242, 247–248
  clients and servers, 242
  defending against attacks, 803
  IMAP4 (Internet Message Access Protocol), 243–244
  phishing, 802
  POP3 (Post Office Protocol), 243
  SMTP (Simple Mail Transfer Protocol), 243
  spam, 801–802
  spear phishing, 802
EMI (electromagnetic interference), 530–531, 535
encapsulation, 79, 85, 102–104, 111–112, 203,344–345
  de-, 345
  Ethernet, 318–319, 321
  IP (Internet Protocol), 346–347
  physical layer, 522
  segment, 222
encoding
  Manchester, 525–526
  message, 79, 85
  physical layer, 525–526
encryption, 833–834, 862–863
end device, 32–33
endpoint security, 837–839. ***See also*** **firewall**
  antivirus/antimalware, 839
  DLP (data loss prevention), 833
  EDR (endpoint detection and response), 832–833
  HIDS (host intrusion detection system), 832
  HIPS (host intrusion prevention system), 832
  host-based firewall, 832
  host-based security suites, 840–841
  NGFW (next-generation firewall), 833
end-system documentation, 718
enterprise network, 712, 863–864
Ethernet, 102, 272–273, 316–317, 336. ***See also*** **MAC(Media Access Control); multiaccess network**
  broadcast domain, 189–190
  encapsulation, 318–319
  evolution, 317–318
  frame, 104–105, 187, 336–337
    fields, 322–323
    filtering, 333–335
  hub, 106–107
  LLC sublayer, 320, 337
  MAC address, 337–338
    broadcast, 327
    hexadecimal and, 324–326
    multicast, 328–329
    table, 330, 338
    unicast, 326–327
  MAC sublayer, 320, 337
    accessing the media, 321–322
    data encapsulation, 321
  standards, 317–318
  straight-through and crossover cable, 539–540
  supported bandwidths, 319
  switch, 107–108, 112, 330–331
    examining the source MAC address, 331–332
    filtering frames, 333–335
    finding the destination MAC address, 332–333
EUI-64 process, 605–606
Event Viewer, 733–734
external network, 178
external threats, 777–778

F

fault tolerance, 267–268, 275
fiber-optic cable, 63, 95, 549
  connectors, 543–544
  versus copper, 547–548
  multimode, 542

patch cords, 545–547
properties, 541
single-mode, 541–542
usage, 543
fileless malware, 830
FIM (federated identity management), 823–824
firewall, 842, 868–869
application gateway, 844–845
benefits, 843
host-based, 832, 840, 849–850
iptables, 850
limitations, 843
next-generation, 833, 846
nftables, 850
packet-filtering, 843–844, 847–848
properties, 843
stateful, 844–845, 848–849
Windows Defender, 850, 851–854
firmware, 834
flooding, 109–110
ARP broadcast, 382
MAC address, 792–793
flow control, TCP (Transmission Control Protocol), 437–440
follow-the-path troubleshooting, 664–665
FQDN (fully qualified domain name), 392
frame, 103
encapsulation, 203
Ethernet, 104–105, 187, 322–323
filtering, 333–335
frequency bands, wireless network, 61, 69–70
FTP (File Transfer Protocol), 238
full-duplex communication, 562

G

gaming console, 11
goodput, 529
GPS (Global Positioning System), 43
grayware, 794
GUA (global unicast address), 589, 591–592, 615–616
global routing prefix, 592
Interface ID, 593
SLAAC (Stateless Address Autoconfiguration), 601–602
static configuration
on a router, 595–596
on a Windows host, 596–597
Subnet ID field, 592–593

H

half-duplex communication, 562
header
IPv4, 350–352
IPv6, 354–356
TCP, 418–419
UDP (User Datagram Protocol), 420–421
help desk, 723, 725, 766–767. ***See also*** **customer support**
remote desktop, 756–757
sources of help, 683–684
technician, 725–726
trouble ticket, 686–687, 727–729. *See also* information gathering
active listening, 731–732
analyze the information, 737–738
information gathering, 733
know, relate, and understand skill set, 729–730
open-ended user questions, 730–731
question end users, 729
work order, 687
hexadecimal number system, 152, 308–310, 311
converting between decimal and, 326
MAC address and, 324–326
hextet, 153
hierarchical addressing, 119–120
hierarchical network design, 271, 275–276
access layer, 273
core layer, 274
distribution layer, 274
physical and logical addresses, 271–272
hoaxes, 786
home network, 58, 69
authentication, 861–862
components, 58–59
frequency bands, 61
router, 59–60
first time setup, 66–67, 70–71
network mode, 65–66
SSID (Service Set Identifier), 65–66

host reachability message, 500–501
hosted hypervisor, 286–287
host/s, 26, 32–33
 -based firewall, 832, 840, 849–850
 -based security suite, 840–841
 default gateway, 488–490, 574–575
 encryption, 833–834
 external, 178
 forwarding decision, 572–573
 internal, 177–178
 intrusion detection system, 832
 intrusion prevention system, 832
 placing all on a local segment, 206
 placing all on a remote segment, 206–207
 remote, 200
 routing table, 575–576, 582–583
hotspot, 43, 52, 170–171
HTML (Hypertext Markup Language), 237–238
HTTP (Hypertext Transfer Protocol), 237–238
hub
 Ethernet, 106–107
 and spoke topology, 558
hybrid cloud, 283
hypervisor, 286
 Type 1, 286
 Type 2, 286–287

I

IaaS (Infrastructure as a Service), 283, 714
IANA (Internet Assigned Numbers Authority), 134
ICANN (Internet Corporation for Assigned Names and Numbers), 220
ICMPv4 (Internet Control Message Protocol version 4), messages
 Destination Unreachable, 501–502
 host reachability, 500–501
 Time Exceeded, 502
ICMPv6 (Internet Control Message Protocol version 6), 148
 messages, 502, 511–512
  NA (Neighbor Advertisement), 504–505
  NS (Neighbor Solicitation), 504
  RA (Router Advertisement), 503, 599–601
  RS (Router Solicitation), 503–504, 599–601
 ND (Neighbor Discovery), 189
identity, 823
 federated management, 823–824
 fraud, 784
IEEE (Institute of Electrical and Electronics Engineers), 63–64, 317
IETF (Internet Engineering Task Force), 80, 353
ifconfig command, 742
IMAP4 (Internet Message Access Protocol), 243–244
impersonation, 786
information gathering, 733
 beep codes, 733
 BIOS, 733
 for Cisco device-related tickets, 736–737, 750–752
 Device Manager, 734–735
 Event Viewer, 733–734
 Task Manager, 735–736
infrastructure, network, 30–31
interface ID
 EUI-64 process, 605–606
 randomly generated, 606–607
interface vlan 1 command, 478
internal network, 177–178
internal threats, 777–778
Internet. *See also* **connections and connectivity**
 backbone, 34
 connected home devices, 8
  appliances, 9–10
  gaming console, 11
  medical devices, 13–14
  RFID tags, 12
  security system, 8–9
  sensors and actuators, 13
  smart car, 11–12
  smart TV, 10
 ownership, 2–3
 phone calls, 245
 routing IPv4 addresses to the, 131
 speed test, 754
intranet, 205
IOC (indicator of compromise), 783
iOS, 53
 cellular data, 48–49
 troubleshooting connectivity, 746
 Wi-Fi, settings, 44–46
IoT (Internet of Things), 149, 865

IP (Internet Protocol), 104, 217–218
best effort delivery, 348
characteristics, 347
connectionless, 347–348
encapsulation, 346–347
media independence, 349–350
telephony, 245
ip address command, 595–596, 742
ip default-gateway command, 478, 490
ip domain-name command, 494
ipconfig command, 254–255, 395, 606, 674, 738–740
/all option, 255–256
/release option, 256–257
/renew option, 256–257
iperf command, 754–755
iptables, 850
IPv4, 118, 121, 126, 157, 164. *See also*DHCP (Dynamic Host Configuration Protocol); MAC address
address, 369
assignment, 134–135
broadcast transmission, 127–128
classful, 133–134, 141–142
destination on remote network, 187–189
destination on the same network, 186–187
dotted-decimal notation, 119
dynamic assignment, 165–166, 170
hierarchical, 119–120
host number, 119–120
link-local, 133
logical AND, 367–369
loopback, 132, 141
multicast transmission, 129–130
network and host portion, 364
network number, 119–120
octet, 119, 153
private, 130, 131, 179
public, 130, 131
static assignment, 164–165, 170
unicast transmission, 126–127
binary and, 294–296
dotted-decimal notation, 307–308
dual stack, 150
GUA (global unicast address), 593. *See also* GUA (global unicast address)
limitations, 352–353
octet, 294
packet, 350, 358
header fields, 350–352
TTL field, 509–510
routing table, 582
routing to the Internet, 131
subnet/subnetting, 137–138
mask, 164, 365–366
reasons for, 138–140
translation, 151
tunneling, 150–151
IPv6, 130, 157–158, 353–354
address format, 152
double colon, 155–156
hextet, 153
omit leading zeros, 153–154
preferred, 153
anycast address, 588
DHCP (Dynamic Host Configuration Protocol), 399
GUA (global unicast address), 589, 591–592, 615–616. *See also* GUA (global unicast address)
global routing prefix, 592
static configuration on a router, 595–596
static configuration on a Windows host, 596–597
Subnet ID field, 592–593
hexadecimal and, 308–310
LLA (link-local address), 593–595, 616
dynamic, 607–609
static configuration, 598–599
multicast address, 588, 616
assigned, 612–613
solicited node, 614
well-known, 613
native, 150
ND (Neighbor Discovery) protocol, 622
address resolution, 623–624
messages, 622–623
need for, 148–149
packet, 354–356, 358
prefix length, 588–589
unicast address, 588, 589
unique local address, 590
verifying address configuration, 609–612

ipv6 address command, 598
ipv6 unicast-routing command, 600
IRM (information rights management), 817
ISN (initial sequence number), 434
ISP (Internet service provider), 33, 130
connections, 34–35, 38
cable, 35
cellular, 36
dial-up, 36
DSL (Digital Subscriber Line), 35
satellite, 36
services, 33–34
ITaaS (IT as a Service), 283–284

J-K

keylogging, 793–794
keystroke shortcuts, Cisco IOS CLI
exiting a command mode, 462
--More-- prompt, 461–462

L

LACNIC (Latin-American and Caribbean Network Information Centre), 135
LAN (local area network), 205, 209–210, 705
all hosts in one local segment, 206
all hosts on a remote segment, 206–207
legacy topologies, 560–561
threats, 780
virtual, 706
wireless, 706–707
latency, 528–529
Layer 2 attacks
MAC flooding, 792–793
spoofing, 792
layers
OSI reference model, 83, 87
TCP/IP model, 82, 86
LC (Lucent connector) simplex connector, 544
LDAP injection, 798
lease period, DHCP (Dynamic Host Configuration Protocol), 398
LEDs, wireless router, 668–670
limited broadcast, 128
link-local address, 133
link-local command, 598
Linux
iptables, 850
nftables, 850
TCP wrappers, 850
troubleshooting connectivity, 741–743
LLA (link-local address), 589, 616
dynamic, 607–608
on Cisco routers, 609
on Windows, 608
IPv6, 593–595
static configuration, 598–599
LLC (Logical Link Control), 319–320
local network, 3–4, 67
medium to large, 4–5
small home, 4
SOHO (small office/home office), 4–5
logic bomb, 789–790
logical access control, 821
logical address, 186, 193, 271
logical AND, 367–369
logical topology, 556–558, 711
loopback address, 132, 141

M

MAC (Media Access Control)
address, 102, 186, 193, 203, 272
ARP (Address Resolution Protocol), 191–192
broadcast, 327
destination on remote network, 187–189
discoverability, 186–187
filtering, 859
flooding, 792–793
hexadecimal and, 324–326
multicast, 328–329
source/destination, 187, 331–333
table, 108, 109–111, 330, 338
unicast, 326–327
sublayer, 320–322, 337
accessing the media, 321–322
data encapsulation, 321
macOS, troubleshooting connectivity, 740–745
malware. *See also* **attacks**
backdoors, 782–783
fileless, 830

logic bomb, 789–790
ransomware, 790
rootkits, 783
scripts, 830
Trojan horse, 789
virus, 789
worm, 789
MAN (metropolitan area network), 708–709
Manchester encoding, 525–526
man-in-the-middle attack, 793, 856–857
man-in-the-mobile attack, 793
manual configuration, Wi-Fi, 46–47
map, ARP (Address Resolution Protocol), 378, 384
Measured Boot, 834–835
measuring, throughput, 754–755
media, 15, 92
cable
coaxial, 94
fiber-optic, 95
twisted-pair, 93–94
physical connection, 520–522
medium to large network, 4–5
mesh topology, 559
messages
DHCP (Dynamic Host Configuration Protocol), 399–400
DNS (Domain Name System), 395
ICMPv4 (Internet Control Message Protocol version 4), 500
Destination Unreachable, 501–502
host reachability, 500–501
Time Exceeded, 502
ICMPv6 (Internet Control Message Protocol version 6), 511–512
NA (Neighbor Advertisement), 504–505
NS (Neighbor Solicitation), 504
RA (Router Advertisement), 503, 599–601
RS (Router Solicitation), 503–504, 599–601
ND (Neighbor Discovery) protocol, 622–623
Metasploit Project, 799
mobile devices, 6. ***See also*** **Android; iOS**
smart glasses, 8–9
smartphone, 6–7
smartwatch, 8
tablet, 7
Wi-Fi, 44
manual configuration, 46–47
settings, 44–46
MSS (Maximum Segment Size), 439
multiaccess network, 563
contention-based access, 563
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 566–567
CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 564–566
controlled access, 564
multicast address, 2, 141, 328–329, 588, 616
assigned, 612–613
solicited node, 614
well-known, 613
multi-factor authentication, 827
multimode fiber, 542

N

NA (Neighbor Advertisement) message, 504–505
NAT (Network Address Translation), 131, 148, 151, 175, 178, 179–180, 181
native IPv6, 150
ncat command, 742–743
ND (Neighbor Discovery) protocol, 189, 622
address resolution, 623–624
messages, 622–623
netstat command, 223–224, 426–427, 576, 680–682
network layer. ***See also*** **IPv4; IPv6**
characteristics, 357
host forwarding decision, 572–573
IP (Internet Protocol)
best effort delivery, 348
connnectionless, 347–348
encapsulation, 346–347
media independence, 349–350
protocols, 344–345
network/s. ***See also*** **data transmission; IPv4 address; LAN (local area network); routers and routing; wirelessnetwork**
access layer, 104, 112, 273
communication, 191
devices, 105–106
Ethernet frame, 104–105
Ethernet hub, 106–107
Ethernet switch, 107–108

MAC address table, 109–111
protocol, 217
antimalware/antivirus, 841–842
application services, 233, 234–236, 246
architecture, 266–267
automation, 769
baseline performance, 718
boundary, 176, 177–178, 180–181
campus area, 708
communication model/s, 81
OSI, 82–83
TCP/IP, 81–82
core layer, 274
default gateway, 203–204
directly connected, 202
distribution layer, 205, 208, 274
documentation, 704, 765–766
end device, 32–33
enterprise, 712
Ethernet, 272–273
fault tolerance, 267–268, 275
hierarchical design, 271–272, 275–276
home, 58, 69
components, 58–59
router, 59–60
infrastructure, 30–31
internal, 177–178
local, 3–4, 67
medium to large, 4–5
small home, 4
SOHO (small office/home office), 4–5
local area, 205, 209–210, 705
all hosts in one local segment, 206
all hosts on a remote segment, 206–207
management, 763–765
mapping, 723
media, 92
coaxial, 94
fiber-optic, 95
twisted-pair, 93–94
metropolitan area, 708–709
multiaccess, 563
contention-based access, 563
controlled access, 564
number, 119–120
P2P (peer-to-peer), 27–28
personal area, 704–705
protocols, 76–79
QoS (quality of service), 269, 275
redundancy, 267
reliability, 266, 275
scalability, 267–268
security, 270
segmentation, 135–136, 142
broadcast domain, 136–137
problems with large broadcast domains, 137–138
reasons for, 138–140
subnetting, 138–140
topology
device discovery, 720–723
hub and spoke, 558
logical and physical, 556–558, 710–711
mesh, 559
point-to-point, 558, 559–560
virtual private, 710
wide area, 709
wired, 62
Category 5e cable, 62
coaxial, 62–63
fiber-optic, 63
wireless, 42–43
Bluetooth, 43
data transmission, 96
frequency bands, 61
GPS (Global Positioning System), 43
mesh, 707
NFC (Near Field Communication), 43
Wi-Fi, 43
NFC (Near Field Communication), 43, 52
nftables, 850
NGFW (next-generation firewall), 833, 846
NIC (network interface card), 102, 118, 191, 193, 521
NS (Neighbor Solicitation) message, 504
nslookup command, 236, 397, 401, 682–683
number system
binary, 294–296, 311
decimal-to-binary conversion, 296–307
hexadecimal, 308–310, 311

O

octet, 119, 153, 294
"online", 2, 3
open-ended user questions, 730–731
operating system security, 829, 867. *See also* **Android; iOS; Linux; Windows**
- baseline, 830
- boot integrity, 834
- Measured Boot, 834–835
- patch management, 831
- Secure Boot, 834
- systematic approach, 829

OSI reference model, 82–83
- comparison with TCP/IP model, 83–85
- layers, 87
- troubleshooting with, 701

out-of-band management, 644
ownership, Internet, 2–3

P

P2P (peer-to-peer) network, 27–28
PaaS (Platform as a Service), 283, 713–714
packet/s
- capture, 752
- encapsulation, 203
- -filtering, 843–844, 847–848
- forwarding, 576–577
- IP, 201
- IPv4, 350–352, 358
- IPv6, 352, 354–356, 358
- maliciously formatted, 791

pairing, Bluetooth devices, 50–51, 53
PAN (personal area network), 704–705
passphrase, 46, 483
password/s, 824, 825–826
- manager, 826–827
- recommendations, 482–483
- remote access, 484

patch cords, 545–547
patch management, 831
performance, baseline
- network, 718
- operating system, 830

pharming, 803
phishing, 802
physical access control, 820–821
physical address, 271
physical attacks, 804
physical layer
- bandwidth, 527–528
  - *goodput, 529*
  - *latency, 528–529*
  - *throughput, 529*
- characteristics, 548–549
- copper cabling, 529–531
- encapsulation process, 522
- encoding, 525–526
- purpose of, 548
- signaling, 525–527
- standards, 523–524
- troubleshooting, using the senses, 667–668

physical security, 836
physical topology, 556–558, 710–711
piggybacking, 787
ping command, 132, 258–259, 505–506, 512–513,612, 654, 678, 740–741
- default gateway, 507–508
- local loopback, 506
- options, 259–260
- remote host, 508–509
- results, 259

point-to-point topology, 558, 559–560
policy, security, 723–725
POP3 (Post Office Protocol), 243
port/s
- Cisco LAN switch, 632
- numbers, 224, 411, 422–423, 447–448
  - *groups, 424–425*
  - *socket, 423–424*
  - *TCP/UDP, 219–221*
  - *well-known, 221, 425–426*
- private, 221, 225
- registered, 221, 225
- router, 59

POST (power-on self-test), 642
preferred format, IPv6, 153
prefix length, 366–367
on-premises network management, 763–765
pretexting, 784
primary command modes, Cisco IOS CLI, 457–458

private cloud, 283, 781
private IPv4 address, 130, 131, 179
private ports, 221, 225
protocol/s, 76–79. ***See also*** **transport layer**
analysis, 752
application layer, 216
characteristics, 79
connectionless, 415
connection-oriented, 414
email
POP3 (Post Office Protocol), 243
SMTP (Simple Mail Transfer Protocol), 243
model, 82
network access layer, 217
network layer, 344–345
server, 234
sliding windows, 438
stateless, 420
transport layer, 216, 413
TCP (Transmission Control Protocol), 413–414
UDP (User Datagram Protocol), 414–417
public cloud, 282
public IPv4 address, 130, 131

Q-R

QoS (quality of service), 269, 275
quid pro quo attack, 784

RA (Router Advertisement) message, 503, 599–601
SLAAC (Stateless Address Autoconfiguration), 601–602
SLAAC with stateless DHCPv6, 602
stateful DHCPv6, 603–604
radio frequency jamming, 795
randomly generated interface ID, 606–607
ransomware, 790
RDP (Remote Desktop Protocol), 759–760
redundancy, 267
reference model, 82–83
registered ports, 221, 225
reliability, 275
network, 266
TCP (Transmission Control Protocol), 433–437, 448–449
UDP (User Datagram Protocol), 441–442
remote access, 483–485
RDP (Remote Desktop Protocol), 759–760
SSH (Secure Shell), 758–759
enabling, 485–486
verification, 487–488
Telnet, 757–758
using remote desktop applications, 756–757
VPN (virtual private network), 761–763
remote code execution, 799
remote host, 200
reply, ARP (Address Resolution Protocol), 380
request, ARP (Address Resolution Protocol), 379
resource records, 395
RFC
790, "Assigned Numbers", 133
1918, 178
RFI (radio frequency interference), 530–531, 535
RFID tags, 12, 836
RIPE NCC (Réseaux IP Européens Network Coordination Centre), 135
RIR (Regional Internet Registry), 134–135
RJ-45 connector, 62, 537–538
RMON (Remote Network Monitoring), 763
rogue access point, 795, 855–856
rootkit, 783
route print command, 576
routers/routing, 137. ***See also*** **Cisco routers; switches and switching**
AP (access point), 60
authentication, 861–862
back panel, 60
banner configuration, 481
as boundary between networks, 177–178
default gateway, 176, 203–204, 380, 574
DHCP service configuration, 169–170, 177
directly connected networks, 202
documentation, 717
dynamic, 580–581
dynamic LLA (link-local address), 609
first time setup, 66–67, 70–71
as gateway, 176–177
initial configuration steps, 479–480, 493
need for, 200–201, 208
network design considerations, 67–68
network mode, 65–66
packet forwarding process, 576–577

  - ports, 59
  - privileged EXEC mode, 479–480
  - remote access, 483–485
  - saving the configuration, 481
  - security, 481, 482–483, 493–494
  - SSID (Service Set Identifier), 65–66
  - static, 579–580
  - static GUA configuration, 595–596
  - table, 201, 202–203, 209, 575–576,577–578, 582–583
  - wireless, 521, 668–670
- **RS (Router Solicitation) message, 503–504, 599–601**
- **RTT (round-trip time), 509**

S

- **SaaS (Software as a Service), 283, 713**
- **SACK (selective acknowledgment), 435**
- **satellite Internet access, 36**
- **SC (subscriber connector) connector, 544**
- **scalability, network, 267–268**
- **scripts**
  - cross-site, 797
  - malware, 830
- **Secure Boot, 834**
- **security. *See also* attacks; firewall; threat/s**
  - access control
    - *administrative, 821–822*
    - *logical, 821*
    - *physical, 820–821*
  - accounting, 823, 828
  - antimalware/antivirus, 836–837
  - Apple, 835
  - authentication, 822
    - *in the enterprise, 863–864*
    - *multi-factor, 827*
    - *what you have, 824–825*
    - *what you know, 824*
    - *who you are, 825*
  - authorization, 822–823
    - *how to implement, 828*
    - *when to implement, 827–828*
  - biometric, 825
  - CIA triad, 816–817
    - *availability, 818–819*
    - *data confidentiality, 816–817*
    - *data integrity, 817–818*
  - encryption, 862–863
  - endpoint, 837–839
    - *DLP (data loss prevention), 833*
    - *EDR (endpoint detection and response), 832–833*
    - *HIDS (host intrusion detection system), 832*
    - *HIPS (host intrusion prevention system), 832*
    - *host-based firewall, 832, 840*
    - *host-based security suites, 840–841*
    - *NGFW (next-generation firewall), 833*
  - network, 270
  - operating system, 829, 867
    - *baseline, 830*
    - *Measured Boot, 834–835*
    - *Secure Boot, 834*
    - *systematic approach, 829*
  - passwords, 825–827
  - physical, 836
  - policy, 723–725
  - router, 481, 482–483, 493–494
  - system, 8–9
  - wireless, 854, 869–870
    - *authentication, 860–862*
    - *DoS attacks, 854–855*
    - *MAC address filtering, 859*
    - *man-in-the-middle attacks, 856–857*
    - *rogue access points, 855–856*
    - *SSID cloaking and MAC address filtering, 858–859*
- **segmentation, 135–136, 142**
  - all hosts in one local segment, 206
  - broadcast domain, 136–137
  - placing all on a remote segment, 206–207
  - problems with large broadcast domains, 137–138
- **segments, 218, 222**
- **send window, 438**
- **sensor, 13**
- **server/s, 27, 231**
  - DHCP (Dynamic Host Configuration Protocol), 166–167, 177,398, 400
  - DNS (Domain Name System), 235–236
  - email, 242
  - FTP (File Transfer Protocol), 238
  - protocol/s, 234
  - software, 231
  - web, 231, 246–247

shoulder surfing, 786
show arp command, 466
show cdp neighbors command, 720–723
show commands, 463, 750–752
show interfaces command, 464–465
show ip arp command, 381, 385
show ip interface command, 465–466
show ip route command, 467
show ipv6 interface brief command, 610
show ipv6 route command, 611
show protocols command, 467
show running-config command, 463–464, 484
show version command, 468
signal/ing, 15–16
  attenuation, 530
  crosstalk, 530
  physical layer, 525–527
simulation tools, 236
single point of failure, 285
single-mode fiber, 541–542
site-to-site VPN, 760–761
SLAAC (Stateless Address Autoconfiguration), 601–602
sliding windows, 438
small home network, 4
smart appliances, 9–10
smart car, 11–12
smart card, 825
smart glasses, 8–9
smart TV, 10
smartphone, 6–7. *See also* wireless network
smartwatch, 8
SMiShing, 795
SNMP (Simple Network Management Protocol), 763
social engineering, 784–785
socket, 222–223, 423–424
software. *See also* malware
  antimalware/antivirus, 836–837, 850–851, 868
  backdoor, 782–783
  client, 231
  client/server, 27
  firmware, 834
  host-based firewall, 840
  server, 231
  trouble ticketing, 699–700
  unapproved, 830–831
SOHO (small office/home office) network, 4–5
solicited node multicast address, 614
SOP (standard operating procedure), 724
spam, 801–802
spear phishing, 802
speedtest, 742
spoofing, 792
SQL injection, 798
SSH (Secure Shell), 241, 758–759
  enabling, 485–486
  verification, 487–488
SSID (Service Set Identifier), 46, 65–66, 858–859
ST (straight-tip) connector, 543
standards, 316–317
  communication, 80–81, 86
  Ethernet, 317–318
  physical layer, 523–524
  UTP (unshielded twisted-pair), 536, 540
  Wi-Fi, 64
  wireless, 63–64, 70, 714–716
stateful firewall, 844–845, 848–849
stateless protocol, 420
static address assignment, IPv4, 164–165, 170
static routing, 579–580
store-and-forward switching, 635–636
STP (shielded twisted-pair), 533
structured troubleshooting methods, 662, 701–702
  bottom-up, 662–663
  comparison, 665
  divide-and-conquer, 664
  educated guess, 665
  follow-the-path, 664–665
  guidelines for choosing, 665–666
  top-down, 663
subnet/subnetting, 137–138
  logical AND, 367–369
  mask, 164, 365–366
  prefix length, 366–367
  reasons for, 138–140
switches and switching, 112, 136, 630–631. *See also* Cisco LAN switches
  auto-MDIX, 640–641
  autonegotiation, 639
  basic configuration steps, 476–478, 492–493
  connecting to a router, 488
  cut-through, 636–638

default gateway, 490–491
documentation, 717
duplex and speed settings, 638–640
Ethernet, 107–108, 112, 330–331
examining the source MAC address, 331–332
filtering frames, 333–335
finding the destination MAC address, 332–333
management address, 476
memory buffering, 638
remote access, 483–485
enable SSH, 485–486
verify SSH, 487–488
security, password recommendations, 482–483
store-and-forward, 635–636
SVI (switch virtual interface) configuration, 478
syntax, Cisco IOS commands, 459–460
Syntax Checker, 236, 458, 482

T

tablet, 7
tailgating, 787
Task Manager, 735–736
TCP (Transmission Control Protocol), 216, 218, 224,413–414, 447
congestion avoidance, 440
connection establishment, 430–431
features, 417
flow control, 437–440
header, 418–419
ISN (initial sequence number), 434
MSS (Maximum Segment Size), 439
port numbers, 422–423
reliability, 433–437, 448–449
SACK (selective acknowledgment), 435
segments, 218
server processes, 427–430
session termination, 431–432
socket, 222–223
three-way handshake, 432–433
use cases, 415–416, 419
wrappers, 850
TCP/IP model, 81–82
comparison with OSI reference model, 83–85
layers, 86
troubleshooting with, 701
technician, help desk, 725–726
Telnet, 240–241, 757–758
text messaging, 244, 248
threat/s, 805–806. ***See also*** **deception**
advanced persistent, 782
to applications, 781–782
complexity, 782
cyber, 777
to devices, 780
domains, 776–777
intelligence, 783
internal versus external, 777–778
to the LAN, 780
to the private cloud, 781
to the public cloud, 781
user, 778–779
three-way handshake, 432–433
throughput, 18, 529, 754–755
ticketing system. ***See*** **help desk**
timing, communication, 79, 85
TKIP (Temporal Key Integrity Protocol), 862
tools, simulation, 236
top-down troubleshooting, 663
top-level domains, 396
topology, 568
device discovery, 720–723
enterprise network, 712
LAN, 560–561
logical, 556–558, 711
physical, 556–558, 710–711
WAN
hub and spoke, 558
mesh, 559
point-to-point, 558, 559–560
traceroute command, 509, 513, 678–680, 741
IPv4 TTL and IPv6 hop limit, 509–510
RTT (round-trip time), 509
transport layer, 216, 408, 413. ***See also*** **TCP (Transmission Control Protocol); UDP (User Datagram Protocol)**
datagram, 409
responsibilities, 409–412
role of, 408
TCP (Transmission Control Protocol), 218, 413–414, 447
congestion avoidance, 440

connection establishment, 430–431
features, 417
flow control, 437–440
header, 418–419
ISN (initial sequence number), 434
MSS (Maximum Segment Size), 439
port numbers, 422–423
reliability, 433–437, 448–449
SACK (selective acknowledgment), 435
server processes, 427–430
session termination, 431–432
three-way handshake, 432–433
use cases, 415–416, 419
UDP (User Datagram Protocol), 218–219, 414–417, 420, 447,449
client processes, 443–445
datagram reassembly, 441–442
features, 420
low overhead, 441–442
port numbers, 219–221, 422–423
reliability, 441–442
server processes and requests, 443
use cases, 415–416, 421–422
Trojan horse, 789
troubleshooting, 261, 654, 699–700, 725, 727–729. *See also* **command/s; documentation; help desk**
active listening, 731–732
analyze information, 700, 737–738
cable issues, 670
connectivity, 689–690
on Android, 747–749
DHCP server configuration errors, 674–675
ipconfig command, 254–257, 738–740
on Linux, 741–743
on macOS, 740–745
netstat command, 223–224
ping command, 258–260, 505–506,506, 507–509, 740–741
traceroute command, 741
define the problem, 699–700
documentation, 703–704
eliminate possible causes, 700
information gathering, 660–661, 700, 733
beep codes, 733
BIOS, 733
for Cisco device-related tickets, 736–737
Device Manager, 734–735
Event Viewer, 733–734
Task Manager, 735–736
know, relate, and understand skill set, 729–730
with layered models, 701
open-ended user questions, 730–731
physical layer, 667–668, 688–689
propose hypothesis, 700
question end users, 729
security policy, 723–725
selecting a method, 702
solve the problem, 700
structured methods, 662, 701–702
bottom-up, 662–663
comparison, 665
divide-and-conquer, 664
educated guess, 665
follow-the-path, 664–665
guidelines for choosing, 665–666
top-down, 663
test hypothesis, 700
wireless network, 671–673, 689
tunneling, 150–151
twisted-pair cable, 93–94
two-factor authentication, 825
Type 1 hypervisor, 286
Type 2 hypervisor, 286–287

U

UDP (User Datagram Protocol), 216, 218–219, 224,420, 447, 449
client processes, 443–445
datagram reassembly, 441–442
features, 420
header, 420–421
low overhead, 441–442
port numbers, 219–221, 422–423
reliability, 441–442
server processes and requests, 443
socket, 222–223
use cases, 415–416, 421–422
UEFI (Unified Extensible Firmware Interface), 834
unicast address, 126–127, 326–327, 588
URI (Uniform Resource Identifier), 232–233
URL (Uniform Resource Locator), 232, 246, 792

URN (Uniform Resource Name), 232, 246
UTP (unshielded twisted-pair), 62, 531–532, 549
categories, 536–537
connectors, 537–539
properties, 535–536
standards, 536, 540
straight-through and crossover, 539–540

V

virtual terminals, 239, 247
SSH (Secure Shell), 241
Telnet, 240–241
virtualization, 284–285
advantages, 285, 288–289
hypervisor, 286
Type 1, 286
Type 2, 286–287
virus, 789
vishing, 802–803
VLAN (virtual LAN), 706
VMware, 284
VoIP (voice over IP), 245
VPN (virtual private network), 710, 760
remote-access, 761–763
site-to-site, 760–761
vty (virtual terminal), 484

W

WAN (wide area network), 709
topology
hub and spoke, 558
mesh, 559
point-to-point, 558, 559–560
web server, 231, 246–247
URI (Uniform Resource Identifier), 232–233
URL (Uniform Resource Locator), 232
well-known port numbers, 221, 225, 425–426
WEP (Wired Equivalent Privacy), 796
whaling, 803
Wi-Fi, 43
attacks, 796
and mobile defense, 797
mobile devices, 44
manual configuration, 46–47
settings, 44–46
standards, 64
Wi-Fi Alliance, 64
Windows. ***See also*** **command/s**
Defender Firewall, 850, 851–854
dynamic LLA (link-local address), 608
ipconfig command, 674, 738–740
ping command, 678, 740–741
static GUA configuration, 596–597
wired network, 62
cable
Category 5e, 62
coaxial, 62–63
fiber-optic, 63
router
first time setup, 66–67
network design considerations, 67–68
wireless network, 42–43, 52, 807–808. ***See also*** **home network**
AP (access point), 520, 795
Bluetooth, 43, 49–50
pairing, 50–51
use cases, 50
cellular data, 47
for Android, 47–48
for iOS, 48–49
data transmission, 96
encryption, 862–863
frequency bands, 61, 69–70
GPS (Global Positioning System), 43
hotspot, 170–171
licensed and unlicensed bands, 716
NFC (Near Field Communication), 43
radio frequency jamming, 795
routers, 521, 668–670
security, 854, 860–861, 869–870
authentication, 860–862, 863–865
DoS attacks, 854–855
MAC address filtering, 859
man-in-the-middle attacks, 856–857
rogue access points, 855–856
SSID cloaking and MAC address filtering, 858–859
standards, 63–64, 70, 714–716

troubleshooting, 671–673, 689
Wi-Fi, 43
manual configuration, 46–47
mobile devices and, 44
settings, 44–46
Wireshark, 752
WLAN (wireless LAN), 706–707
WMN (wireless mesh network), 707
work order, 687
World Wide Web, 236
WPA2-Enterprise, 863
WPA3, 864–865

X-Y-Z

XaaS (anything/everything as a service), 714
XML injection, 798

zero-day attack, 793