



Networking Essentials

Companion Guide



FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Networking Essentials Companion Guide

Cisco Networking Academy

Cisco Press

Networking Essentials Companion Guide

Cisco Networking Academy

Copyright © 2022 Cisco Systems, Inc.

Published by:
Cisco Press

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.

ScoutAutomatedPrintCode

Library of Congress Control Number: 2021952296

ISBN-13: 978-0-13-766048-3

ISBN-10: 0-13-766048-0

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.

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

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.

Editor-in-Chief

Mark Taub

Alliances Manager,

Cisco Press

Arezou Gol

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

Chuck Hutchinson

Technical Editor

Dave Holzinger

Editorial Assistant

Cindy Teeters

Cover Designer

Chuti Prasertsith

Composition

codeMantra

Indexer

Tim Wright

Proofreader

Donna Mulder

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



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.



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)

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

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

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, 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.

About the Technical Reviewers

Dave Holzinger has been a curriculum developer, project manager, author, and technical editor for the Cisco Networking Academy Program in Phoenix, Arizona, since 2001. Dave works on the team that develops their online curricula including CCNA, CCNP, and IT Essentials. He has been working with computer hardware and software since 1981. Dave has certifications from Cisco, BICSI, and CompTIA.

Contents at a Glance

	Introduction	xxvii
Chapter 1	Communications in a Connected World	1
Chapter 2	Online Connections	31
Chapter 3	Explore Networks with Packet Tracer	49
Chapter 4	Build a Simple Network	67
Chapter 5	Communication Principles	89
Chapter 6	Network Design and the Access Layer	111
Chapter 7	Routing Between Networks	137
Chapter 8	The Internet Protocol	157
Chapter 9	Dynamic Addressing with DHCP	181
Chapter 10	IPv4 and IPv6 Address Management	193
Chapter 11	Transport Layer Services	211
Chapter 12	Application Layer Services	229
Chapter 13	Build a Home Network	249
Chapter 14	Connect to the Internet	271
Chapter 15	Security Considerations	299
Chapter 16	Configure Network and Device Security	325
Chapter 17	Cisco Switches and Routers	349
Chapter 18	The Cisco IOS Command Line	373
Chapter 19	Build a Small Cisco Network	391
Chapter 20	Troubleshoot Common Network Problems	415

Appendix A **Answers to the “Check Your Understanding” Questions** **459**

Glossary **471**

Index **491**

Contents

Introduction xxvii

Chapter 1 Communications in a Connected World 1

Objectives 1

Key Terms 1

Introduction (1.0) 2

Network Types (1.1) 3

Everything Is Online (1.1.1) 3

Who Owns “The Internet”? (1.1.2) 3

Local Networks (1.1.3) 3

Small Home Networks 4

Small Office and Home Office Networks 4

Medium to Large Networks 6

Worldwide Networks 6

Mobile Devices (1.1.5) 7

Smartphone 7

Tablet 8

Smartwatch 8

Smart Glasses 9

Connected Home Devices (1.1.6) 10

Security System 10

Appliances 10

Smart TV 11

Gaming Console 12

Other Connected Devices (1.1.7) 12

Smart Cars 12

RFID Tags 13

Sensors and Actuators 14

Medical Devices 14

Data Transmission (1.2) 15

Types of Personal Data (1.2.2) 15

Common Methods of Data Transmission (1.2.4) 16

Bandwidth and Throughput (1.3) 17

Bandwidth (1.3.1) 17

Throughput (1.3.3) 18

Clients and Servers (1.4) 19

Client and Server Roles (1.4.1) 19

- Peer-to-Peer Networks (1.4.2) 20
- Peer-to-Peer Applications (1.4.3) 21
- Multiple Roles in the Network (1.4.4) 22

Network Components (1.5) 23

- Network Infrastructure (1.5.2) 23
- End Devices (1.5.3) 25

Summary (1.6) 26

Practice 27

Check Your Understanding 27

Chapter 2 Online Communications 31

Objectives 31

Key Terms 31

Introduction (2.0) 32

Wireless Networks (2.1) 32

- Mobile Telephones (2.1.2) 32
- Cell Phone Network (2.1.3) 32
- Other Wireless Networks (2.1.5) 33
 - Global Positioning System (GPS)* 33
 - Wi-Fi* 34
 - Bluetooth* 34
 - Near-Field Communication* 34

Local Network Connections (2.2) 34

- LAN Components (2.2.2) 34
 - Hosts* 35
 - Peripherals* 35
 - Network Devices* 36
 - Network Media* 37
- End Device Addressing (2.2.4) 39
- Manual and Automatic Address Assignment (2.2.6) 40
 - Manual IP Configuration* 40
 - Dynamic IP Configuration* 41

Network Documentation (2.3) 41

- Device Names and Address Planning (2.3.1) 41
- Network Topologies and Representations (2.3.2) 42
- Logical Network Information (2.3.4) 43

Summary (2.4) 45

	Practice	46
	Check Your Understanding Questions	46
Chapter 3	Explore Networks with Packet Tracer	49
	Objectives	49
	Key Terms	49
	Introduction (3.0)	50
	Packet Tracer Network Simulator (3.1)	50
	Packet Tracer Installation (3.2)	50
	The Packet Tracer User Interface (3.3)	51
	Locate and Deploy Devices (3.3.2)	52
	Packet Tracer Network Configuration (3.4)	53
	GUI and CLI Configuration in Packet Tracer (3.4.2)	54
	<i>Physical Tab</i>	54
	<i>Config Tab</i>	55
	<i>CLI Tab</i>	56
	<i>Desktop Tab</i>	56
	<i>Services Tab</i>	57
	Summary (3.5)	59
	Practice	61
	Packet Tracer Activities	61
	Check Your Understanding Questions	61
Chapter 4	Build a Simple Network	67
	Objectives	67
	Key Terms	67
	Introduction (4.0.1)	68
	Network Media Types (4.1)	68
	Three Media Types (4.1.2)	68
	Common Network Cables (4.1.3)	69
	<i>Twisted-Pair Cable</i>	69
	<i>Coaxial Cable</i>	70
	<i>Fiber-Optic Cable</i>	70
	Ethernet Cabling (4.2)	71
	Twisted-Pair Cables (4.2.1)	71
	Types of Twisted-Pair Cables (4.2.2)	72
	<i>UTP Cable</i>	73
	<i>STP Cable</i>	74

Coaxial and Fiber-Optic Cabling (4.3) 75

Cable TV and Satellite Cables (4.3.1) 75

Fiber-Optic Cables (4.3.2) 76

Twisted-Pair Operation (4.4) 78

Twisted-Pair Wiring Schemes (4.4.1) 78

Twisted-Pair Transmit and Receive Pairs (4.4.2) 79

Verify Connectivity (4.5) 79

Using the ping Command (4.5.2) 80

The traceroute Command (4.5.3) 81

Summary (4.6) 83

Practice 85

Labs 85

Check Your Understanding Questions 85

Chapter 5

Communication Principles 89

Objectives 89

Key Terms 89

Introduction (5.0.1) 90

The Rules (5.1) 90

The Three Elements (5.1.1) 90

Communication Protocols (5.1.2) 91

Why Protocols Matter (5.1.3) 93

Communication Standards (5.2) 95

The Internet and Standards (5.2.2) 95

Network Standards Organizations (5.2.3) 95

Network Communication Models (5.3) 96

The Protocol Stack (5.3.3) 97

The TCP/IP Model (5.3.4) 98

The OSI Reference Model (5.3.5) 99

Upper and Lower Layers of the OSI Model (5.3.6) 100

OSI Model and TCP/IP Model Comparison (5.3.7) 101

Ethernet (5.4) 103

The Rise of Ethernet (5.4.1) 103

Ethernet Evolution (5.4.2) 104

The Ethernet MAC Address (5.4.4) 105

	Summary (5.5)	107
	Practice	108
	Labs	108
	Check Your Understanding Questions	108
Chapter 6	Network Design and the Access Layer	111
	Objectives	111
	Key Terms	111
	Introduction (6.0.1)	112
	Encapsulation and the Ethernet Frame (6.1)	112
	Encapsulation (6.1.2)	112
	Ethernet Frame (6.1.3)	114
	Hierarchical Network Design (6.2)	115
	Physical and Logical Addresses (6.2.2)	115
	Hierarchical Analogy (6.2.5)	117
	Benefits of a Hierarchical Design (6.2.7)	117
	Access, Distribution, and Core (6.2.8)	119
	<i>Access Layer</i>	119
	<i>Distribution Layer</i>	119
	<i>Core Layer</i>	120
	The Access Layer (6.3)	120
	Access Layer Devices (6.3.1)	121
	Ethernet Hubs (6.3.2)	121
	Ethernet Switches (6.3.4)	123
	The MAC Address Table (6.3.6)	124
	Broadcast Containment (6.4)	126
	Ethernet Broadcasts in the Local Network (6.4.2)	126
	Broadcast Domains (6.4.3)	127
	Access Layer Communication (6.4.4)	128
	ARP (6.4.6)	129
	Summary (6.5)	131
	Practice	133
	Labs	133
	Check Your Understanding Questions	133

Chapter 7	Routing Between Networks	137
	Objectives	137
	Key Terms	137
	Introduction (7.0.1)	138
	The Need for Routing (7.1)	138
	Criteria for Dividing the Local Network (7.1.2)	138
	<i>Broadcast Containment</i>	138
	<i>Security Requirements</i>	139
	<i>Physical Locations</i>	140
	<i>Logical Grouping</i>	140
	When Routing Is Needed (7.1.3)	141
	The Routing Table (7.2)	142
	Path Selection (7.2.2)	142
	Packet Forwarding (7.2.5)	143
	Routing Table Entries (7.2.7)	145
	The Default Gateway (7.2.8)	146
	Create a LAN (7.3)	147
	Local-Area Networks (7.3.1)	147
	Local and Remote Network Segments (7.3.2)	148
	<i>All Hosts in One Local Segment</i>	148
	<i>Hosts on a Remote Segment</i>	149
	Summary (7.4)	152
	Practice	153
	Labs	153
	Packet Tracer Activities	153
	Check Your Understanding Questions	153
Chapter 8	The Internet Protocol	157
	Objectives	157
	Key Terms	157
	Introduction (8.0.1)	158
	Purpose of the IPv4 Address (8.1)	158
	The IPv4 Address (8.1.1)	158
	Binary Conversion of an IPv4 Address (8.2)	159
	IPv4 Addressing (8.2.1)	159
	Binary to Decimal (8.2.3)	160

The IPv4 Address Structure (8.3) 162

Networks and Hosts (8.3.2) 162

Logical AND (8.3.5) 163

Calculate Whether the Destination Is Local or Remote
(8.3.6) 164

Calculate the Number of Hosts (8.3.7) 165

Classful IPv4 Addressing (8.4) 166

Classful and Classless Addressing (8.4.1) 166

Public and Private IPv4 Addresses (8.5) 168

Private IPv4 Addressing (8.5.1) 168

Assignment of IPv4 Addresses (8.5.2) 169

Unicast, Broadcast, and Multicast Addresses (8.6) 171

Unicast Transmission (8.6.2) 171

Broadcast Transmission (8.6.4) 172

Multicast Transmission (8.6.6) 173

Summary (8.7) 175**Practice 177**

Labs 177

Packet Tracer Activities 177

Check Your Understanding Questions 177**Chapter 9 Dynamic Addressing with DHCP 181****Objectives 181****Key Terms 181****Introduction (9.0.1) 182****Static and Dynamic Addressing (9.1) 182**

Static IPv4 Address Assignment (9.1.1) 182

Dynamic IPv4 Address Assignment (9.1.2) 183

DHCP Servers (9.1.3) 184

DHCPv4 Configuration (9.2) 185

DHCPv4 Operation (9.2.2) 185

DHCP Service Configuration (9.2.4) 186

Summary (9.3) 188**Practice 189**

Packet Tracer Activities 189

Check Your Understanding Questions 189

Chapter 10	IPv4 and IPv6 Address Management	193
	Objectives	193
	Key Terms	193
	Introduction (10.0.1)	194
	Network Boundaries (10.1)	194
	Routers as Gateways (10.1.2)	194
	Routers as Boundaries Between Networks (10.1.3)	195
	Network Address Translation (10.2)	196
	NAT Operation (10.2.2)	196
	IPv4 Issues (10.3)	198
	Need for IPv6 (10.3.1)	198
	<i>Internet of Things</i>	200
	IPv6 Address Size (10.3.2)	200
	IPv4 and IPv6 Coexistence (10.3.4)	201
	<i>Dual Stack</i>	201
	<i>Tunneling</i>	202
	<i>Translation</i>	203
	IPv6 Features (10.4)	203
	IPv6 Autoconfiguration and Link-Local Addresses (10.4.3)	203
	IPv6 Address Representation (10.4.5)	204
	<i>Compressing IPv6 Addresses</i>	204
	<i>Rule 1: Omit Leading Zeros</i>	205
	<i>Rule 2: Omit One “All Zero” Segment</i>	205
	Summary (10.5)	206
	Practice	207
	Labs	207
	Packet Tracer Activities	207
	Check Your Understanding Questions	208
Chapter 11	Transport Layer Services	211
	Objectives	211
	Key Terms	211
	Introduction (11.0.1)	212
	The Client/Server Relationship (11.1)	212
	Client and Server Interaction (11.1.1)	212
	Client Requests a Web Page (11.1.3)	213
	URI, URN, and URL (11.1.4)	214

TCP and UDP (11.2) 215

- Protocol Operations (11.2.1) 215
- TCP and UDP (11.2.3) 216
- TCP Reliability (11.2.4) 216
- UDP Best Effort Delivery (11.2.5) 217

Port Numbers (11.3) 218

- TCP and UDP Port Numbers (11.3.2) 218
- Destination and Source Port Numbers (11.3.3) 220
 - Source Port* 220
 - Destination Port* 221
- Socket Pairs (11.3.4) 221
- The netstat Command (11.3.5) 223

Summary (11.4) 224**Practice 225**

- Packet Tracer Activities 225

Check Your Understanding Questions 225**Chapter 12 Application Layer Services 229****Objectives 229****Key Terms 229****Introduction (12.0.1) 230****Network Application Services (12.1) 230**

- Common Network Application Services (12.1.1) 230

Domain Name System (12.2) 231

- Domain Name Translation (12.2.1) 231
- DNS Servers (12.2.3) 232

Web Clients and Servers (12.3) 233

- HTTP and HTML (12.3.2) 233

FTP Clients and Servers (12.4) 234

- File Transfer Protocol (12.4.1) 235
- FTP Client Software (12.4.3) 236

Virtual Terminals (12.5) 237

- Telnet (12.5.2) 237
- Security Issues with Telnet (12.5.3) 238

Email and Messaging (12.6) 239

- Email Clients and Servers (12.6.1) 239
- Email Protocols (12.6.2) 240
 - Simple Mail Transfer Protocol (SMTP)* 240
 - Post Office Protocol (POP3)* 241
 - Internet Message Access Protocol (IMAP4)* 241
- Text Messaging (12.6.3) 242
- Internet Phone Calls (12.6.4) 243

Summary (12.7) 244

Practice 246

- Labs 246
- Packet Tracer Activities 246

Check Your Understanding Questions 246

Chapter 13 Build a Home Network 249

Objectives 249

Key Terms 249

Introduction (13.0.1) 250

Home Network Basics (13.1) 250

- Connecting Home Devices (13.1.1) 250
- Components of a Home Network (13.1.2) 251
- Typical Home Network Routers (13.1.3) 252

Network Technologies in the Home (13.2) 253

- The Electromagnetic Spectrum (13.2.1) 253
- LAN Wireless Frequencies (13.2.2) 254
- Wired Network Technologies (13.2.3) 255
 - Category 5e Cable* 256
 - Coaxial Cable* 256
 - Ethernet over Powerline* 256

Wireless Standards (13.3) 257

- Wi-Fi Networks (13.3.1) 257
- Wireless Settings (13.3.2) 257

Wireless Traffic Controls (13.4) 259

- Wireless Channels (13.4.1) 259
- Wireless as a Shared Media (13.4.2) 260

Set Up a Home Router (13.5) 261

- First Time Setup (13.5.1) 261

	Design Considerations (13.5.2)	261
	MAC Address Filtering (13.5.3)	263
	Summary (13.6)	265
	Practice	267
	Labs	267
	Check Your Understanding Questions	267
Chapter 14	Connect to the Internet	271
	Objectives	271
	Key Terms	271
	Introduction (14.0.1)	272
	ISP Connectivity Options (14.1)	272
	ISP Services (14.1.1)	272
	ISP Connections (14.1.2)	273
	Cable and DSL Connections (14.1.3)	274
	Additional Connectivity Options (14.1.4)	275
	Network Virtualization (14.2)	276
	Cloud Computing (14.2.2)	276
	Types of Clouds (14.2.3)	276
	Cloud Services (14.2.4)	277
	Cloud Computing and Virtualization (14.2.5)	277
	Advantages of Virtualization (14.2.6)	279
	Hypervisors (14.2.7)	279
	<i>Type 1 Hypervisors</i>	279
	<i>Type 2 Hypervisor</i>	280
	Network Virtualization (14.2.9)	281
	Control Plane and Data Plane (14.2.10)	282
	Network Virtualization and SDN (14.2.11)	283
	SDN Architecture (14.2.12)	283
	Mobile Device Connectivity (14.3)	284
	Mobile Devices and Wi-Fi (14.3.1)	284
	Wi-Fi Settings (14.3.2)	285
	Configure Mobile Wi-Fi Connectivity (14.3.3)	286
	Configure Cellular Data Settings (14.3.4)	288
	<i>Android Cellular Data</i>	288
	<i>iOS Cellular Data</i>	289

Simple Connectivity with Bluetooth (14.3.6) 290

Bluetooth Pairing (14.3.7) 290

Summary (14.4) 293

Practice 295

Labs 295

Check Your Understanding Questions 295

Chapter 15 Security Considerations 299

Objectives 299

Key Terms 299

Introduction (15.0.1) 300

Security Threats (15.1) 300

Types of Threats (15.1.1) 300

Internal and External Threats (15.1.2) 301

Internal Threats 301

External Threats 302

Social Engineering Attacks (15.2) 302

Overview of Social Engineering (15.2.1) 302

Types of Social Engineering Attacks (15.2.2) 303

Pretexting 303

Phishing 303

Vishing/Phone Phishing 304

Malware (15.3) 304

Malicious Software (15.3.1) 305

Types of Malware (15.3.2) 305

Viruses 305

Worms 305

Trojan Horses 305

Spyware (15.3.3) 306

Spyware 306

Tracking Cookies 306

Adware and Popups (15.3.4) 306

Botnets and Zombies (15.3.5) 307

Denial-of-Service Attacks (15.4) 308

Denial of Service (15.4.1) 308

Distributed Denial of Service (15.4.2) 309

Brute Force (15.4.3) 310

	Security Tools (15.5)	310
	Security Practices and Procedures (15.5.1)	310
	Security Tools and Applications (15.5.2)	312
	Patches and Updates (15.5.3)	313
	Antimalware Software (15.6)	314
	Signs of Infections (15.6.1)	314
	Antivirus Software (15.6.2)	315
	Antispam Software (15.6.3)	316
	Antispyware Software (15.6.4)	316
	<i>Antispyware and Adware</i>	317
	<i>Popup Blockers</i>	317
	Additional Safeguards (15.6.5)	317
	Summary (15.7)	318
	Practice	321
	Labs	321
	Check Your Understanding Questions	321
Chapter 16	Configure Network and Device Security	325
	Objectives	325
	Key Terms	325
	Introduction (16.0.1)	326
	Wireless Security Measures (16.1)	326
	Wireless Vulnerabilities (16.1.1)	326
	A Comprehensive Security Plan (16.1.2)	327
	SSID Broadcasts (16.1.4)	333
	Changing Default Settings (16.1.5)	334
	MAC Address Filtering (16.1.6)	335
	Implement Wireless Security (16.2)	336
	Open Authentication (16.2.1)	336
	Authentication and Association (16.2.2)	336
	Authentication Protocols (16.2.3)	337
	Configure a Firewall (16.3)	338
	Firewall Overview (16.3.1)	338
	Firewall Operation (16.3.2)	338
	The DMZ (16.3.3)	339
	Port Forwarding (16.3.4)	340

Port Triggering (16.3.5) 341

Summary (16.4) 344

Practice 345

Labs 345

Packet Tracer Activities 346

Check Your Understanding Questions 346

Chapter 17 Cisco Switches and Routers 349

Objectives 349

Key Terms 349

Introduction (17.0.1) 350

Cisco Switches (17.1) 350

Connect More Devices (17.1.1) 350

Cisco LAN Switches (17.1.2) 351

Type of Port 352

Speed Required 352

Expandability 353

Manageability 353

LAN Switch Components (17.1.5) 354

Switch Boot Process (17.2) 355

Power Up the Switch (17.2.1) 355

In-Band and Out-of-Band Management (17.2.3) 358

In-Band Management 358

Out-of-Band Management 358

IOS Startup Files (17.2.4) 358

Cisco Routers (17.3) 359

Router Components (17.3.2) 360

Router Interface Ports (17.3.3) 360

Router Boot Process (17.4) 361

Power Up the Router (17.4.1) 361

Management Ports (17.4.2) 365

Summary (17.5) 367

Practice 368

Packet Tracer Activities 368

Check Your Understanding Questions 368

Chapter 18	The Cisco IOS Command Line	373
	Objectives	373
	Key Terms	373
	Introduction (18.0.1)	374
	Navigate the IOS (18.1)	374
	The Cisco IOS Command-Line Interface (18.1.1)	374
	Primary Command Modes (18.1.2)	375
	A Note About Syntax Checker Activities (18.1.5)	376
	The Command Structure (18.2)	376
	Basic IOS Command Structure (18.2.1)	376
	IOS Command Syntax (18.2.2)	377
	Hotkeys and Shortcuts (18.2.4)	378
	View Device Information (18.3)	380
	Show Commands (18.3.2)	381
	Summary (18.4)	387
	Practice	388
	Packet Tracer Activities	388
	Check Your Understanding Questions	388
Chapter 19	Build a Small Cisco Network	391
	Objectives	391
	Key Terms	391
	Introduction (19.0.1)	392
	Basic Switch Configuration (19.1)	392
	Basic Switch Configuration Steps (19.1.1)	392
	Switch Virtual Interface Configuration (19.1.2)	394
	Configure Initial Router Settings (19.2)	395
	Basic Router Configuration Steps (19.2.1)	395
	Basic Router Configuration Example (19.2.2)	396
	Secure the Devices (19.3)	398
	Password Recommendations (19.3.1)	398
	Secure Remote Access (19.3.2)	399
	Configure SSH (19.3.3)	400
	Verify SSH (19.3.5)	402

Connecting the Switch to the Router (19.4) 404

Default Gateway for a Host (19.4.1) 404

Default Gateway on a Switch (19.4.2) 406

Summary (19.5) 409

Practice 411

Packet Tracer Activities 411

Check Your Understanding Questions 412

Chapter 20 Troubleshoot Common Network Problems 415

Objectives 415

Key Terms 415

Introduction (20.0.1) 416

The Troubleshooting Process (20.1) 416

Network Troubleshooting Overview (20.1.1) 416

Gather Information (20.1.2) 416

Structured Troubleshooting Methods (20.1.3) 418

Bottom-Up 418

Top-Down 419

Divide-and-Conquer 420

Follow-the-Path 420

Substitution 421

Comparison 421

Educated Guess 421

Guidelines for Selecting a Troubleshooting Method (20.1.4) 422

Physical Layer Problems (20.2) 423

Common Layer 1 Problems (20.2.1) 423

The Sense of Sight 423

The Senses of Smell and Taste 424

The Sense of Touch 424

The Sense of Hearing 424

Wireless Router LEDs (20.2.2) 424

Cabling Problems (20.2.3) 426

Troubleshooting Commands (20.3) 426

Overview of Troubleshooting Commands (20.3.1) 426

The ipconfig Command (20.3.2) 427

The ping Command (20.3.4) 430

Ping Results (20.3.5) 431

Divide and Conquer with ping (20.3.7) 432

	The tracert Command (20.3.8)	433
	The netstat Command (20.3.9)	434
	The nslookup Command (20.3.10)	436
	Troubleshoot Wireless Issues (20.4)	438
	Causes of Wireless Issues (20.4.1)	438
	Authentication and Association Errors (20.4.2)	439
	Common Internet Connectivity Issues (20.5)	441
	DHCP Server Configuration Errors (20.5.1)	441
	Check Internet Configuration (20.5.2)	442
	Check Firewall Settings (20.5.3)	444
	Customer Support (20.6)	444
	Sources of Help (20.6.1)	445
	When to Call for Help (20.6.2)	445
	Support Desk Interaction (20.6.3)	446
	Issue Resolution (20.6.4)	447
	Support Desk Tickets and Work Orders (20.6.5)	448
	Summary (20.7)	450
	Practice	453
	Labs	453
	Packet Tracer Activities	453
	Check Your Understanding Questions	454
Appendix A	Answers to the “Check Your Understanding” Questions	459
	Glossary	471
	Index	491

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 is the official supplemental textbook for the Cisco Networking Academy Networking Essentials version 2 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.

This book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. The 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.

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 self-paced. The primary emphasis is on networking knowledge with a small amount of basic skills that are useful for a home or a small office/home office (SOHO) network. The online version of this course 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 you complete the course in an instructor-led class.

Online Course Enrollment

The online version of Networking Essentials version 2 is offered in two ways: self-paced or instructor led:

- To enroll for free in a self-paced version of Networking Essentials, visit <https://skillsforall.com/course/networking-essentials>.
- To find a location near you that offers instructor-led Cisco Networking Academy courses, visit https://www.netacad.com/portal/netacad_academy_search.

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 short sidebars point out interesting facts, time-saving 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 chapter, there is a full list of all the labs, class activities, and Packet Tracer activities to refer 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. This handy reference enables you to find a term, flip to the page where the term appears, and see the term used in context.
- **Glossary:** The Glossary defines all the highlighted key terms plus more.

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:

- **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.



Interactive
Graphic

Video

- **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, a practice section collects a list of all the labs and activities to provide practice with the topics introduced in this chapter.
- **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 20 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, “Communications in a Connected World”:** This chapter explains the concept of network communication including the concept of a network, network data, network speed and capacity, the role of clients and servers, and the role of network infrastructure devices.
- **Chapter 2, “Online Connections”:** This chapter explains the basic requirements for getting online, including the different types of networks used by cell phones and mobile devices, the requirements for host connectivity, and the importance of network documentation.

- **Chapter 3, “Explore Networks with Packet Tracer”:** This chapter explains how to create a simulated network using Packet Tracer, including the purpose and function of Packet Tracer, installing Packet Tracer on a local device, investigating the Packet Tracer user interface, configuring a Packet Tracer network, and creating a simulated network in Packet Tracer.
- **Chapter 4, “Build a Simple Network”:** This chapter explains how to build a simple home network with common types of network cables including Ethernet twisted-pair, coaxial, and fiber-optic cabling. Also included is an explanation of how a twisted-pair cable transmits and receives signals. Finally, the chapter explains how to verify connectivity in a simple routed network.
- **Chapter 5, “Communication Principles”:** This chapter explains the importance of standards and protocols in network communications, including network communication protocols and standards, the OSI and TCP/IP models, and the functions of Layer 1 and Layer 2 in an Ethernet network
- **Chapter 6, “Network Design and the Access Layer”:** This chapter explains how communication occurs on Ethernet networks and describes the process of encapsulation and Ethernet framing, the function at each layer of the three-layer network design model, how to improve network communication at the access layer, and why it is important to contain broadcasts within a network.
- **Chapter 7, “Routing Between Networks”:** This chapter explains how to configure devices on a LAN and the need for routing, as well as how routers use tables. The chapter then explains how to build a fully connected network.
- **Chapter 8, “The Internet Protocol”:** This chapter explains the features of an IP address, including the purpose of an IPv4 address, how to calculate numbers between decimal and binary systems, how IPv4 addresses and subnets are used together; the different IPv4 address classes; public and private IPv4 address ranges; and unicast, multicast, and broadcast addresses.
- **Chapter 9, “Dynamic Addressing with DHCP”:** This chapter explains static and dynamic IPv4 addressing and how to configure a DHCPv4 server to dynamically assign IPv4 addresses.
- **Chapter 10, “IPv4 and IPv6 Address Management”:** This chapter explains the principles of IPv4 and IPv6 address management, including network boundaries, the purpose of Network Address Translation in small networks, why IPv6 addressing will replace IPv4 addressing, and some of the features of IPv6.
- **Chapter 11, “Transport Layer Services”:** This chapter explains how clients access Internet services and also describes client and server interaction, TCP and UDP transport layer functions, and how TCP and UDP use port numbers.

- **Chapter 12, “Application Layer Services”:** This chapter explains the function of common application layer services, including DNS, HTTP and HTML, FTP, Telnet and SSH, and email protocols.
- **Chapter 13, “Build a Home Network”:** This chapter explains how to configure an integrated wireless router and wireless client to connect securely to the Internet. It also describes the components required to build a home network, the wired and wireless network technologies used, and how wireless traffic is controlled.
- **Chapter 14, “Connect to the Internet”:** This chapter explains how to configure Wi-Fi settings on mobile devices to connect to the Internet, including ISP connectivity options. The chapter also explains the purpose and characteristics of network virtualization.
- **Chapter 15, “Security Considerations”:** This chapter explains different types of network security threats, including social engineering attacks, various types of malicious software, and denial-of-service attacks. The chapter explains how security tools, software updates, and antimalware software mitigate network security threats.
- **Chapter 16, “Configure Network and Device Security”:** This chapter explains how to configure basic network security, including basic ways to address wireless security vulnerabilities, configure encryption on a wireless router, and configure firewall settings.
- **Chapter 17, “Cisco Switches and Routers”:** This chapter explains Cisco LAN switches and the Cisco LAN switch boot process. The chapter also explains Cisco small business routers and the Cisco router boot process. Finally, the chapter explains in-band and out-of-band management access.
- **Chapter 18, “The Cisco IOS Command Line”:** This chapter explains how to use the Cisco IOS; it also covers the correct commands to navigate the Cisco IOS modes, how to navigate the Cisco IOS to configure network devices, and how to use show commands to monitor device operations.
- **Chapter 19, “Build a Small Cisco Network”:** This chapter explains how to build a simple computer network using Cisco devices. In addition, it describes the initial settings on a Cisco switch and a Cisco router, how to configure the devices for secure remote management, and how to connect the devices together in a network.
- **Chapter 20, “Troubleshoot Common Network Problems”:** This chapter explains some of the approaches used to troubleshoot networks, including the process of detecting physical layer problems and network troubleshooting utilities. The chapter also explains how to troubleshoot a wireless network problem, common Internet connectivity problems, and how to use outside sources and Internet resources for troubleshooting.

- **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 definitions for all the key terms identified in each chapter, plus more terms you might encounter.

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 are the differences and similarities of the OSI and TCP/IP models?
- How do the OSI model's Layer 1 and Layer 2 function in an Ethernet network?

Key Terms

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

Ethernet page 103

Institute of Electrical and Electronic Engineers (IEEE) page 104

International Organization for Standardization (ISO) page 99

Internet Engineering Task Force (IETF) page 96

protocol page 93

protocol suite page 99

reference model page 99

Request for Comments (RFC) page 96

Introduction (5.0.1)

When you talk with someone, you are communicating. When you mail a card to a relative, you are communicating. You probably don't think much about the rules of communication when you do these two things. But there are rules, and good communication happens only when all parties know and follow those rules. It is the same with devices on a network. This chapter explains the rules, which are called protocols, of network communication. When you understand the various protocols and how they work with other protocols, you not only will understand how networks and the Internet work but also be able to troubleshoot problems in your own network.

The Rules (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.

The Three Elements (5.1.1)

The primary purpose of any network is to provide a method to communicate and share information. From the earliest primitive human societies to the most advanced technological societies of today, sharing information with others has been crucial for human advancement.

All communication begins with a message, or information, that must be sent from one individual or device to another. The methods used to send, receive, and interpret messages change over time as technology advances.

All communication methods have three elements in common. The first of these elements is the message source, or sender. Message sources are people or even electronic devices that need to communicate a message to other individuals or devices. The second element of communication is the destination, or receiver, of the message. The destination receives the message and interprets it. The third element is called a transmission medium, or channel. It provides the pathway over which the message can travel from source to destination.

For example, in Figure 5-1, two people can communicate face-to-face. Prior to communicating, they must agree on how to communicate. If the communication is using voice, they must first agree on the language. Next, when they have a message to share, they must be able to format that message in a way that is understandable. If

someone uses the English language but poor sentence structure, the message can easily be misunderstood. Each of these tasks describes protocols that are used to accomplish communication.

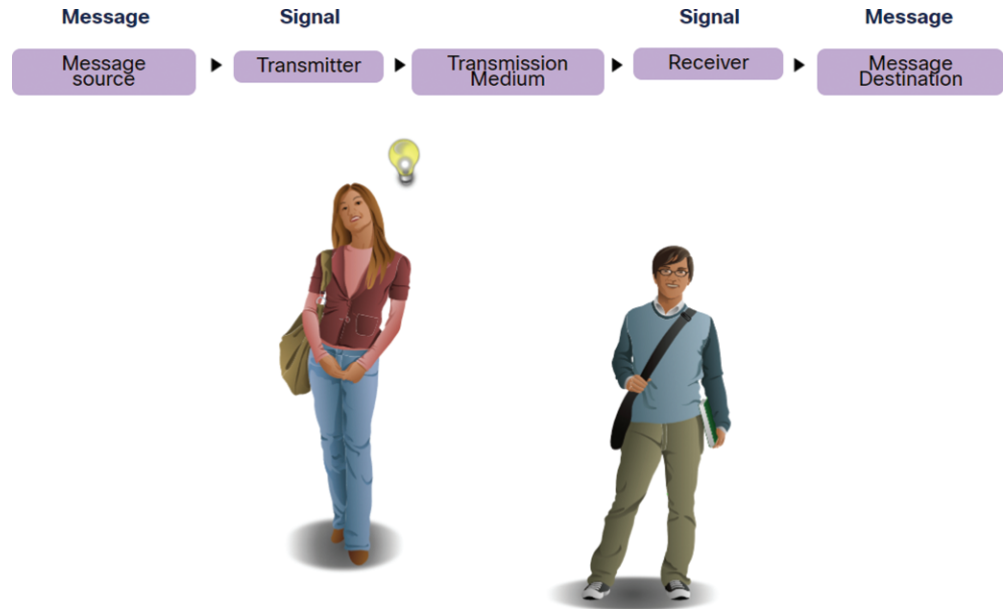


Figure 5-1 Protocols for Face-to-Face Communications

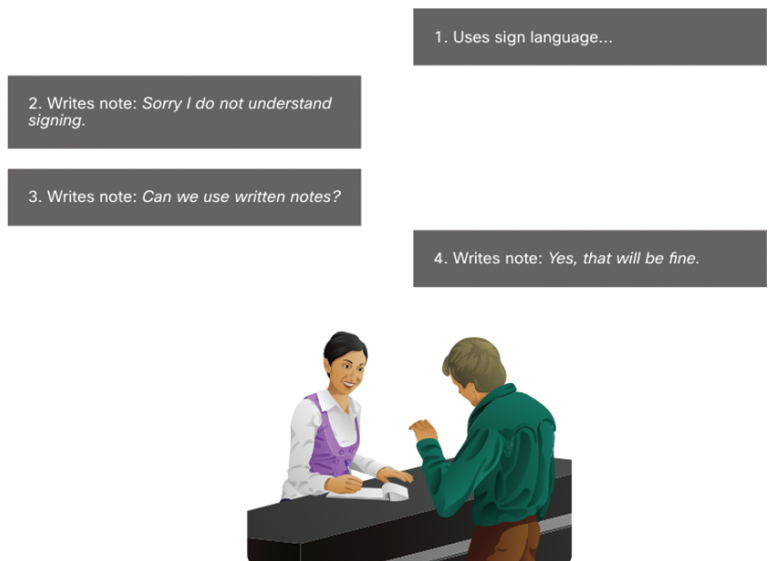
Communication Protocols (5.1.2)

Communication in your daily life takes many forms and occurs in many environments. You have different expectations depending on whether you 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, you establish rules or agreements to govern the conversation. These agreements include the following:

- What method of communication should you use? (See Figure 5-2.)
- What language should you use? (See Figure 5-3.)
- Do you need to confirm that your messages are received? (See Figure 5-4.)

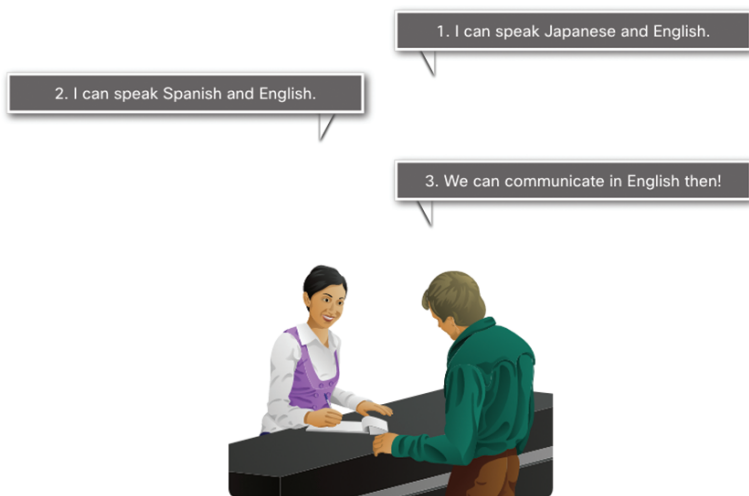
Figure 5-2 shows two people agreeing on a method of communication.



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

Figure 5-2 Method of Communication

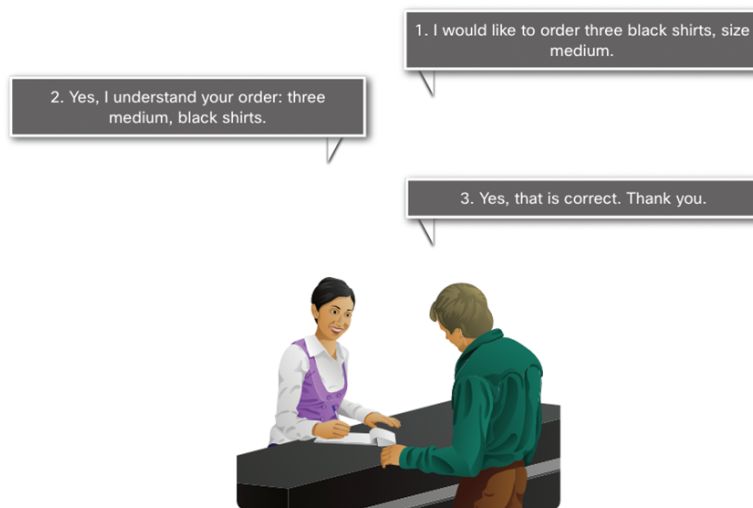
Figure 5-3 shows two people agreeing on a common language to use for communication.



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

Figure 5-3 Language Used for Communication

Figure 5-4 shows the communication between two people, including confirmation of the order.



Communication is successful when the intended message has been received and confirmed.

Figure 5-4 Confirmation of Communication

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.

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

Why Protocols Matter (5.1.3)

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 protocols include message format, message size, timing, encoding, encapsulation, and message patterns.

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, breaking the message into smaller pieces might be necessary 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 impulses 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, other information in the header may ensure 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, other types of messages may be simply streamed across the network, without concern as to whether they reach their destination.

**Lab—My Protocol Rules (5.1.4)**

In this lab, you will complete the following objectives:

- Relate computer network protocols to the rules that you use every day for various forms of communication.
 - Define the rules that govern how you send and interpret text messages.
 - Explain what would happen if the sender and receiver did not agree on the details of the protocol.
-

Communication Standards (5.2)

Communication standards are required in all aspects of human communications such as when addressing an envelope. There is a standard regarding the placement of the sender's address, destination address, and even where you put the stamp. Network communication also requires standards to ensure that all the devices in the network use 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 determine 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, different types of devices are able 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, as shown in Figure 5-5. 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)*.

Other standards organizations that support the Internet are shown in Figure 5-5.



Figure 5-5 Internet Standards Organizations

Network Communication Models (5.3)

Network communication models help you understand the various components and protocols used in network communications. These models help you 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 Protocol Stack (5.3.3)

Successful communication between hosts requires interaction between many protocols. 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, as shown in Figure 5-6. 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.

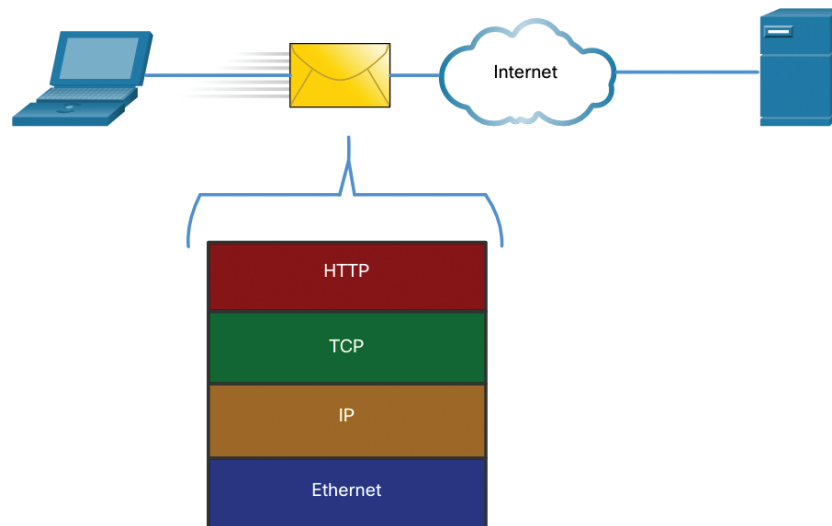


Figure 5-6 A Protocol Stack for Internet Communications

The separation of functions enables each layer in the stack to operate independently of others. For example, you can use your laptop computer connected to a cable modem at home to access your favorite website, or you can view the same website on your laptop using a wireless connection at the library. The function of the web browser is not affected by the change in the physical location or the method of connectivity.

The protocols in Figure 5-6 are described as follows:

- **Hypertext Transfer Protocol (HTTP)**—This protocol governs the way a web server and a web client interact. HTTP defines the content and formatting of the requests and responses that are exchanged between the client and server. Both the client and the web server software implement HTTP as part of the application. HTTP relies on other protocols to govern how the messages are transported between the client and server.
- **Transmission Control Protocol (TCP)**—This protocol manages the individual conversations. TCP is responsible for guaranteeing the reliable delivery of the information and managing flow control between the end devices.
- **Internet Protocol (IP)**—This protocol is responsible for delivering messages from the sender to the receiver. IP is used by routers to forward the messages across multiple networks.
- **Ethernet**—This protocol is responsible for the delivery of messages from one NIC to another NIC on the same Ethernet local-area network (LAN).

The TCP/IP Model (5.3.4)

Layered models help you 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 in order 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 dialogue 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 (5.3.5)

Two basic types of models are used to describe the functions that must occur in order for network communications to be successful: protocol models and reference models.

- **Protocol model**—This 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.

OSI Model Layer	Description
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 bit transmission to and from a network device.

Upper and Lower Layers of the OSI Model (5.3.6)

You can visualize how data moves across a network by using the seven layers of the OSI model, as shown in Table 5-3. The OSI model breaks down network communication into multiple processes, as shown in Table 5-4. Each process is a small part of the larger task.

For example, in a vehicle manufacturing plant, the entire vehicle is not assembled by one person. Rather, the vehicle moves from station to station where specialized teams add specific components. The complex task of assembling a vehicle is made easier by breaking it into manageable and logical tasks. This process also makes troubleshooting easier. When a problem occurs in the manufacturing process, it is possible to isolate the problem to the specific task where the defect was introduced and then fix that problem.

In a similar manner, the OSI model helps you troubleshoot by focusing on a specific layer to identify and resolve network problems. Networking teams often refer to different functions occurring on a network by the number of the OSI model layer that specifies that functionality. For example, the process of encoding the data bits for transmission across the media occurs at Layer 1, the physical layer. The formatting of data so it can be interpreted by the network connection in your laptop or phone is described at Layer 2, the data link layer.

Table 5-4 Common Components of the Layers of the OSI Model

Group	Layer Number	Layer Name	Common Network Components Associated with This Layer
Upper Layers	7	Application	<ul style="list-style-type: none"> ■ Network-aware applications
	6	Presentation	<ul style="list-style-type: none"> ■ Email
	5	Session	<ul style="list-style-type: none"> ■ Web browsers and servers ■ File transfer ■ Name resolution
Lower Layers	4	Transport	<ul style="list-style-type: none"> ■ Video and voice streaming mechanisms ■ Firewall filtering lists
	3	Network	<ul style="list-style-type: none"> ■ IP addressing ■ Routing
	2	Data Link	<ul style="list-style-type: none"> ■ Network interface cards and drivers ■ Network switching ■ WAN connectivity
	1	Physical	<ul style="list-style-type: none"> ■ Physical medium (copper twisted-pair, fiber-optic cables, wireless transmitters)

OSI Model and TCP/IP Model Comparison (5.3.7)

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 5-7. 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.

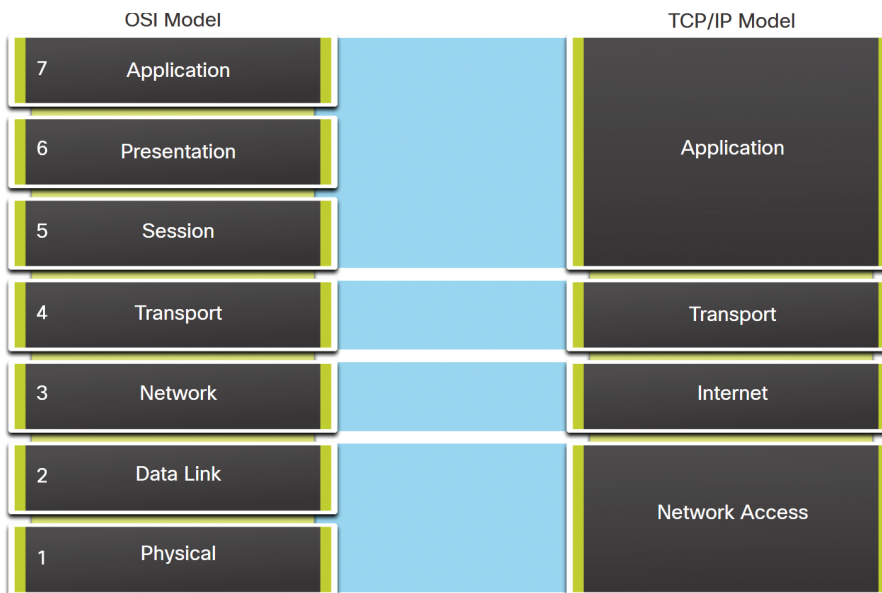


Figure 5-7 The OSI and TCP/IP Models

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.

Ethernet (5.4)

When you are connecting to a network using a wired interface, you are using the Ethernet protocol. Even most wireless networks ultimately connect to a wired Ethernet network. Ethernet is an important data link layer protocol used in LANs and most wide-area networks (WANs).

The Rise of Ethernet (5.4.1)

In the early days of networking, each vendor used its own proprietary methods of interconnecting network devices and networking protocols. If you bought equipment from different vendors, there was no guarantee that the equipment would work together. Equipment from one vendor might not communicate with equipment from another.

As networks became more widespread, standards were developed that defined rules by which network equipment from different vendors operated. Standards are beneficial to networking in many ways:

- Facilitate design
- Simplify product development
- Promote competition
- Provide consistent interconnections
- Facilitate training
- Provide more vendor choices for customers

There is no official local-area networking standard protocol, but over time, one technology, Ethernet, has become more common than the others. *Ethernet* protocols define how data is formatted and how it is transmitted over the wired network. The Ethernet standards specify protocols that operate at Layer 1 and Layer 2 of the OSI model. Ethernet has become the de facto standard, which means that it is the technology used by almost all wired local-area networks, as shown in Figure 5-8.

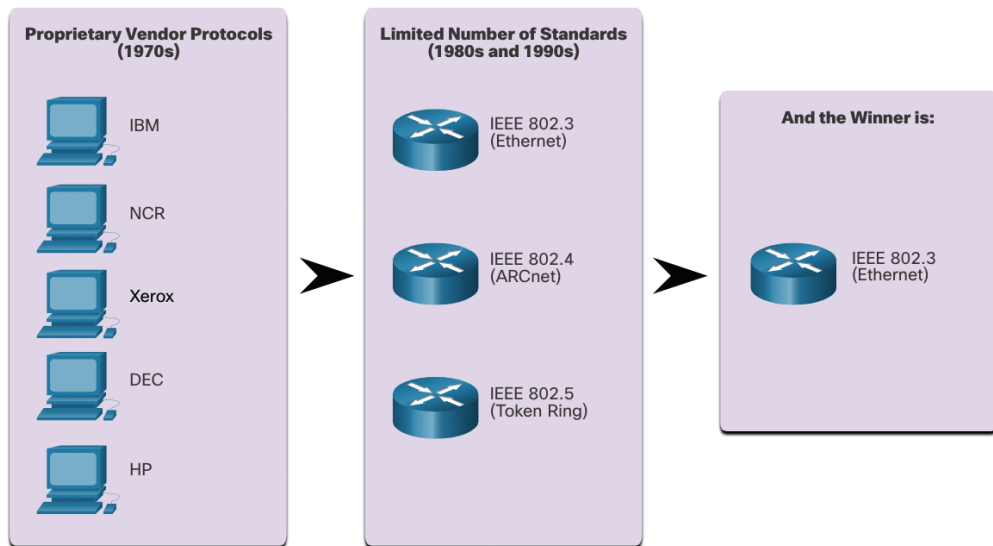


Figure 5-8 The Evolution from Proprietary LAN Protocols to Ethernet

Ethernet Evolution (5.4.2)

The *Institute of Electrical and Electronic Engineers*, or *IEEE* (pronounced “eye-triple-e”), maintains the networking standards, including Ethernet and wireless standards. IEEE committees are responsible for approving and maintaining the standards for connections, media requirements, and communication protocols. Each technology standard is assigned a number that refers to the committee that is responsible for approving and maintaining the standard. The committee responsible for Ethernet standards is 802.3.

Since the creation of Ethernet in 1973, standards have evolved for specifying faster and more flexible versions of the technology. This ability for Ethernet to improve over time is one of the main reasons that it has become so popular. Each version of Ethernet has an associated standard. For example, 802.3 100BASE-T represents the 100 megabit Ethernet using twisted-pair cable standards. The standard notation translates as follows:

- 100 is the speed in Mbps.
- BASE stands for baseband transmission.
- T stands for the type of cable—in this case, twisted-pair.

Early versions of Ethernet were relatively slow at 10 Mbps. The latest versions of Ethernet operate at 10 gigabits per second and more. Imagine how much faster these new versions are than the original Ethernet networks.

Video

Video—Ethernet Addressing (5.4.3)

Refer to the online course to view this video.

The Ethernet MAC Address (5.4.4)

All communication requires a way to identify the source and destination. The source and destination in human communication are represented by names.

When your name is called, you listen to the message and respond. Other people in the room may hear the message, but they ignore it because it is not addressed to them.

On Ethernet networks, a similar method exists for identifying source and destination hosts. Each host connected to an Ethernet network is assigned a physical address that serves to identify the host on the network.

Every Ethernet network interface has a physical address assigned to it when it is manufactured. This address is known as the Media Access Control (MAC) address. The MAC address identifies each source and destination host on the network, as shown in Figure 5-9.

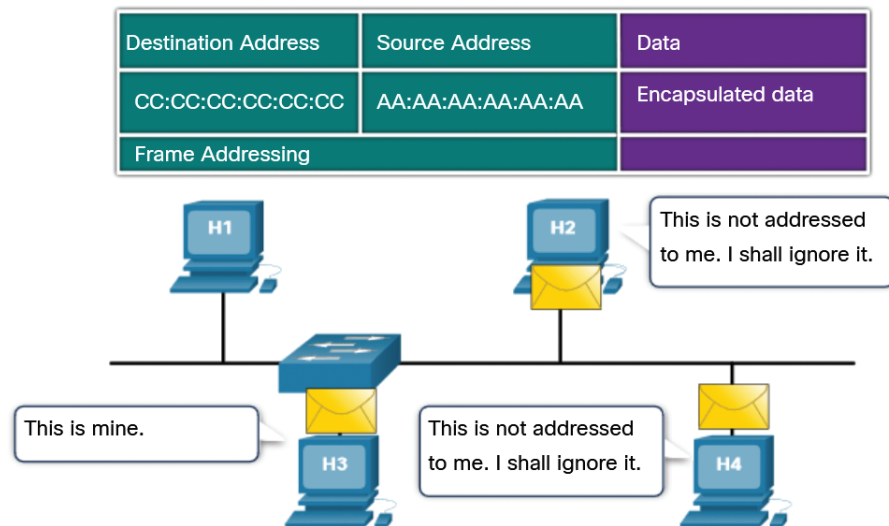


Figure 5-9 MAC Addresses Identify Unique Hosts on a LAN



Lab—Determine the MAC Address of a Host (5.4.5)

In this lab, you will complete the following objectives:

- Determine the MAC address of a Windows computer on an Ethernet network using the `ipconfig /all` command.
 - Analyze a MAC address to determine the manufacturer.
-

Summary (5.5)

The following is a summary of each topic in the chapter:

- **The Rules**—All communication methods have three elements in common. The first is the message source, or sender. Message sources are people or electronic devices that need to communicate a message to other individuals or devices. The second is the destination, or receiver, of the message. The destination receives the message and interprets it. The third is the transmission medium, or channel. It provides the pathway over which the message can travel from source to destination.

Among the protocols that govern successful human communication are an identified sender and receiver, an agreed-upon method of communicating, common language and grammar, speed and timing of delivery, and confirmation or acknowledgment requirements. Networking protocols define the message format, message size, timing, encoding, and message patterns over the local network.

- **Communication Standards**—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, different types of devices are able to send information to each other over the Internet. These 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**—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 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 suite of TCP/IP protocols used for Internet communications follows the structure of the stack model. The two basic types of models to describe the

functions that must occur for network communications to be successful are protocol models and reference models. The most widely known internetwork reference model is the OSI model. The OSI model breaks down network communications into multiple processes. Each process is a small part of the larger task.

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. 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.

- **Ethernet**—There is no official LAN standard protocol, but over time, Ethernet has become more common than the others. Ethernet protocols define how data is formatted and how it is transmitted over the wired network. The Ethernet standards specify protocols that operate at Layer 1 and Layer 2 of the OSI model. Ethernet standards have evolved for specifying faster and more flexible versions of the technology. Each version of Ethernet has an associated standard. Each host connected to an Ethernet network is assigned a physical address that serves to identify the host on the network. Every Ethernet network interface has a physical address assigned to it when it is manufactured. This address is known as the MAC address. The MAC address identifies each source and destination host on the network.

Practice

The following labs provide practice with the topics introduced in this chapter.

Labs



Lab—My Protocol Rules (5.1.4)

Lab—Determine the MAC Address of a Host (5.4.5)

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 the ‘Check Your Understanding’ Questions,” lists the answers.

1. Which organization publishes and manages the Request for Comments (RFC) documents?
 - a. TIA/EIA
 - b. IETF
 - c. ISO
 - d. IEEE

2. What identifier is used at the data link layer to uniquely identify an Ethernet device?
 - a. MAC address
 - b. Sequence number
 - c. IP address
 - d. UDP port number
 - e. TCP port number

3. Which layers of the OSI model are comparable in function to the application layer of the TCP/IP model? (Choose three.)
 - a. Data link
 - b. Transport
 - c. Network
 - d. Presentation
 - e. Application
 - f. Session
 - g. Physical

4. Which term refers to a common set of rules that are developed to define rules by which network equipment from different vendors can interoperate?
 - a. Domain
 - b. Standard
 - c. Model
 - d. Protocol

5. Which standards organization publishes current Ethernet standards?
 - a. ANSI
 - b. CCITT
 - c. IEEE
 - d. EIA/TIA

6. Which statement describes a MAC address?
 - a. It contains two portions: the network portion and a host portion.
 - b. It is 128 bits in length.
 - c. It identifies the source and destination addresses of hosts on the Internet.
 - d. It is a physical address assigned to an Ethernet NIC by the manufacturer.

7. Which elements do all communication methods have in common? (Choose three.)
 - a. Message priority
 - b. Message source
 - c. Transmission medium
 - d. Message type
 - e. Message data
 - f. Message destination

8. Which layers of the OSI model specify protocols that are associated with Ethernet standards? (Choose two.)
 - a. Physical layer
 - b. Transport layer
 - c. Session layer
 - d. Data link layer
 - e. Network layer

9. Which layer of the OSI model defines services to segment and reassemble data for individual communications between end devices?
 - a. Network
 - b. Presentation
 - c. Transport
 - d. Session
 - e. Application

10. Which statement defines a data communications protocol?
 - a. An alliance of network device manufacturers
 - b. A set of product standards for types of network devices
 - c. An exchange agreement of network devices among vendors
 - d. A set of rules that govern the communication process

Numerics

4/5G, 32–33

A

access layer, 119

- ARP (Address Resolution Protocol), 129–130
- communication, 128–129
- devices, 121
- Ethernet
 - broadcasts*, 126–128
 - hubs*, 121–122
 - switches*, 123–124
- MAC address table, 124–126

actuators, 14

adware, 306, 317

Android

- cellular data settings, 288
- Wi-Fi settings, 285–286

antimalware software, 314–315

antispam software, 316

antispym software, 316–317

antivirus software, 315–316

Apple iOS

- cellular data settings, 289
- Wi-Fi settings, 285–287

appliances, 10–11

application layer

- DNS (Domain Name System), 231
 - domain name translation*, 231
 - server*, 232
- email, 239–240
 - IMAP4 (Internet Message Access Protocol)*, 241
 - POP3 (Post Office Protocol)*, 241
 - SMTP (Simple Mail Transfer Protocol)*, 240–241
- FTP (File Transfer Protocol), 235–236
- HTML (Hypertext Markup Language), 233–234
- HTTP (Hypertext Transfer Protocol), 233–234

- network application services, 230–231

- Telnet, 237–239

- text messaging, 242

- VoIP (voice over IP), 243

applications. *See also* Packet Tracer

- P2P (peer-to-peer), 21–22

- security, 312–313

- web browser, 213

ARP (Address Resolution Protocol), 129–130

attacks

- brute force, 310
- DDoS (distributed denial-of-service), 309–310
- DoS (denial-of-service), 308–309
- malware, 304–305
 - Trojan horse*, 305–306
 - viruses*, 305
 - worms*, 305
- signs of infection, 314–315
- social engineering
 - phishing*, 303–304
 - pretexting*, 303
 - vishing*, 304
- war driving, 327
- war walking, 327

authentication

- open, 336
- wireless network, 336–337
 - troubleshooting*, 439–440
 - WEP (Wired Equivalency Protocol)*, 337–338
 - WPA (Wi-Fi Protected Access)*, 338

B

in-band management, 358

bandwidth, 17–18

binary numbers, converting to decimal, 159–161

Bluetooth, 34, 254, 290–291

boot process

- routers, 361
- switches, 355

botnets, 307

bottom-up troubleshooting, 418–419

broadcast(s), 126, 172–173

containment, 138–139

domains, 127–128

in the local network, 126–127

brute force attacks, 310

business networks, 4

C

cable Internet, 274

category 5e cable, 256

cell phones, 32–33. *See also* smartphones

5G, 32–33

GSM (Global System for Mobile Communication), 32

cellular Internet, 275

CIDR (classless interdomain routing), 167

Cisco IOS CLI, 374–375

command(s), 376–377

exiting, 380

modes, 375–376

--More-- prompt, 379–380

shortcuts, 378–379

show, 381–386

syntax, 377–378

Syntax Checker, 376

Cisco Packet Tracer. *See* Packet Tracer

classful IP addressing, 166–167

classless IP addressing, 167

client/server interaction, 19–20, 22, 212–213.

See also servers

email, 239–240

FTP, 235–236

web server

client requests, 213

data center, 213

HTTP (Hypertext Transfer Protocol), 233–234

URI (Uniform Resource Identifier), 214

cloud computing, 276

models, 276–277

services, 277

virtualization, 277–278

advantages of, 279

hypervisors, 279–280

network, 281, 282

SDN (software-defined networking) and,
283–284

coaxial cable, 70, 75–76, 83, 256

commands

Cisco IOS, 376–377

exiting, 380

--More-- prompt, 379–380

shortcuts, 378–379

show, 381–386

syntax, 377–378

netstat, 223

ping, 80, 84

traceroute, 81, 84

troubleshooting, 426, 451

ipconfig, 427–430

netstat, 434–435

nslookup, 436–437

ping, 430–433

tracert, 433–434

communication

models, 96

OSI, 99–100–101–102

TCP/IP, 98–99

protocols, 90–91–93

characteristics, 94

importance of, 93–94

rules and, 90

standards, 95

Internet and, 95

organizations, 95–96

community cloud, 277

comparison approach to troubleshooting, 421

configuration

Cisco switch, 392

basic, 392–393

SVI, 394

DHCPv4, 185, 186–187

Packet Tracer security, 327–332

router, 395–397

Wi-Fi for mobile devices, 286–287

connected home devices

appliances, 10–11

gaming consoles, 12

security systems, 10

- smart TVs, 11
- connectivity
 - ping command, 80, 84
 - traceroute command, 81, 84
 - troubleshooting, 442–443, 452–453
 - DHCP server configuration errors, 441–442
 - verify firewall settings, 444
- control plane, 282
- cookies, 306
- core layer, 120
- crossover cable, 79
- crosstalk, 71–72
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 260
- CTS (Clear to Send), 260

D

- data center, 213
- data manipulation, 300
- data plane, 282
- data transmission
 - bandwidth, 17–18
 - interference, 71–72
 - signal transmission, 16–17
 - throughput, 18–19
 - types of personal data, 15–16
- DDoS (distributed denial-of-service) attacks, 309–310
- default gateway, 39, 146–147
 - for a host, 404–406
 - for a switch, 406–407
- destination port number, 221
- devices
 - access layer, 121
 - in-band management, 358
 - hubs, 121–122
 - LEDs, 424–425
 - out-of-band management, 358
 - routers, 359, 367–368
 - boot process, 361
 - as boundaries between networks, 195–196
 - components, 360
 - configuration, 395–397
 - as gateways, 194–195
 - home network, 252–253
 - interface ports, 360–361
 - management ports, 365–366
 - passwords, 398–399–400
 - ports, 252
 - powering up, 361–364
 - remote access, 399–400
 - wireless technology, 250–251
 - switches, 123–124, 350–351, 367
 - basic configuration, 392–393
 - boot process, 355
 - default gateway, 406–407
 - expandability, 353
 - LAN, 351
 - manageability, 353–354
 - passwords, 398–399–400
 - ports, 352
 - powering up, 355–357
 - remote access, 399–400
 - running configuration file, 359
 - speed required, 352–353
 - SSH configuration, 400–404
 - startup configuration file, 358–359
 - SVI configuration, 394
- DHCP (Dynamic Host Configuration Protocol), 183–184, 194–195
 - configuration, 185
 - operation, 185–186
 - servers, 184–185
 - service configuration, 186–187
- dial-up Internet, 275
- disruption of service, 301
- distribution layer, 119–120, 140
- divide-and-conquer approach to troubleshooting, 420
- DMZ (demilitarized zone), 339–340
- DNS (Domain Name System), 40, 231
 - domain name translation, 231
 - server, 232
- documentation
 - network, 41
 - logical network information, 43–44
 - topologies, 42–43
 - troubleshooting, 416
- DoS (denial-of-service) attacks, 308–309

dotted decimal notation, 159
DSL (Digital Subscriber Line), 274
dual stack, 201–202
dynamic IP address configuration, 41

E

educated guess approach to troubleshooting, 421
electromagnetic spectrum, 253–254
email, 212

- antispam software, 316
- client/server interaction, 239–240
- protocols
 - IMAP4 (*Internet Message Access Protocol*), 241
 - POP3 (*Post Office Protocol*), 241
 - SMTP (*Simple Mail Transfer Protocol*), 240–241
- spam, 307, 317

EMI (electromagnetic interference), 71
encapsulation, 112–113, 172
end devices, 25
Ethernet, 38, 103–104, 117, 255

- broadcast(s), 126
 - domains, 127–128
 - in the local network, 126–127
- frames, 114–115, 141
- MAC (Media Access Control) address, 105, 115–116, 124–126
- NIC (network interface card), 84, 367
- over Powerline, 256–257
- standards, 104–105
- switches, 123–124
- twisted-pair cable, 71–72
 - STP (*shielded twisted-pair*), 75
 - transmit and receive pairs, 79
 - UTP (*unshielded twisted-pair*), 73–74
 - wiring schemes, 78–79

external threats, 302

F

fiber-optic cable, 70–71, 76–78
firewalls, 338–339. *See also* security
troubleshooting, 444
follow-the-path approach to troubleshooting,
420–421

frames, 114–115, 141
FTP (File Transfer Protocol), 235–236

G

gaming consoles, 12
GPS (global positioning system), 33
GSM (Global System for Mobile Communication), 32

H

hexadecimal numbers, 204–205
hierarchical network design, 115

- access layer, 119
 - ARP (*Address Resolution Protocol*), 129–130
 - broadcasts, 126–128
 - communication, 128–129
 - devices, 121
 - Ethernet hubs, 121–122
 - Ethernet switches, 123–124
- analogy, 117
- benefits of, 117–118
- core layer, 120
- distribution layer, 119–120
- physical and logical addresses, 115–116

home networks, 250

- components, 251–252
- dial-up Internet, 275
- Internet connectivity
 - cable, 274
 - cellular, 275
 - DSL (*Digital Subscriber Line*), 274
 - satellite, 275
- MAC address filtering, 263–264
- media, 256–257
- routers, 252–253, 261
 - design considerations, 261–262
 - first time setup, 261
- wired technology, 255
- wireless technology, 250–251
 - electromagnetic spectrum, 253–254
 - legacy mode, 262
 - settings, 257–259
 - Wi-Fi, 257
 - wireless frequencies, 254–255

hosts, 35

- default gateway, 404–406
- IP addressing and, 162–163
- remote, 141, 152

hotspots, 34**HTML (Hypertext Markup Language), 233–234****HTTP (Hypertext Transfer Protocol), 233–234****hybrid cloud, 276****hypervisors, 279**

- Type 1, 279–280
- Type 2, 280

I-J-K

IaaS (Infrastructure as a Service), 277**IANA (Internet Assigned Numbers Authority), 170****ICMP (Internet Control Message Protocol), 199****identity theft, 300****IEEE (Institute of Electrical and Electronic Engineers), 104, 257, 258****IMAP4 (Internet Message Access Protocol), 241****information theft, 300****installing, Packet Tracer, 50, 51****interference, 71–72****internal threats, 301–302****Internet**

- backbone, 273
- cable, 274
- cellular, 275
- connected devices outside the home
 - medical devices, 14–15*
 - RFID (radio frequency identification) tags, 13*
 - sensors and actuators, 14*
 - smart cars, 12*
- connected home devices, 10
 - appliances, 10–11*
 - gaming consoles, 12*
 - security systems, 10*
 - smart TVs, 11*
- dial-up, 275
- DSL (Digital Subscriber Line), 274
- online interactions, 3–4
- phone calls, 243
- satellite, 275
- troubleshooting, 442–443, 452–453
 - DHCP server configuration errors, 441–442*

sources of help, 445

support desk interaction, 445–449

verify firewall settings, 444

intranet, 148**iOS**

cellular data settings, 289

Wi-Fi settings, 285–287

IoT (Internet of Things), 200**IP (Internet Protocol), 113****IP addressing, 39–40, 115–116, 158. *See also*****routing**

classful, 166–167

classless, 167

default gateway, 39

device names and address planning, 41

DHCP (Dynamic Host Configuration Protocol),
183–184

configuration, 185

operation, 185–186

routing and, 194–196

servers, 184–185

service configuration, 186–187

DNS (Domain Name System), 40

dotted decimal notation, 159

dual stack, 201–202

dynamic configuration, 41

IANA (Internet Assigned Numbers Authority), 170

IoT (Internet of Things), 200

IPv4, 158–159, 176–177, 198

address assignment, 169–170

binary-to-decimal conversion, 159–161

broadcast transmission, 172–173

depletion of address space, 198–200

multicast transmission, 173–174

private, 168–169, 176

static address assignment, 182–183

unicast transmission, 171–172

IPv6, 118, 203, 206–207

address representation, 204–205

address size, 200–201

autoconfiguration, 203–204

link-local address, 204

need for, 198–200

logical AND operation, 163–164, 175

manual configuration, 40

NAT (Network Address Translation), 169, 196–198, 203, 206, 339
networks and hosts, 162–163
RIRs (Regional Internet Registries), 170
socket pairs, 221–223
subnet mask, 39, 164–166
tunneling, 202
ipconfig command, 427–430
IPv4, 175
ISP (Internet service provider), 272
 connection options
 cable Internet, 274
 cellular, 275
 dial-up, 275
 DSL (Digital Subscriber Line), 274
 satellite, 275
 connections, 273–274
 services, 272–273
 support desk, 445–449
ITaaS (IT support as a Service), 277

L

LAN (local-area network), 34–35, 147–148, 153.
 See also home networks
 devices, 36–37
 Ethernet, 38
 hosts, 35
 intranet, 148
 local segment, 148–149
 media, 37–38
 NIC (network interface card), 38, 39
 peripherals, 35–36
 remote segment, 149–150
 switches, 351
 boot process, 355
 expandability, 353
 manageability, 353–354
 ports, 352
 powering up, 355–357
 speed required, 352–353
link-local address, 204
local networks, 4
 broadcasts, 126–127
 business, 4
 criteria for dividing, 138
 broadcast containment, 138–139
 physical locations, 140
 security, 139
 medium to large, 6
 small home, 4–5
 SOHO (small office/home office), 3, 4–5
logical addresses, 115–116
logical AND operation, 163–164, 175
logical network information, documenting, 43–44

M

MAC (Media Access Control) address, 105, 115–116, 124–126
 filtering, 263–264, 266–267, 335
malware, 304–305
 Trojan horse, 305–306
 viruses, 305
 worms, 305
manual IP address configuration, 40
media, 37–38, 68, 83
 category 5e cable, 256
 coaxial cable, 70, 75–76
 crossover cable, 79
 crosstalk, 71–72
 EMI (electromagnetic interference), 71
 fiber-optic cable, 70–71, 76–78
 home network, 256–257
 troubleshooting, 426
 twisted-pair cable, 69–70, 71–72, 83
 STP (shielded twisted-pair) cable, 75
 transmit and receive pairs, 79
 UTP (unshielded twisted-pair) cable, 73–74
medical devices, 14–15
medium to large networks, 6
mobile devices, 7
 smart glasses, 9
 smartphones, 7–8
 smartwatches, 8–9
 tablets, 8
 Wi-Fi, 284–285
 configuration, 286–287
 settings, 285–286
multicast transmission, 173–174

N

- NAT (Network Address Translation), 169, 196–198, 203, 206, 339
- netstat command, 223, 434–435
- network(s). *See also* communication protocols; Ethernet; Internet; IP addressing; protocols; routing; wireless networks
- application services, 230–231
 - email*, 239–243
 - FTP (File Transfer Protocol)*, 235–236
 - HTML (Hypertext Markup Language)*, 233–234
 - HTTP (Hypertext Transfer Protocol)*, 233–234
 - Telnet*, 237–239
 - text messaging*, 242
 - VoIP (voice over IP)*, 243
 - boundaries, 194, 206
 - clients and servers, 19–20, 22
 - communication models, 96
 - OSI*, 99–100–101–102
 - TCP/IP*, 98–99
 - components, 23
 - end devices*, 25
 - infrastructure*, 23–24
 - connectivity
 - ping command*, 80, 84
 - traceroute command*, 81, 84
 - data transmission, 15
 - bandwidth*, 17–18
 - signal transmission*, 16–17
 - throughput*, 18–19
 - types of personal data*, 15–16
 - documentation, 41
 - logical network information*, 43–44
 - topologies*, 42–43
 - hierarchical design, 115. *See also* access layer; core layer; distribution layer
 - access layer*, 119
 - analogy*, 117
 - benefits of*, 117–118
 - core layer*, 120
 - distribution layer*, 119–120
 - home, 250. *See also* wireless networks
 - cable Internet*, 274
 - cellular Internet*, 275
 - components*, 251–252
 - dial-up Internet*, 275
 - DSL (Digital Subscriber Line)*, 274
 - media*, 256–257
 - routers*, 252–253
 - satellite Internet*, 275
 - wired technology*, 255
 - wireless technology*, 250–251, 253–255
 - IP addressing, 39–40
 - address assignment*, 169–170
 - binary-to-decimal conversion*, 159–161
 - broadcast transmission*, 172–173
 - classful*, 166–167
 - classless*, 167
 - default gateway*, 39
 - depletion of address space*, 198–200
 - device names and address planning*, 41
 - DNS (Domain Name System)*, 40
 - dotted decimal notation*, 159
 - dual stack*, 201–202
 - dynamic configuration*, 41
 - hosts*, 162–163
 - IANA (Internet Assigned Numbers Authority)*, 170
 - IPv6 address space*, 200–201
 - manual configuration*, 40
 - multicast transmission*, 173–174
 - NAT (Network Address Translation)*, 169, 196–198, 203
 - private*, 168–169
 - RIRs (Regional Internet Registries)*, 170
 - socket pairs*, 221–223
 - static address assignment*, 182–183
 - subnet mask*, 39, 164–166
 - tunneling*, 202
 - unicast transmission*, 171–172
 - LAN (local-area network), 34–35, 147–148, 153
 - devices*, 36–37
 - Ethernet*, 38
 - hosts*, 35
 - intranet*, 148
 - local segment*, 148–149
 - media*, 37–38
 - NIC (network interface card)*, 38, 39
 - peripherals*, 35–36
 - remote segment*, 149–150

local, 4
broadcast containment and, 138–139
broadcasts, 126–127
business, 4
criteria for dividing, 138
medium to large, 6
routing, 140
security, 139
small home, 4–5
SOHO (small office/home office), 3, 4–5

logical addresses, 115–116

media, 68
coaxial cable, 70, 75–76
crossover cable, 79
crosstalk, 71–72
EMI (electromagnetic interference), 71
fiber-optic cable, 70–71, 76–78
STP (shielded twisted-pair) cable, 75
twisted-pair cable, 69–70, 71–72, 78–79
UTP (unshielded twisted-pair) cable, 73–74

P2P (peer-to-peer), 20–22

Packet Tracer, 50, 60–61
 CLI tab, 56
 Config tab, 55
 Desktop tab, 56–57
 GUI and CLI configuration, 54
 installing, 50, 51
 locating and deploying devices, 52
 network configuration, 53
 network management menu, 52
 Physical tab, 54
 Services tab, 57–58
 uses of, 50–51

physical addresses, 115–116

software-defined, 283–284

troubleshooting, physical layer, 423–426

virtualization, 281

worldwide, 6–7

NFC (near-field communication), 34

NIC (network interface card), 38, 39, 84, 367

nslookup command, 436–437

O

open authentication, 336

OSI (Open Systems Interconnection) reference

model, 99–100
 layers, 100–101
 TCP/IP and, 101–102

OSI reference model. *See also* transport layer

out-of-band management, 358

P

P2P (peer-to-peer) networks, 20–22, 68

PaaS (Platform as a Service), 277

Packet Tracer, 50, 395, 397, 408, 450
 building a simple network, 60–61
 CLI tab, 56
 Config tab, 55
 Desktop tab, 56–57
 GUI and CLI configuration, 54
 installing, 50
 locating and deploying devices, 52
 network configuration, 53
 network management menu, 52
 Physical tab, 54
 security settings, 327–332
 Services tab, 57–58
 uses of, 50–51
 Wireless Settings interface, 257–259

passwords, 310–312, 398–399–400, 409–410

patches, 313–314

peripherals, 35–36

personal data, 15–16

phishing, 303–304

physical addresses, 115–116

physical layer, troubleshooting, 423, 450
 cabling problems, 426
 using the senses, 423–424
 wireless router LEDs, 424–425

ping command, 84, 430–433

POP3 (Post Office Protocol), 241

popups, 307, 317

port forwarding, 340–341

port numbers, 220
 destination port, 221
 socket pairs, 221–223
 source port, 220
 well-known, 218–220

port triggering, 341–342

powering up switches, 355–357

pretexting, 303
private cloud, 276
private IPv4 addresses, 168–169
protocols, 90. *See also* communication protocols
 characteristics, 94
 communication, 91–93
 IMAP4 (Internet Message Access Protocol), 241
 importance of, 93–94
 models, 99
 OSI reference model, 99
 layers, 99–101
 TCP/IP and, 101–102
 POP3 (Post Office Protocol), 241
 server, 231
 SMTP (Simple Mail Transfer Protocol), 240–241
 stack, 97–98
 TCP/IP, 98
 layers, 99
 OSI reference model and, 101–102
public cloud, 276

Q-R

reference model, 99
remote hosts, 141, 152
RFID (radio frequency identification) tags, 13
RIRs (Regional Internet Registries), 170
routers, 359, 367–368
 boot process, 361
 as boundaries between networks, 195–196
 components, 360
 configuration, 395–397
 as gateways, 194–195
 home network, 252–253, 261
 design considerations, 261–262
 first time setup, 261
 interface ports, 360–361
 LEDs, 424–425
 management ports, 365–366
 passwords, 398–399–400
 ports, 252
 powering up, 361–364
 remote access, 399–400
 SSID (service set Identifier), 263–264
 wireless technology, 250–251
routing, 138, 141, 152
 broadcast containment, 138–139
 default gateway, 146–147
 DHCP and, 194–196
 distribution layer, 140
 security and, 139
 table, 142, 152
 entries, 145–146
 packet forwarding, 143–145
 path selection, 142–143
RTS (Request to Send), 260

S

SaaS (Software as a Service), 277
satellite Internet, 275
SDN (software-defined networking), 283–284
security
 antimalware software, 314–315
 antispymware software, 316–317
 antivirus software, 315–316
 botnets, 307
 brute force attacks, 310
 DDoS (distributed denial-of-service) attacks,
 309–310
 DoS (denial-of-service) attacks, 308–309
 MAC address filtering, 263–264
 malware, 304–305
 Trojan horse, 305–306
 viruses, 305
 worms, 305
 passwords, 310–312, 398–399, 409–410
 patches and updates, 313–314
 routing and, 139
 social engineering, 302–303
 phishing, 303–304
 pretexting, 303
 vishing, 304
 spyware, 306
 adware, 306
 popups, 307
 tracking cookies, 306
 systems, 10
 Telnet and, 238–239
 threats, 300–301
 external, 302
 internal, 301–302

- tools, 310, 312–313
- wireless network
 - DMZ (*demilitarized zone*), 339–340
 - firewalls, 338–340
 - MAC address filtering, 335
 - port forwarding, 340–341
 - port triggering, 341–342
 - SSID broadcasts, 333
 - vulnerabilities, 326–327
 - WEP (*Wired Equivalency Protocol*), 337–338
 - WPA (*Wi-Fi Protected Access*), 338
- sensors, 14
- server(s), 3, 213
 - DHCP (*Dynamic Host Configuration Protocol*), 184–185
 - DNS (*Domain Name System*), 232
 - FTP (*File Transfer Protocol*), 235–236
 - protocols, 231
 - single point of failure, 278
 - virtualization, 277–278
 - advantages of, 279
 - hypervisors, 279–280
 - web, 212, 233
 - client requests, 213
 - data center, 213
 - HTML (*Hypertext Markup Language*), 233–234
 - HTTP (*Hypertext Transfer Protocol*), 233–234
 - TCP/IP and, 215
 - URI (*Uniform Resource Identifier*), 214
- shortcuts, IOS command, 378–379
- show commands, 381–386
- signal transmission, 16–17
- single point of failure, 278
- SLAAC (*Stateless Address Autoconfiguration*), 203–204
- small home networks, 4–5
- smart cars, 12
- smart glasses, 9
- smart TVs, 11
- smartphones, 7–8. *See also* mobile devices
 - Android
 - cellular data settings, 288
 - Wi-Fi settings, 286–287
 - GPS (*global positioning system*), 33
 - iOS
 - cellular data settings, 289
 - Wi-Fi settings, 285–287
 - Wi-Fi
 - configuration, 286–287
 - settings, 285–286
- smartwatches, 8–9
- social engineering, 302–303
 - phishing, 303–304
 - pretexting, 303
 - vishing, 304
- socket pairs, 221–223
- SOHO (*small office/home office*) networks, 3, 4–5
- source port number, 220
- spam, 307, 317
- spyware, 306
 - adware, 306
 - popups, 307
 - tracking cookies, 306
- SSH (*Secure Shell*), 238–239, 399, 400–404, 410–411
- SSID (*service set Identifier*), 259, 263–264
- standards
 - communication, 95
 - Ethernet, 104–105
 - Internet and, 95
 - organizations, 95–96
- static address assignment, 182–183
- STP (*shielded twisted-pair*) cable, 75. *See also* twisted-pair cable
- subnet mask, 39, 164–166
- substitution approach to troubleshooting, 421
- switches, 123–124, 350–351, 367, 409
 - in-band management, 358
 - basic configuration, 392–393
 - default gateway, 406–407
 - LAN, 351
 - boot process, 355
 - expandability, 353
 - manageability, 353–354
 - ports, 352
 - powering up, 355–357
 - speed required, 352–353
 - LEDs, 424–425
 - out-of-band management, 358
 - passwords, 398–399–400
 - remote access, 399–400
 - running configuration file, 359

SSH configuration, 400–404
 startup configuration file, 358–359
 SVI configuration, 394

T

tablets, 8
 TCP (Transport Control Protocol), 216–217, 218–220
 TCP/IP, 98. *See also* transport layer layers, 99
 OSI reference model and, 101–102
 web servers and, 215
 Telnet, 237–239, 399
 text messaging, 242
 threats, 300–301
 external, 302
 internal, 301–302
 throughput, 18–19
 top-down troubleshooting, 419
 topologies, 42–43
 traceroute command, 81, 84
 tracert command, 433–434
 transport layer, 212, 216
 client/server interaction, 212–213–215
 netstat command and, 223
 port numbers, 218–220
 destination port, 221
 socket pairs, 221–223
 source port, 220
 TCP (Transport Control Protocol), 216–217
 UDP (User Datagram Protocol), 217–218
 troubleshooting, 418, 450
 bottom-up, 418–419
 commands, 426, 451
 ipconfig, 427–430
 netstat, 434–435
 nslookup, 436–437
 ping, 430–433
 tracert, 433–434
 comparison approach, 421
 divide-and-conquer, 420
 documentation, 416
 educated guess approach, 421
 follow-the-path, 420–421

gathering information, 416–417
 Internet connectivity, 442–443, 452–453
 DHCP server configuration errors, 441–442
 sources of help, 445
 support desk interaction, 445–449
 verify firewall settings, 444
 physical layer, 423–426, 450
 cabling problems, 426
 LEDs, 424–425
 using the senses, 423–424
 selecting a method, 422
 substitution approach, 421
 top-down, 419
 wireless networks, 438, 452
 authentication and association errors, 439–440
 causes of issues, 438
 tunneling, 202
 twisted-pair cable, 69–70, 71–72, 83
 STP (shielded twisted-pair), 75
 transmit and receive pairs, 79
 UTP (unshielded twisted-pair), 73–74
 wiring schemes, 78–79
 Type 1 hypervisors, 279–280
 Type 2 hypervisors, 280

U

UDP (User Datagram Protocol), 217–218–220
 unicast transmission, 171–172
 updates, 313–314
 URI (Uniform Resource Identifier), 214
 URL (Uniform Resource Locator), 214
 URN (Uniform Resource Name), 214
 UTP (unshielded twisted-pair) cable, 73–74. *See also* twisted-pair cable

V

virtual terminals, Telnet, 237–239
 virtualization, 277–278
 advantages of, 279
 hypervisors, 279
 Type 1, 279–280
 Type 2, 280
 network, 281

- control plane*, 282
- data plane*, 282
- SDN (software-defined networking) and*, 283–284

viruses, 305

- antivirus software and, 315–316
- signs of infection, 314–315

vishing, 304

VoIP (voice over IP), 243

vulnerabilities, wireless network

- default settings, 334
- open authentication, 336
- SSID broadcasts, 333

W

war driving, 327

war walking, 327

web servers

- client requests, 213
- data center, 213
- HTML (Hypertext Markup Language), 233–234
- HTTP (Hypertext Transfer Protocol), 233–234
- TCP/IP and, 215
- URI (Uniform Resource Identifier), 214

WEP (Wired Equivalency Protocol), 337–338

Wi-Fi, 34, 257

- cellular data settings, 288
 - Android*, 288
 - iOS*, 289
- configuring on mobile devices, 286–287
- mobile devices, 284–285

wireless networks, 32, 250–251. *See also* Wi-Fi

- authentication, 336–337
 - WEP (Wired Equivalency Protocol)*, 337–338
 - WPA (Wi-Fi Protected Access)*, 338
- Bluetooth, 34, 254, 290–291
- cell phone, 32–33
 - 5G, 32–33
 - GPS (global positioning system)*, 33
 - GSM (Global System for Mobile Communication)*, 32
- channels, 259
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 260
- CTS (Clear to Send), 260
- DMZ (demilitarized zone), 339–340
- electromagnetic spectrum, 253–254
- firewalls, 338–339
- IP addressing, 39–40
 - device names and address planning*, 41
 - DNS (Domain Name System)*, 40
 - dynamic configuration*, 41
 - manual configuration*, 40
- LAN (local-area network), 34–35
 - devices*, 36–37
 - Ethernet*, 38
 - hosts*, 35
 - media*, 37–38
 - NIC (network interface card)*, 38, 39
 - peripherals*, 35–36
- legacy mode, 262
- MAC address filtering, 263–264, 335
- NFC (near-field communication), 34
- port forwarding, 340–341
- port triggering, 341–342
- routers, 261
 - design considerations*, 261–262
 - first time setup*, 261
- RTS (Request to Send), 260
- shared media, 260–261
- SSID (service set Identifier), 259
- troubleshooting, 438–439, 452
 - authentication and association errors*, 439–440
 - causes of issues*, 438
- vulnerabilities, 326–327
 - default settings*, 334
 - open authentication*, 336
 - SSID broadcasts*, 333

Wi-Fi, 34, 257

- mobile devices*, 284–285
- wireless frequencies, 254–255

worldwide networks, 6–7

worms, 305, 314–315

WPA (Wi-Fi Protected Access), 338

X-Y-Z

zombies, 307