



Review Exercises

31 Days Before Your CCST Networking Exam

A Day-By-Day Review Guide
for the CCST Networking
100-150 Certification Exam

ciscopress.com

Allan Johnson

FREE SAMPLE CHAPTER |



31 Days Before Your Cisco Certified Support Technician (CCST) Networking 100-150 Exam

A Day-By-Day Review Guide for the
CCST-Networking Certification Exam

Allan Johnson

31 Days Before Your Cisco Certified Support Technician (CCST) Networking 100-150 Exam

Allan Johnson

Copyright © 2024 Cisco Systems, Inc.

Published by:

Cisco Press

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

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

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose all such documents and related graphics are provided “as is” without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

\$PrintCode

Library of Congress Control Number: 2024902156

ISBN-13: 978-0-13-822291-8

ISBN-10: 0-13-822291-6

Warning and Disclaimer

This book is designed to provide information about exam topics for the Cisco Certified Support Technician (CCST) certification. 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 author, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

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

Trademark Acknowledgments

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

Special Sales

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

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

GM K12, Early Career and Professional Learning

Alliances Manager, Cisco Press

Director, ITP Product Management

Executive Editor

Managing Editor

Development Editor

Senior Project Editor

Copy Editor

Technical Editor

Editorial Assistant

Designer

Composition

Indexer

Proofreader

Soo Kang

Caroline Antonio

Brett Bartow

James Manly

Sandra Schroeder

Ellie C. Bru

Mandie Frank

Bart Reed

Patrick Gargano

Cindy Teeters

Chuti Prasertsith

CodeMantra

Ken Johnson

Jennifer Hinchliffe

About the Author

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 an account lead for Unicon (unicon.net) supporting Cisco's educational efforts.

About the Technical Reviewer

Patrick Gargano is a lead content advocate and instructor on the Technical Education team within Learning & Certifications at Cisco. Before joining Cisco in 2021, he worked as a Cisco Networking Academy instructor and instructor-trainer since 2000, and as a Certified Cisco Systems Instructor (CCSI) since 2005 for Fast Lane UK, Skyline ATS, and NterOne teaching CCNA and CCNP courses. Recently, he was responsible for developing Cisco's official ENARSI, ENSDWI, ENCC, SDWFND, and SDWSCS course content. He has published four Cisco Press books, and he holds CCNA, CyberOps Associate, and CCNP Enterprise certifications. He also holds BEd and BA degrees from the University of Ottawa and has a Master of Professional Studies (MPS) degree in computer networking from Fort Hays State University. He is a regular speaker at Cisco Live, presenting on topics related to SD-WAN and network troubleshooting. He lives in Quebec, Canada with his wife and son.

Dedications

For my wife, Becky. Thank you for all your support during this crazy whirlwind of a year. You are the stabilizing force that keeps me grounded.

Acknowledgments

As a technical author, I rely heavily on my technical editor; Patrick Gargano had my back for this work. Thankfully, when James Manly contacted him, he was willing and able to do the arduous review work necessary to make sure that you get a book that is both technically accurate and unambiguous.

Russ White's *Cisco Certified Support Technician CCST Networking 100-150 Official Cert Guide, First Edition* was one of my main sources. Russ is well known in the computer networking community where he is a highly respected expert. I recommend subscribing to the podcast *Hedge*, where Russ is a co-host.

The Cisco Network Academy authors for the online curriculum take the reader deeper, past the CCST Networking exam topics, with the ultimate goal of preparing the student not only for CCST Networking certification, but for more advanced college-level technology courses and degrees as well. Thank you especially to Rick Graziani, Bob Vachon, John Pickard, Dave Holzinger, Martin Benson, Suk-Yi Pennock, Allan Reid, Anna Bolen and the rest of the ACE team. Their excellent treatment of the material is reflected throughout this book.

James Manly, executive editor, effectively juggles multiple projects simultaneously, steering each from beginning to end. Thank you, James, for shepherding this project for me.

Thank you to the professional and thorough review of this work by development editor Ellie Bru, project editor Mandie Frank, and copy editor Bart Reed. Their combined efforts ensure that what I authored is ready for publication.

And to the rest of the Pearson family who contributes in countless ways to bring a book to the reader, thank you for all your hard work.

Contents at a Glance

Day 31: Networking Models	1
Day 30: TCP/IP Layer Functions	5
Day 29: Data Encapsulation	9
Day 28: Measuring Network Performance	13
Day 27: Network Topologies	21
Day 26: Cloud Computing	31
Day 25: Transport Protocols	37
Day 24: FTP, NTP, and ICMP	43
Day 23: HTTP, DHCP, and DNS	55
Day 22: Private Addressing and NAT	63
Day 21: IPv4 Addressing	69
Day 20: IPv6 Addressing	77
Day 19: Cables and Connectors	91
Day 18: Wireless Technologies	105
Day 17: Endpoint Devices	113
Day 16: Configure PC and Mobile Access	121
Day 15: Device Status Lights	139
Day 14: Connecting Cables	143
Day 13: Device Ports	151
Day 12: Routing Concepts	155
Day 11: Switching Concepts	169
Day 10: Troubleshooting and Help Desks	177
Day 9: Wireshark	185
Day 8: Diagnostic Commands	191
Day 7: Device Management	205
Day 6: Show Commands	215
Day 5: Firewalls	227
Day 4: Threats, Vulnerabilities, and Attacks	235

Day 3: Security Protocols and Practices	245
Day 2: Secure Wireless Access	253
Day 1: Review and Practice	267
Exam Day	269
Post-Exam Information	271
CCST Networking Countdown Calendar	273
Exam Checklist	275
Index	279

Reader Services

Register your copy at www.ciscopress.com/title/9780138222918 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9780138222918 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Contents

Day 31: Networking Models 1

- CCST Networking Exam Topic 1
- Key Topics 1
- The OSI and TCP/IP Models 1
 - OSI Layers 2
 - TCP/IP Layers and Protocols 3
- Study Resources 4

Day 30: TCP/IP Layer Functions 5

- CCST Networking 100-150 Exam Topic 5
- Key Topics 5
- The TCP/IP Application Layer 5
- The TCP/IP Transport Layer 5
- The TCP/IP Internet Layer 6
- The TCP/IP Network Access Layer 7
- Study Resources 8

Day 29: Data Encapsulation 9

- CCST Networking 100-150 Exam Topic 9
- Key Topics 9
- Data Encapsulation Summary 9
- Encapsulating in Tunnels 10
- Study Resources 11

Day 28: Measuring Network Performance 13

- CCST Networking 100-150 Exam Topic 13
- Key Topics 13
- Bandwidth, Throughput, and Goodput 13
 - Bandwidth 13
 - Throughput 13
 - Goodput 14
 - End-to-End Bandwidth 14
- Sources of Delay 15
 - Physical Path Length 15
 - Serialization Delay 15

Queueing Delay 15

Jitter 15

Speed Tests 16

The iPerf Tool 17

Study Resources 20

Day 27: Network Topologies 21

CCST Networking 100-150 Exam Topic 21

Key Topics 21

LANs and WANs 21

LANs 21

LAN Topologies 21

WANs 22

WAN Topologies 23

Physical and Logical Topologies 24

Topology Variations 26

Small Office/Home Office (SOHO) 26

SOHO Routers 27

Hierarchical Campus Design 27

Study Resources 29

Day 26: Cloud Computing 31

CCST Networking 100-150 Exam Topic 31

Key Topics 31

On-Premises Computing 31

Cloud Computing 32

Cloud Computing Services 33

Server Virtualization 34

Study Resources 36

Day 25: Transport Protocols 37

CCST Networking 100-150 Exam Topic 37

Key Topics 37

TCP and UDP 37

TCP Header 38

Port Numbers 38

Error Recovery 39

- Flow Control 40
- Connection Establishment and Termination 40
- UDP 41

Study Resources 42

Day 24: FTP, NTP, and ICMP 43

CCST Networking 100-150 Exam Topic 43

Key Topics 43

File Transfer Protocols 43

- FTP 43

- SFTP 45

- TFTP 46

NTP 46

- NTP Configuration and Verification 47

Internet Control Message Protocol (ICMP) 48

- ICMPv4 and ICMPv6 48

- Ping and Traceroute 49

- ICMPv6 Messages 51

- RA Message 51

- RS Message 51

- NS Message 52

- NA Message 52

Study Resources 53

Day 23: HTTP, DHCP, and DNS 55

CCST Networking 100-150 Exam Topic 55

Key Topics 55

HTTP 55

- HTTP Operation 56

DHCP 57

- DHCPv4 58

- DHCPv6 58

- SLAAC 58

- Stateless and Stateful DHCPv6 Operation 60

DNS Operation 61

Study Resources 62

Day 22: Private Addressing and NAT 63

CCST Networking 100-150 Exam Topic 63

Key Topics 63

Private Addressing 63

Reserved Addresses 63

NAT Concepts 64

A NAT Example 66

Dynamic and Static NAT 66

NAT Overload 67

NAT Benefits 68

NAT Limitations 68

Study Resources 68

Day 21: IPv4 Addressing 69

CCST Networking 100-150 Exam Topic 69

Key Topics 69

IPv4 Addressing 69

Header Format 69

Classes of Addresses 70

Purpose of the Subnet Mask 71

Subnetting in Four Steps 72

Determine How Many Bits to Borrow 72

Determine the New Subnet Mask 73

Determine the Subnet Multiplier 74

List the Subnets, Host Ranges, and Broadcast Addresses 74

Subnetting Example 1 74

Subnetting Example 2 75

Subnetting Example 3 75

Study Resources 76

Day 20: IPv6 Addressing 77

CCST Networking 100-150 Exam Topic 77

Key Topics 77

Overview and Benefits of IPv6 77

The IPv6 Protocol 78

IPv6 Address Types 79

Unicast 80

Global Unicast Address 80

Link-Local Address 82

- Loopback Address 83
- Unspecified Address 83
- Unique Local Address 84
- IPv4 Embedded Address 84
- Multicast 85
 - Assigned Multicast 85
 - Solicited-Node Multicast 86
- Anycast 87
- Representing the IPv6 Address 88
 - Conventions for Writing IPv6 Addresses 88
 - Conventions for Writing IPv6 Prefixes 88
- Migration to IPv6 89
- Study Resources 90

Day 19: Cables and Connectors 91

- CCST Networking 100-150 Exam Topic 91
- Key Topics 91
- Network Media Forms and Standards 91
- Copper Cabling 93
 - Unshielded Twisted Pair (UTP) 94
 - Shielded Twisted Pair (STP) 95
 - Coaxial Cable 95
- UTP Cabling Standards and Connectors 96
 - UTP Categories 96
 - UTP Connectors 97
 - Straight-through and Crossover UTP Cables 97
- Fiber-Optic Cabling 98
 - Types of Fiber Media 98
 - Single-Mode Fiber (SMF) 99
 - Multimode Fiber (MMF) 99
 - Fiber-Optic Connectors 100
 - Fiber Patch Cords 101
 - Fiber versus Copper 104
- Study Resources 104

Day 18: Wireless Technologies 105

- CCST Networking 100-150 Exam Topic 105
- Key Topics 105
- Wi-Fi 105
 - RF Spectrum 105

Channels 105
802.11 Standards 107
Wireless Interference 108
Wi-Fi Networks 109

Cellular Networks 110
5G Cellular Network Components 110
Radio Access Network (RAN) 111
Mobile Core 111
Advantages and Disadvantages of Cellular Networks 111
Study Resources 112

Day 17: Endpoint Devices 113

CCST Networking 100-150 Exam Topic 113
Key Topics 113
Hosts 113
 Sending a Packet 114
 Virtual Hosts 114
Mobile Devices 116
 Early Developments 116
 The Advent of Mobile Phones 116
 The Smartphone Era 116
 Tablets and Phablets 117
 Operating Systems 117
Internet of Things 117
Study Resources 119

Day 16: Configure PC and Mobile Access 121

CCST Networking 100-150 Exam Topic 121
Key Topics 121
Windows 121
 The Settings App 121
 The Control Panel 122
 The Command Line 124
 Verifying Connectivity 127
Linux 129
 Verifying Connectivity 130
Finding Your Public IP Address 132
macOS 132

- Mobile Devices 134
 - Verify Connectivity 135
 - iOS 135
 - Android 135

Study Resources 138

Day 15: Device Status Lights 139

CCST Networking 100-150 Exam Topic 139

Key Topics 139

Cisco Device Link Lights 139

Study Resources 141

Day 14: Connecting Cables 143

CCST Networking 100-150 Exam Topic 143

Key Topics 143

Networking Icons 143

Switches 143

- Access Layer Switches 144

- Distribution Layer Switches 145

- Core Layer Switches 145

LAN Device Connection Guidelines 145

Physical and Logical Topologies 146

Topology Examples 147

- Physical Topology Example 147

- Logical Topology Example 148

Cable Management 149

Study Resources 150

Day 13: Device Ports 151

CCST Networking 100-150 Exam Topic 151

Key Topics 151

Cisco 4461 ISR Ports 151

- Fixed Ports and NIMs 151

- SM-X Slots 153

Study Resources 154

Day 12: Routing Concepts 155

- CCST Networking 100-150 Exam Topic 155
- Key Topics 155
- Packet Forwarding 155
 - Path Determination and Switching Function Example 156
- Routing Methods 157
- Classifying Dynamic Routing Protocols 158
 - IGP and EGP 159
 - Distance Vector Routing Protocols 159
 - Link-State Routing Protocols 159
 - Classful Routing Protocols 160
 - Classless Routing Protocols 160
- Dynamic Routing Metrics 160
- Administrative Distance 161
- IGP Comparison Summary 163
- Routing Loop Prevention 163
- Link-State Routing Protocol Features 164
 - Building the Link-State Database 164
 - Calculating the Dijkstra Algorithm 165
 - Convergence with Link-State Protocols 166
- Study Resources 167

Day 11: Switching Concepts 169

- CCST Networking 100-150 Exam Topic 169
- Key Topics 169
- Evolution to Switching 169
- Switching Logic 170
- Collision and Broadcast Domains 171
- Frame Forwarding 171
 - Switch Forwarding Methods 171
 - Symmetric and Asymmetric Switching 172
 - Memory Buffering 172
 - Layer 2 and Layer 3 Switching 172
- VLAN Concepts 172
 - Traffic Types 173
 - Types of VLANs 174
 - Voice VLAN Example 175
- Study Resources 175

Day 10: Troubleshooting and Help Desks 177

CCST Networking 100-150 Exam Topic 177

Key Topics 177

Troubleshooting Methodology Overview 177

Structured Troubleshooting Methods 178

Help Desks 180

Policies and Procedures 180

Prioritization and Escalation 180

Ticketing Systems 181

Study Resources 183

Day 9: Wireshark 185

CCST Networking 100-150 Exam Topic 185

Key Topics 185

Wireshark Overview 185

Features 185

Who Uses Wireshark? 186

Wireshark Packet Capture 186

Download and Install Wireshark 186

Save a Packet Capture 187

Open a Packet Capture 189

Study Resources 189

Day 8: Diagnostic Commands 191

CCST Networking 100-150 Exam Topic 191

Key Topics 191

IP Diagnostic Commands 191

The ipconfig Command 191

The ifconfig Command 194

The ip Command 195

The ip addr Command 195

The ip addr add Command 196

The ip route Command 197

The ip neigh Command 197

The ping Command 197

The tracert Command 201

The nslookup Command 203

Study Resources 204

Day 7: Device Management 205

CCST Networking 100-150 Exam Topic 205

Key Topics 205

Remote Access 205

RDP 205

SSH 206

Telnet 207

Virtual Private Networks (VPNs) 207

Windows VPN Configuration 207

Scripting a VPN Connection 207

Terminal Emulators 208

Consoles 209

Network Management Systems 210

NMS Functions 210

Network Management Tools 211

Simple Network Management Protocol (SNMP) 211

Command-Line Interfaces (CLI) 211

REST APIs 211

Syslog 211

NetFlow 211

Network Cloud Management Using Meraki 211

Meraki Dashboard Features 212

APIs and Advanced Control 212

Study Resources 213

Day 6: Show Commands 215

CCST Networking 100-150 Exam Topic 215

Key Topics 215

Cisco IOS Help Facility 215

Command Auto-Complete 216

Privilege Levels 216

Cisco Discovery Protocol (CDP) 218

Common show Commands 219

The show ip interface brief Command 226

Study Resources 226

Day 5: Firewalls 227

CCST Networking 100-150 Exam Topic 227

Key Topics 227

Firewall Devices 227

Stateless Firewalls 227

Stateful Firewalls 229

Application Gateway Firewalls 229

Next-Generation Firewalls 229

Cisco IOS Firewall Configuration Example 230

Host-Based Firewalls 231

Windows Defender Firewall 231

iptables 232

nftables 232

TCP Wrappers 233

Study Resources 233

Day 4: Threats, Vulnerabilities, and Attacks 235

CCST Networking 100-150 Exam Topic 235

Key Topics 235

Security Fundamentals 235

Security Terms 235

Data Exfiltration 236

Penetration Testing Tools 236

Attack Types 237

Types of Malware 238

Network Attacks 239

Reconnaissance Attacks 239

Access Attacks 240

Social Engineering Attacks 240

DoS and DDoS Attacks 241

IP Attacks 241

Transport Layer Attacks 242

Study Resources 243

Day 3: Security Protocols and Practices 245

CCST Networking 100-150 Exam Topic 245

Key Topics 245

Security Fundamentals 245

The Cybersecurity Cube 245

Security Principles 245

Data States	246
Safeguards	246
The CIA Triad	247
Confidentiality	248
Integrity	248
Availability	249
Access Control	249
Types of Access Control	249
Physical Access Control	249
Logical Access Control	249
Administrative Access Control	249
Authentication, Authorization, and Accounting (AAA)	250
Authentication	250
Authorization	250
Accounting	250
Identity Stores	251
AD Functions	251
AD Key Components	251
Security Program	251
Study Resources	252

Day 2: Secure Wireless Access 253

CCST Networking 100-150 Exam Topic	253
Key Topics	253
Wireless Attacks and Security	253
DoS Attacks	253
Rogue Access Points	254
Man-in-the-Middle Attack	254
SSID Cloaking	255
MAC Addresses Filtering	255
Shared Key Authentication Methods	256
Authenticating a Home User	256
Encryption Methods	257
Home Router Configuration	258
Log in to the Wireless Router	258
Basic Network Setup	259
Step 1: Log in to the router from a web browser.	259
Step 2: Change the default administrative password.	259
Step 3: Log in with the new administrative password.	260
Step 4: Change the default DHCP IPv4 addresses.	261
Step 5: Renew the IP address.	262
Step 6: Log in to the router with the new IP address.	262

Basic Wireless Setup 262

Step 1: View the WLAN defaults. 262

Step 2: Change the network mode. 263

Step 3: Configure the SSID. 264

Step 4: Configure the channel. 264

Step 5: Configure the security mode. 264

Step 6: Configure the passphrase. 266

Step 7: Verify connectivity for devices connected to the router. 266

Study Resources 266

Day 1: Review and Practice 267

Configure a Home Network 267

Instructions 267

Exam Day 269

What You Need for the Exam 269

What You Should Receive After Completion 270

Summary 270

Post-Exam Information 271

Receiving Your Certificate and Badge 271

Determining Career Options 271

Examining Certification Options 272

If You Did Not Pass the Exam 272

Summary 272

CCST Networking Countdown Calendar 273

Exam Checklist 275

Index 279

Icons Used in This Book



Access Point



Switch



Router



Printer



Clock



Server



WWW Server



ASA 5500



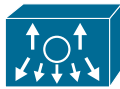
Phone



Laptop



File Server



Cisco Nexus 1000



Cloud



Firewall



Terminal

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

If you're reading this introduction, you've probably already spent a considerable amount of time and energy pursuing your CCST Networking certification. Regardless of how you got to this point in your travels through your studies, *31 Days Before Your Cisco Certified Support Technician (CCST) Networking 100-150 Exam* most likely represents the last leg of your journey on your way to the destination: to become a Cisco Certified Support Technician in Networking. However, if you are like me, you might be reading this book at the *beginning* of your studies. If so, this book provides an excellent overview of the material you must now spend a great deal of time studying and practicing. But I must warn you: unless you are extremely well-versed in networking technologies and have considerable experience supporting networks, this book will *not* serve you well as the sole resource for your exam preparations. Therefore, let me spend some time discussing my recommendations for study resources.

Study Resources

Cisco Press and Pearson IT Certification offer an abundance of networking-related books to serve as your primary source for learning how to install, configure, operate, and troubleshoot small to medium-size routed and switched networks.

Safari Books Online

All the resources I reference in the book are available with a subscription to Safari Books Online (<https://www.safaribooksonline.com>). If you don't have an account, you can try it free for ten days.

Primary Resources

First on the list must be Russ White's *Cisco Certified Support Technician CCST Networking 100-150 Official Cert Guide 1st Edition* (ISBN: 9780138213428). If you do not buy any other books, buy this one. Russ's method of teaching, combined with his technical expertise and down-to-earth style, is unsurpassed in our industry. As you read through his book, you sense that he is sitting right there next to you walking you through the material. With your purchase, you get access to practice exams and study materials and other online resources that are worth the price of the book. There is no better resource on the market for a CCST Networking candidate.

If you are a Cisco Networking Academy student, you are blessed with access to the online version of the Networking Essentials version 3 curriculum and the wildly popular Packet Tracer network simulator. However, this content is also available for free to anyone who signs up at <https://skillsforall.com>. After registering and logging in, look for the Network Technician Career Path (<https://skillsforall.com/career-path/network-technician>). Here, you can gain access to the following four mini-courses that add up to 70 hours of training:

- Networking Basics
- Networking Devices and Initial Configuration
- Network Addressing and Basic Troubleshooting
- Network Support and Security

You can also buy *Networking Essentials Companion Guide v3: Cisco Certified Support Technician (CCST) Networking 100-150, Second Edition* (ISBN: 978-0-13-832133-8), which maps to both the Networking Essentials version 3 instructor-led online course and the four self-enroll mini-courses. You might also consider purchasing *Networking Essentials Lab Manual v3: Cisco Certified Support Technician (CCST) Networking 100-150, 2nd Edition* (ISBN: 9780138293727). You can find these books at <http://www.ciscopress.com> by clicking the Cisco Networking Academy link.

The Cisco Learning Network

Finally, if you have not done so already, you should register with The Cisco Learning Network at <https://learningnetwork.cisco.com>. Sponsored by Cisco, The Cisco Learning Network is a free social learning network where IT professionals can engage in the common pursuit of enhancing and advancing their IT careers. Here, you can find many resources to help you prepare for your CCST Networking exam, in addition to a community of like-minded people ready to answer your questions, help you with your struggles, and share in your triumphs.

So which resources should you buy? The answer to that question depends largely on how deep your pockets are or how much you like books. If you're like me, you must have it all! I admit it; my bookcase is a testament to my Cisco "geekness." Whatever you choose, you will be in good hands. Any or all of these resources will serve you well.

Goals and Methods

The main goal of this book is to provide you with a clear and succinct review of the CCST Networking objectives. Each day, we will review an exam topic, starting with the first one and proceeding through the list objectives until they are all covered. Each day is structured using the following format:

- A title for the day that concisely states the overall topic
- A list of one or more CCST Networking 100-150 exam topics to be reviewed
- A "Key Topics" section to introduce the review material and quickly orient you to the day's focus
- An extensive review section consisting of short paragraphs, lists, tables, examples, and graphics
- A "Study Resources" section to give you a quick reference for locating more in-depth treatment of the day's topics

The book counts down starting with Day 31 and continues through exam day to provide post-test information. Inside this book is also a calendar and checklist that you can tear out and use during your exam preparation.

Use the calendar to enter each actual date beside the countdown day and the exact day, time, and location of your CCST Networking exam. The calendar provides a visual for the time you can dedicate to each exam topic.

The checklist highlights important tasks and deadlines leading up to your exam. Use it to help you map out your studies.

Who Should Read This Book?

The audience for this book is anyone finishing preparation for taking the CCST Networking 100-150 exam. A secondary audience is anyone needing a refresher review of CCST Networking exam topics, possibly as a review before attempting to sit for another certification for which the CCST Networking exam topics provide a foundation.

Getting to Know the CCST Networking 100-150 Exam

Cisco announced the current CCST Networking 100-150 exam in January 2023. This certification is aimed at entry-level network technicians, networking students, and interns. It tests foundational knowledge and skills in network operation, including the understanding of devices, media, and protocols vital for network communication. This certification serves as an entry point into the Cisco certification program, with CCNA being the next level. The exam is targeted toward secondary and post-secondary students, as well as entry-level IT and Networking professionals. To qualify, candidates should have a minimum of 150 hours of instruction and hands-on experience, and successful candidates will be recognized as qualified entry-level network technicians and customer support technicians.

To earn your certification, you must pass a 50-minute exam composed of 35 to 50 questions. Certiport has an exam tutorial here:

https://certiport.pearsonvue.com/Educator-resources/Exam-details/Exam-tutorials/Cisco_Tutorial.pdf

If that link doesn't work, be sure to register at <https://www.certiport.com> and then look for the exam tutorials link. One of the nice features of the CCST Networking exam is that you can move forward and back through test items, changing your answers if desired, before the exam ends or you select **Finish**.

What Topics Are Covered on the CCST Networking Exam

The six domains of the CCST Networking 100-150 exam are as follows:

- 1.0 Standards and Concepts
- 2.0 Addressing and Subnet Formats
- 3.0 Endpoints and Media Types
- 4.0 Infrastructure
- 5.0 Diagnosing Problems
- 6.0 Security

Although Cisco outlines general exam topics, not all topics might appear on the CCST Networking exam; likewise, topics that are not specifically listed might appear on the exam. The exam topics that Cisco provides and this book covers are a general framework for exam preparation. Be sure to check Cisco's website for the latest exam topics.

Purchase an Exam Voucher and Schedule Your Exam

If you are starting *31 Days Before Your Cisco Certified Support Technician (CCST) Networking 100-150 Exam* today, register with Certiport (<https://www.certiport.com>) and purchase your exam voucher right now. Next, use Certiport's locator to find a testing center (<https://www.certiport.com/locator>). Many testing centers provide remote testing in your chosen space. In my testing experience, there is no better motivator than a scheduled test date staring me in the face. I'm willing to bet the same holds true for you. So, if you're ready, gather the following information and register right now!

- Legal name
- Social Security or passport number
- Company name
- Valid email address
- Method of payment

You can schedule your exam at any time. I recommend that you schedule it for 31 days from now. The process and available test times vary based on the local testing center you choose.

Remember, there is no better motivation for study than an actual test date. *Sign up today.*

Credits

Figures 2.3–2.6, 2.8–2.19: Linksys Holdings

Figures 5.4, 7.1, 7.2, 16.1–16.5: Microsoft Corporation

Figure 7.3: PuTTY

Figures 9.1– 9.3: Wireshark Foundation

Figure 14.5a: Wavebreakmedia/Shutterstock

Figure 14.5b: WhiteYura/Shutterstock

Figure 16.6: The Linux Foundation

Figures 16.7, 16.8, 16.10: Apple Inc

Figures 16.9, 16.11: Google LLC

Figure 19.1a: Galushko Sergey/Shutterstock

Figure 19.1b: ZayacSK/Shutterstock

Figure 19.1c: Ra3rn/Shutterstock

Figure 19.4b: Monte_a/Shutterstock

Figure 19.4c: Nattapan72/Shutterstock

Figure 19.4d: Darkroom Graphic/Shutterstock

Figure 19.5a: Peter Kotoff/Shutterstock

Figure 19.5b: Rogerutting/123RF

Figure 19.6a: Shaffandi/123RF

Figure 19.6b: Shahril KHMD/Shutterstock

Figure 19.10: Datskevich Aleh/Shutterstock

Figure 19.11: tom_tom_13/Shutterstock

Figure 19.12: Artush/123RF

Figure 19.13: Horvathta/Shutterstock

Figure 19.15: Suyanawut/123RF

Figures 19.14, 19.16, 19.17: Andrey Renteev/Shutterstock

Figures 28.5, 28.6: Ookla, LLC

Measuring Network Performance

CCST Networking 100-150 Exam Topic

- 1.2. Differentiate between bandwidth and throughput.
 - *Latency, delay, speed test vs. iPerf*
-

Key Topics

Today's review focuses on the different measurements for network performance, the sources of delay, testing network performance online, and testing network performance using the Windows iPerf tool.

Bandwidth, Throughput, and Goodput

There are three basic measurements for network performance: bandwidth, throughput, and goodput.

Bandwidth

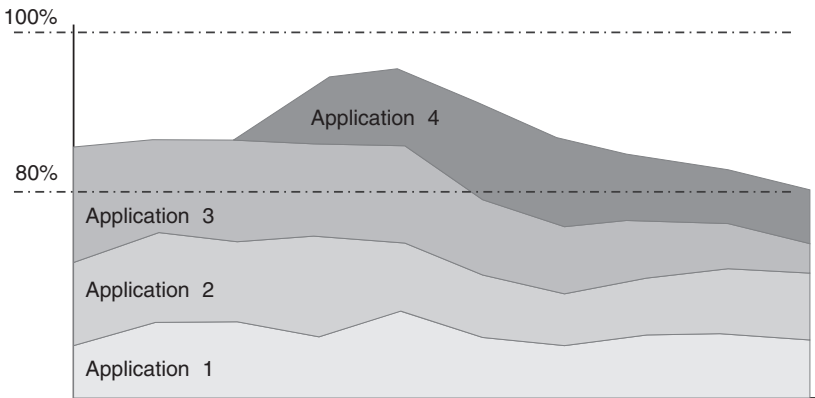
Bandwidth is determined by the medium's physical properties and is measured in bits per second. For example, 10GBASE-T Ethernet has a maximum capacity of 10Gbps (gigabits per second). The available bandwidth of a connection is how Internet service providers (ISPs) advertise and charge for their services.

Throughput

Throughput is the actual rate of data transfer across the network and will be less than the bandwidth. This is because there is overhead on the link, such as routing protocols, Layer 2 minimum frame sizes (Ethernet), network congestion, and more.

Another important reason that throughput is less than bandwidth is because network engineers want to ensure the link has enough capacity to adjust to new demand bursts. For example, in Figure 28-1, Application 4 might not be able to start if the other three applications are consuming closer to 100% of the link's capacity. For this reason, it is common for network designers to consider a link at 80% bandwidth utilization as full utilization.

Figure 28-1 Providing Enough Bandwidth for Another Application to Start



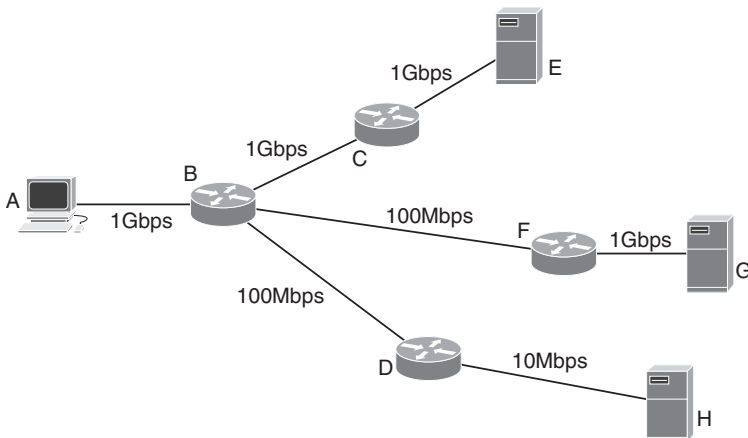
Goodput

Although less commonly mentioned, goodput is the measure of the actual payload of data that is transmitted across the network. Goodput will always be less than throughput because every data packet contains fields of overhead. For example, Ethernet has a 20-byte header and IPv6 has a 40-byte header. In addition, there will always be a small number of errors in data transmission where packets must be retransmitted.

End-to-End Bandwidth

The bandwidth of an end-to-end path is limited by the lowest bandwidth link along the path. For example, a 1Gbps local link does not guarantee 1Gbps to all destinations. In Figure 28-2, Host A will have an end-to-end bandwidth of 1Gbps to Server E. However, Host A will be limited to 100Mbps to Server G and 10Mbps to Server H.

Figure 28-2 Lowest Bandwidth Link Determines End-to-End Bandwidth



Sources of Delay

Delay is the time it takes for a packet to travel from source to destination. Sources of delay include the following:

- The physical path length
- The time it takes to transmit data onto the wire (serialization delay)
- Queuing when there is congestion between the source and destination
- Jitter, which is the measure of difference in delay between packets

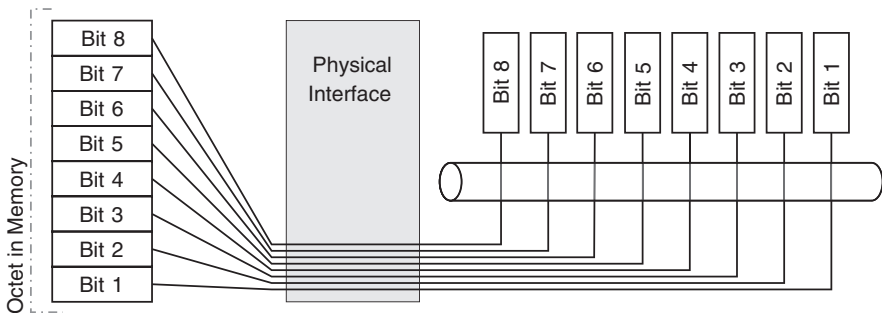
Physical Path Length

Physical path length is the actual distance that packets need to travel from the source to the destination. The physical path length is a fundamental factor in determining delay, as it contributes to the overall time it takes for a signal to traverse the distance. In general, longer physical paths result in higher delays.

Serialization Delay

Serialization delay refers to the time it takes to convert digital data into a stream of bits and transmit it onto the network. This process involves encoding the data and sending it out as a series of bits, as shown for the 8 bits in Figure 28-3.

Figure 28-3 Converting Digital Bits to the Physical Medium



Queueing Delay

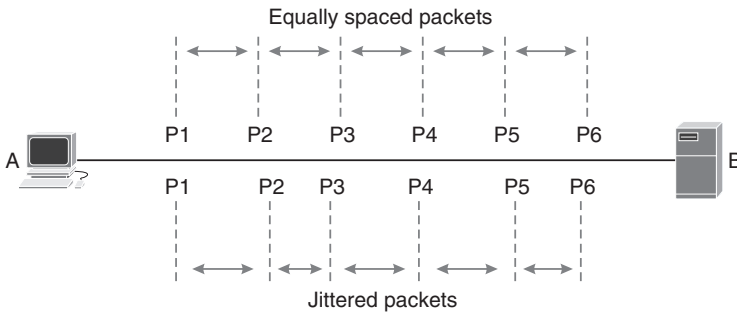
Queueing delay occurs when there is congestion or contention for resources within the network. When multiple packets are trying to traverse the same network link simultaneously, they may have to wait in a queue before they can be transmitted. This queueing delay is directly related to network traffic and the network's capacity. Higher levels of congestion lead to longer queueing delays.

Jitter

Jitter is the measure of variation in delay between packets. In an ideal network, packets would all arrive at the destination with consistent and predictable delays, as shown for the top row of packets in Figure 28-4. However, in real-world networks, factors such as varying traffic loads,

different routing paths, and queuing delays can introduce variation in the arrival times of packets, as shown in the bottom row of packets in Figure 28-4.

Figure 28-4 An Example of Equally Spaced and Jittered Packets

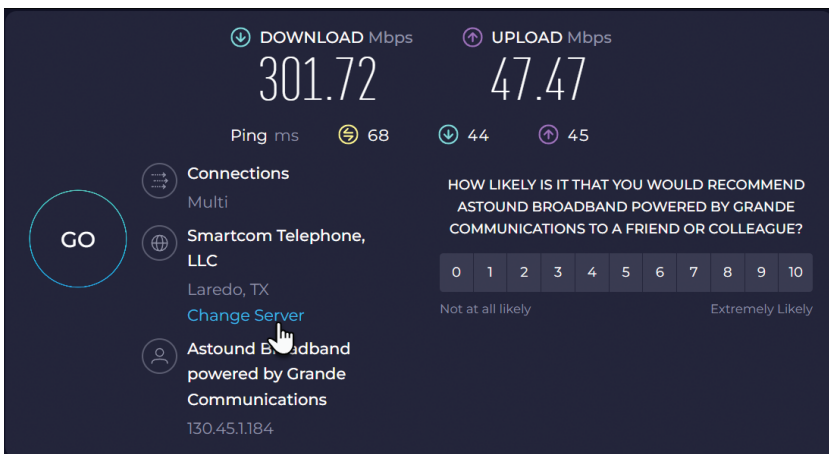


Jitter can be a significant issue in real-time applications like Voice over Internet Protocol (VoIP) or video streaming applications, where consistent timing is essential. To mitigate jitter, network engineers often use techniques like quality of service (QoS) to prioritize certain types of traffic and reduce variability in delay.

Speed Tests

It's relatively easy for you to test the speed of your personal Internet connections. A quick Internet search will reveal several ad-supported sites that provide this service for free. Speed tests measure the throughput of your link. Specifically, they measure the throughput between you and the destination server that the speed test chooses for your test. Some speed tests, such as the one provided by Ookla, allow you to change the destination server, as shown in Figure 28-5.

Figure 28-5 Example of a Web-Based Speed Test by Ookla



Ookla also has an app you can use to test the throughput of your cellular bandwidth, as shown in Figure 28-6.

Figure 28-6 Ookla’s Mobile App Speedtest



The iPerf Tool

Although there are a variety of other tools you could download for measuring your network’s performance, the CCST-Networking exam specifically calls out the iPerf tool. As of this writing, iPerf is in version 3 and can be downloaded for all the major operating systems at <https://iperf.fr>.

Example 28-1 shows the iPerf tool running on a Windows machine, testing the connection to a public iPerf server in Dallas.

Example 28-1 Output from the iPerf Windows Tool

```
C:\tools\iperf-3.1.3-win32> iperf3 -c dal.speedtest.clouvider.net
Connecting to host dal.speedtest.clouvider.net, port 5200
[ 4] local 192.168.68.106 port 61680 connected to 2.56.188.136 port 5200
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-1.00   sec    441 KBytes  3.60 Mbits/sec
[ 4]  1.00-2.00   sec    756 KBytes  6.19 Mbits/sec
[ 4]  2.00-3.01   sec    756 KBytes  6.18 Mbits/sec
[ 4]  3.01-4.00   sec    693 KBytes  5.68 Mbits/sec
[ 4]  4.00-5.00   sec    756 KBytes  6.20 Mbits/sec
[ 4]  5.00-6.00   sec    756 KBytes  6.19 Mbits/sec
[ 4]  6.00-7.00   sec    756 KBytes  6.21 Mbits/sec
[ 4]  7.00-8.00   sec    756 KBytes  6.20 Mbits/sec
[ 4]  8.00-9.01   sec    819 KBytes  6.62 Mbits/sec
[ 4]  9.01-10.01  sec    819 KBytes  6.71 Mbits/sec
- - - - -
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-10.01  sec    7.14 MBytes  5.98 Mbits/sec  sender
[ 4]  0.00-10.01  sec    7.14 MBytes  5.98 Mbits/sec  receiver

iperf Done.

C:\tools\iperf-3.1.3-win32>
```

NOTE You can easily find available iPerf public servers by doing an Internet search. The server chosen for Example 28-1 was found at <https://github.com/R0GGER/public-iperf3-servers>.

In Example 28-1, the number of kilobytes of data being transferred is measured every second. This value is then converted into the number of bits per second. After 10 seconds, we can see that the average throughput is 5.98Mbps for both the sender and the receiver.

Be sure you review the documentation for iPerf at <https://iperf.fr/iperf-doc.php> and practice different command-line options, including the following:

- **-s** sets the device to run in server mode.
- **-t** changes the amount of time in seconds to something other than the default 10 seconds.
- **-w** can be used to set the TCP window size.
- **-4** or **-6** indicate to only use IPv4 or IPv6, respectively.

Example 28-2 shows all the available options for iPerf on Windows.

Example 28-2 Windows iPerf Options

```

C:\tools\iperf-3.1.3-win32> iperf3 -h
Usage: iperf [-s|-c host] [options]
        iperf [-h|--help] [-v|--version]

Server or Client:
  -p, --port #          server port to listen on/connect to
  -f, --format [kmgKMG] format to report: Kbits, Mbits, KBytes, MBytes
  -i, --interval #      seconds between periodic bandwidth reports
  -F, --file name       xmit/recv the specified file
  -B, --bind <host>    bind to a specific interface
  -V, --verbose         more detailed output
  -J, --json            output in JSON format
  --logfile f          send output to a log file
  -d, --debug          emit debugging output
  -v, --version        show version information and quit
  -h, --help          show this message and quit

Server specific:
  -s, --server         run in server mode
  -D, --daemon        run the server as a daemon
  -I, --pidfile file   write PID file
  -l, --one-off       handle one client connection then exit

Client specific:
  -c, --client <host> run in client mode, connecting to <host>
  -u, --udp           use UDP rather than TCP
  -b, --bandwidth # [KMG] [/#] target bandwidth in bits/sec (0 for unlimited)
                          (default 1 Mbit/sec for UDP, unlimited for TCP)
                          (optional slash and packet count for burst mode)
  -t, --time #       time in seconds to transmit for (default 10 secs)
  -n, --bytes # [KMG] number of bytes to transmit (instead of -t)
  -k, --blockcount # [KMG] number of blocks (packets) to transmit
(instead of -t or -n)
  -l, --len # [KMG]  length of buffer to read or write
                          (default 128 KB for TCP, 8 KB for UDP)
  --cport <port>     bind to a specific client port (TCP and UDP,
default: ephemeral port)
  -P, --parallel #   number of parallel client streams to run
  -R, --reverse      run in reverse mode (server sends, client receives)
  -w, --window # [KMG] set window size / socket buffer size
  -M, --set-mss #    set TCP/SCTP maximum segment size (MTU - 40 bytes)
  -N, --no-delay     set TCP/SCTP no delay, disabling Nagle's Algorithm
  -4, --version4     only use IPv4
  -6, --version6     only use IPv6

```

```

-S, --tos N           set the IP 'type of service'
-Z, --zerocopy       use a 'zero copy' method of sending data
-O, --omit N         omit the first n seconds
-T, --title str      prefix every output line with this string
--get-server-output  get results from server
--udp-counters-64bit use 64-bit counters in UDP test packets

```

[KMG] indicates options that support a K/M/G suffix for kilo-, mega-, or giga-

iPerf3 homepage at: <http://software.es.net/iperf/>

Report bugs to: <https://github.com/esnet/iperf>

```
C:\tools\iperf-3.1.3-win32>
```

If you want to test the performance in your own network, download iPerf on the computer that will receive the iPerf packets. Use the **-s** option to start an iPerf server, as shown in Example 28-3.

Example 28-3 iPerf Running in Server Mode

```
C:\tools\iperf-3.1.3-win32> iperf3 -s
```

```
-----
Server listening on 5201
-----
```

NOTE You will most likely need to configure a rule on your local firewalls to allow iPerf traffic.

Study Resources

For today's exam topics, refer to the following resources for more study:

Resource	Module or Chapter
SFA Self Enroll: Networking Basics	1
SFA Self Enroll: Network Support and Security	1
SFA Instructor Led: Networking Essentials	1, 37
CCST Networking 100-150 Official Cert Guide	9

NOTE SFA: <https://skillsforall.com/>

This page intentionally left blank

Symbols

? command, 215

Numbers

3–1–4 (pi) rule, 80

5G cellular networks, 109–110

802.11 standards, 107–108

A

AAA (Authentication, Authorization,

Accounting), 250

accounting, 250

authentication, 250

authorization, 250

access

ACL, 250

attacks, 240

controlling, 248

administrative access control, 249–250

logical access control, 249

physical access control, 249, 252

home routers, 267–268

HTTPS connectivity/access, Linux,
131–132

improper access control as a data loss
vector, 236

network connectivity

access layer switches, 144

Android, 135–137

cable management, 149–150

core layer switches, 145

distribution layer switches, 145

iOS, 134–136

*LAN device connectivity guidelines,
145–146*

Linux, 129–132

logical topologies, 24–25, 147, 148–149

macOS, 132–134

mobile devices, 134–137

networking icons, 143–144

physical topologies, 24–25, 146, 147–148

switches, overview, 143

Windows 11, 121–128

remote access

RDP, 205

SSH, 206

Telnet, 207

TCP Wrappers, 233

wireless security

attacks (overview), 253

basic setups, 262–266

DoS attacks, 253–254

encryption, 257

home router configurations, 258

home user authentication, 256–257

MAC address filtering, 255–256

MITM attacks, 254–255

passphrases, 266

rogue AP, 254

shared key authentication, 256

SSID cloaking, 255

verifying connectivity/access, 266

WEP, 256

wireless router logins, 258–259

WPA, 256, 257

WPA2, 256–257

WPA3, 256

access layer switches, 144

accounting, 250

ACL (Access Control Lists), 250

AD (Active Directory), 251

administration, 251

authentication, 251

authorization, 251

components of, 251

directory services, 251

domains, 251

forests, 251

functions, 251

OU, 251

trees, 251

**AD (Administrative Distance),
161–163**

address classes, IPv4 addressing, 70–71

**address resolution, solicited-node
multicast addresses, 86**

address spoofing attacks, 242

addressing schemes, subnetting, 74

administration

access control, 249–250

AD, 251

adware, 238

AES (Advanced Encryption Standard), 257

algorithms, hashing, 248

All People Seem To Need Data Processing memorization technique, OSI model, 3

amplification/reflection attacks, 242

ANDing, IPv4 addressing, 71

Android OS, 117, 134–137

anycast addresses, 87

AP (Access Points)

- rogue AP, 254
- SSID cloaking, 255

application gateway (proxy) firewalls, 229–230

application layer

- OSI model, 2
- TCP/IP model, 3, 5

ARP (Address Resolution Protocol)

- arp -a command, 125–126
- caches, viewing in Windows 11, 125–126
- show arp command, 219, 222
- tables, viewing, 197

assets, security, 235

assigned multicast addresses, 85–86

asymmetric switching, 172

attacks

- access attacks, 240
- amplification/reflection attacks, 242
- baiting, 241
- buffer overflow attacks, 240
- compromised key attacks, 238
- data modification attacks, 237
- DDoS attacks, 241
- DoS attacks, 238, 241, 253–254
- dumpster diving, 241
- eavesdropping attacks, 237
- ICMP attacks, 242
- impersonation, 241
- IP attacks, 241–242
- MITM attacks, 238, 240, 242, 254–255
- overview, 253
- password attacks, 238, 240
- phishing, 240
- port redirection attacks, 240
- pretexting, 240
- reconnaissance attacks, 239
- rogue AP, 254
- session hijacking, 242

shoulder surfing, 241

sniffer attacks, 238

social engineering attacks, 240–241
“something for something” (quid pro quo), 241

spam, 241

spear phishing, 240

spoofing attacks, 237, 240, 242

tailgating, 241

TCP

reset attacks, 242

session hijacking, 242

TCP SYN flood attacks, 242

transport layer attacks, 242–243

trust exploitation attacks, 240

UDP flood attacks, 243

audit trails, 248

authentication, 250

AD, 251

home users, 256–257

MFA, 250

shared key authentication, 256

WEP, 256

WPA, 256, 257

WPA2, 256–257

WPA3, 256

authorization, 250, 251

auto-completing commands, 216

automating VPN connections, 207–208

auxiliary ports, Cisco 4461 ISR, 152

availability, CIA Triad, 245, 249

awareness, security, 251

B

badges (certification), receiving, 271

baiting, 241

bandwidth, 13, 14

basic network setups, 259–262

billing systems, security, 250

binary values, subnetting

octet binary values, 73

subnet masks, 72

biometric security, 250

bits borrowed, subnetting, 72–73

black hole VLAN, 174

borrowing bits, subnetting, 72–73

bottom-up troubleshooting method, 178

broadcast domains, 171

buffer overflow attacks, 240

Building Your I.T. Career: A Complete Toolkit for a Dynamic Career in Any Economy, Second Edition (Pearson IT Certification, 2013), 271–272

C

cable management, 91, 149–150

- advantages of, 92
- coaxial cable, 95–96
- copper cable, 92, 93, 104
- disadvantages of, 92
- fiber patch cords, 101–103
- fiber-optic cable, 91, 92, 98
 - connectors, 100–101*
 - copper cable versus, 104*
 - MMF cable, 99*
 - SMF cable, 98–99*
- LAN cabling standards, 92–93
- STP cable, 95
- UTP cable, 94–95
 - categories, 96–97*
 - connectors, 97*
 - crossover UTP cable, 97–98*
 - straight-through UTP cable, 97–98*

CACT (Certipoint Authorized Testing Centers), 269

**calendars, CCST networking
countdown, 273–274**

CAN (Campus Area Networks), 26

capturing packets with Wireshark, 186
opening captures, 189
saving captures, 187–189

career options, determining, 271–272

CCST networking

- countdown calendars, 273–274
- exams
 - after completion, 270*
 - career options, 271–272*
 - certificates/badges, 271*
 - certification options, 272*
 - checklists, 275–277*
 - failing, 272*
 - in-person exams, 269*
 - remote exams, 269–270*
 - requirements, 269*
 - scoring, 270*
- post-exam information, 271–272

CDP (Cisco Discovery Protocol), 218

cellular networks, 109–110

certificates, digital, 248

certification

- post-exam options, 272
- receiving certificates/badges, 271

Certipoint

- in-person CCST exams, 269
- remote exams, 269–270

channels, 105–106

CIA Triad, 247

- availability, 245, 249
- confidentiality, 245, 248
- defined, 245–246
- integrity, 245, 248

Cisco 4461 ISR, ports, 151

- auxiliary ports, 152
- console ports, 152
- fixed ports, 151–153
- Gigabit Ethernet 0/0/0 and 0/0/1 ports, 152
- Gigabit Ethernet 0/0/2 and 0/0/3 ports, 152
- management network ports, 152
- NIM, 152
- SM-X slots, 153–154
- Ten Gigabit Ethernet 0/0/4 and 0/0/5 ports, 152
- USB ports, 152

Cisco Certified Support Technician CCST Networking 100–150 Official Cert Guide (Cisco Press, 2023), 272

Cisco IOS

- firewall configuration example, 230–231
- help facility, 216
 - ? command, 215*
 - command syntax help, 215*
 - console error messages, 215–216*
 - Word help, 215*

classful routing protocols, 160

classless routing protocols, 160

CLI (Command-Line Interfaces), 211

cloaking, SSID, 255

cloud computing, 31, 32

- advantages of, 32
- community clouds, 34
- disadvantages of, 32
- hybrid clouds, 33
- Meraki cloud management, 212–213

- models of, 33–34
- private clouds, 33
- public clouds, 33
- server virtualization, 34–35
- services
 - IaaS, 33
 - NIST service characteristics, 33
 - PaaS (Platform as a Service), 33
 - SaaS, 33
- storage as a data loss vector, 236
- workflows, 33

coaxial cable, 95–96**collision domains, 171****command line (Windows 11), 124–127****commands**

- ? command, 215
- arp -a command, 125–126
- auto-completing commands, 216
- Cisco IOS help facility, 216
 - ? command, 215
 - command syntax help, 215
 - console error messages, 215–216
 - Word help, 215
- curl command, 132
- FTP commands, 43–45
- getmac /v command, 124
- Get-NetRoute command, 126–127
- ifconfig command, 194–195
 - Linux, 129–130
 - macOS, 132–133
- ip addr add command, 196–197
- ip addr command, 195–196
- ip address command, 130
- ip command, 195
- ipconfig command, 124–125, 191–194
- ip route command, 197
- ipv6 unicast-routing global configuration command, 85–86
- nc command/Ncat, 131–132
- netstat command, 203
- netstat -rn command, 132
- networksetup -getinfo <network service> command, 133–134
- networksetup -listallnetworkservices command, 133–134
- nslookup command, 203
- ping command, 49, 197–200
 - reconnaissance attacks, 239
 - verifying Linux connectivity, 130–131
 - verifying Windows 11 connectivity, 127

privileges

- levels of, 216–217
- syntax, 217

- route print command, 127

- SFTP commands, 45

show commands

- defined, 219
- show arp command, 219, 222
- show interface status command, 219, 224
- show interfaces command, 219
- show inventory command, 219, 225
- show ip interface brief command, 226
- show ip interface command, 219, 221–222
- show ip route command, 131, 160–161, 219, 222
- show mac address-table command, 219, 225
- show protocols command, 219, 223
- show running-config command, 219–220
- show version command, 219, 223–224

- speedtest command, 131

- traceroute command, 49–50

- tracert command, 128, 201–203

community clouds, 34**community protocols, security, 248****comparison troubleshooting method, 179****compromised key attacks, 238****confidentiality, CIA Triad, 245, 248****configuring**

- Cisco IOS firewalls, example, 230–231
- home networks, 267–268
- home routers, 258
- IP configuration information, viewing in
 - Windows 11, 124–125
- networks
 - basic setups, 259–262
 - wireless setups, 262–266
- NTP, 47–48
- VPN for Windows devices, 207–208

connectionless protocols, 37–38, 41**connection-oriented protocols, 37–38****connectivity**

- cable management, 149–150
- coaxial cable, 95–96
- copper cable, 91, 92, 93, 104
- crosstalk, 93
- EMI, 93
- fiber patch cords, 101–103
- fiber-optic cable, 91, 92, 98

connectors, 100–101
 copper cable versus, 104
 MMF cable, 99
 SMF cable, 98–99

interference, 93, 108–109

iOS
 activating connectivity/access, 134–135
 verifying connectivity/access, 135–136

LAN device connectivity guidelines, 145–146

Linux
 finding public IP addresses, 132
 HTTPS connectivity/access, 131–132
 verifying connectivity/access, 130–132
 verifying IP configuration information, 129–130

macOS, verifying configuration information, 132–134

mobile devices
 activating connectivity/access, 134–135
 verifying connectivity/access, 135–137

networking icons, 143–144

RFI, 93

STP cable, 95

switches
 access layer switches, 144
 core layer switches, 145
 distribution layer switches, 145
 overview, 143

TCP connection establishment/
 termination, 40–41

topologies
 logical topologies, 24–25, 147, 148–149
 physical topologies, 24–25, 146, 147–148

UTP cable, 94–95
 categories, 96–97
 connectors, 97
 crossover UTP cable, 97–98
 straight-through UTP cable, 97–98

Windows 11
 command line, 124–127
 Control Panel, 122–124
 PowerShell, 124–127
 Settings app, 121–122
 verifying connectivity/access, 127–128
 viewing ARP caches, 125–126
 viewing host routing tables, 126–127
 viewing IP configuration information, 124–125

wireless connectivity, 91, 92

wireless security, verifying, 266

console error messages, 215–216

console ports, 152, 209–210

Control Panel (Windows 11), 122–124

controlling access, 248
 administrative access control, 249–250
 logical access control, 249
 physical access control, 249, 252

convergence, link-state routing protocols, 166–167

copper cable, 91, 92, 93, 104

core layer switches, 145

countdown calendars, CCST networking, 273–274

crackers, password, 237

CRC (Cyclic Redundancy Checks), 171–172

crossover UTP cable, 97–98

crosstalk, 93

curl command, 132

cut-through switching, 172

cybersecurity (McCumber) cube, 245
 CIA Triad, 247
 availability, 245, 249
 confidentiality, 245, 248
 defined, 245–246
 integrity, 245, 248
 data states, 246
 principles of, 245–246
 safeguards, 246–247

D

DAD (Duplicate Address Detection), 86

data encapsulation
 PDU, 9–10
 summary, 9–10
 tunnels, 10–11

data encryption, 257

data exfiltration, 236

data link layer, OSI model, 2

data loss vectors, security, 236

data modification attacks, 237

data processing, 246

data states, cybersecurity (McCumber) cube, 246

data storage, 246

data transmission, 246

data VLAN, 174

databases, link-state, 164–165

DDoS attacks, 241

debuggers, 237

decimal values, subnetting, 73

default VLAN, 174

delays, network performance, 15

jitter, 15–16

physical path lengths, 15

queueing delays, 15

serialization delays, 15

DELETE messages, 56

desktops, RDP, 205

Destination Unreachable messages, 48

device management

console ports, 209–210

Meraki cloud management, 212–213

NMS

CLI, 211

defined, 210

functions, 210–211

NetFlow, 211

REST API, 211

SNMP, 211

Syslog, 211

RDP, 205

SSH, 206

Telnet, 207

terminal emulators, 208–209

VPN, 207

device ports, Cisco 4461 ISR, 151

auxiliary ports, 152

console ports, 152

fixed ports, 151–153

Gigabit Ethernet 0/0/0 and 0/0/1
ports, 152

Gigabit Ethernet 0/0/2 and 0/0/3
ports, 152

management network ports, 152

NIM, 152

SM-X slots, 153–154

Ten Gigabit Ethernet 0/0/4 and 0/0/5
ports, 152

USB ports, 152

device status lights, 139–140

DHCPv4 (Dynamic Host Configuration Protocol version 4), 57–58

DHCPv6 (Dynamic Host Configuration Protocol version 6), 58

SLAAC, 58–59

neighbor discovery, 59–60

NS messages, 59–60

operation of, 60–61

RA messages, 59

RS messages, 58–59

stateful operations, 58–61

diagnostic commands, 191

ifconfig command, 194–195

ip addr add command, 196–197

ip addr command, 195–196

ip command, 195

ip route command, 197

ipconfig command, 191–194

netstat command, 203

nslookup command, 203

ping command, 49, 197–200

tracert command, 128, 201–203

digital certificates, 248

Dijkstra algorithm, 165–166

directly connected routing, 157

directory services, 251

discovery protocols

CDP, 218

LLDP, 218

distance vector protocols, 159

distribution layer switches, 145

divide-and-conquer troubleshooting method, 178

DNS (Domain Name System)

operation of, 61–62

process of, 61–62

resource records, 61–62

URI, 61

domains, AD, 251

DoS attacks, 238, 241, 253

dual-stacking, IPv6 addressing, 89–90

dumpster diving, 241

dynamic NAT, 66–67

dynamic routing, 157–158

classful routing protocols, 160

classless routing protocols, 160

distance vector protocols, 159

EGP, 157–158

EIGRP, 163

IGP, 159, 163

- link-state routing protocols, 159–160
 - building databases, 164–165*
 - convergence, 166–167*
 - Dijkstra algorithm, 165–166*
 - features of, 164*
 - LSA, 164–165, 166–167*
 - SPF algorithm, 165–166*
- metrics, 160–161
- OSPF, 163
- R2 routing tables, 161
- RIPv2, 163
- show ip route command, 160–161, 219, 222

E

- eavesdropping attacks, 237**
- Echo messages, 48**
- educated guess troubleshooting method, 179**
- EGP (Exterior Gateway Protocols), 159**
- EIGRP (Enhanced Interior Gateway Routing Protocol), 163**
- email as a data loss vector, 236**
- EMI (Electromagnetic Interference), 93**
- encapsulating data**
 - PDU, 9–10
 - summary, 9–10
 - tunnels, 10–11
- encryption, 248**
 - data, 257
 - tools, 237
- endpoints**
 - hosts
 - defined, 114*
 - virtual hosts, 114–116*
 - IoT, 117–119
 - mobile devices, 117
 - development of, 116*
 - smartphones, 116*
 - tablets/phablets, 117*
 - packets, sending, 114
 - virtual hosts, 114–116
- end-to-end bandwidth, 14**
- error messages, console, 215–216**
- error recovery (reliability), TCP, 39–40**
- escalation/prioritization, help desks, 180–181**
- establishing TCP connections, 40–41**

Ethernet

- crossover UTP cable, 97–98
- Gigabit Ethernet 0/0/0 and 0/0/1 ports, 152
- Gigabit Ethernet 0/0/2 and 0/0/3 ports, 152
- switches, 170
- Ten Gigabit Ethernet 0/0/4 and 0/0/5 ports, 152

exams

- after completion, 270
- certification, receiving certificates/badges, 271
- checklists
 - Days 9–1, 277*
 - Days 17–10, 276*
 - Days 24–18, 275–276*
 - Days 31–25, 275*
- failing, 272
- in-person exams, 269
- post-exam information
 - career options, 271–272*
 - certificates/badges, 271*
 - certification options, 272*
- remote exams, 269–270
- requirements, 269
- scoring, 270

exfiltrating data, 236

exploits, security, 235, 237

F

- failing exams, 272**
- failover mechanisms, 249**
- FF02:0:0:0:FF00::/104 multicast prefix, 86**
- FF02::1 All-nodes multicast group, 85**
- FF02::2 All-routers multicast group, 85–86**
- fiber patch cords, 101–103**
- fiber-optic cable, 91, 92, 98**
 - connectors, 100–101
 - copper cable versus, 104
 - MMF cable, 99
 - SMF cable, 98–99
- file permissions, Linux, 250**
- filtering MAC addresses, 255–256**
- finding public IP addresses, Linux, 132**

firewalls, 227

- application gateway (proxy) firewalls, 229–230
- Cisco IOS firewall example, 230–231
- host-based firewalls, 231–233
- iptables, 232
- nftables, 232
- NGFW, 229–230
- stateful firewalls, 229
- stateless firewalls, 227–228
- TCP Wrappers, 233
- Windows Defender Firewall, 231–232

fixed ports, Cisco 4461 ISR, 151–153**flood attacks**

- TCP SYN, 242
- UDP, 243

flow control, TCP, 40**follow-the-path troubleshooting method, 178****forensic tools, security, 237****forests, AD, 251****forwarding**

- frame forwarding, 171
- packets, 155
 - path determination, 156*
 - switching, 156*
- switch forwarding, 170

fragment-free switching, 172**frame forwarding, 171****frequency channels, 105–106****FTP (File Transfer Protocol), 43, 45**

- commands, 43–45
- SFTP, 43, 45
- TFTP, 43, 46

full mesh topologies, 23–24**G****GET messages, 55****getmac /v command, 124****Get-NetRoute command, 126–127****Gigabit Ethernet 0/0/0 and 0/0/1 ports, 152****Gigabit Ethernet 0/0/2 and 0/0/3 ports, 152****global unicast addresses, 80–82****goodput, 14****Graziani's 3–1–4 (pi) rule, 80****H****hacking tools**

- network scanning/hacking, 237
- OS hacks, 237
- wireless hacking, 237

hard copies as data loss vectors, 236**hashing algorithms, 248****HEAD messages, 56****headers**

- IPv4 addressing, 69
- IPv6 addressing, 78–79
- TCP, 38, 41
- UDP, 41

help desks, 180

- policies/procedures, 180
- prioritization/escalation, 180–181
- ticketing systems, 181–182
- trouble tickets
 - fields, 182*
 - ticketing process, 181*

help facility, Cisco IOS, 216

- ? command, 215
- command syntax help, 215
- console error messages, 215–216
- Word help, 215

hierarchical campus design, 27–29**hijacking sessions, 242****hold-down timers, 164****home networks, configuring, 267–268****home routers**

- access, 267–268
- configuring, 258

home users, authentication, 256–257**host reachability messages, 48****host routing tables, viewing in Windows 11, 126–127****host-based firewalls, 231–233****hosts**

- defined, 113–114
- virtual hosts, 114–116

HTTP (HyperText Transfer Protocol), 55

- DELETE messages, 56
- GET messages, 55
- HEAD messages, 56
- operation of, 56–57
- POST messages, 55
- PUT messages, 56

HTTPS, Linux connectivity/access,
131–132

hub-and-spoke topologies, 23

hybrid clouds, 33

hybrid topologies, 24

I

IaaS (Infrastructure as a Service), 33

ICMP attacks, 242

ICMPv4 (Internet Control Message Protocol version 4), 48

Destination Unreachable messages, 48

Echo messages, 48

host reachability messages, 48

ping command, 49

Service Unreachable messages, 48

Time Exceeded messages, 49

traceroute command, 49–50

ICMPv6 (Internet Control Message Protocol version 6), 48

Destination Unreachable messages, 48

Echo messages, 48

host reachability messages, 48

messaging (overview), 51

NA messages, 52–53

NS messages, 52

ping command, 49

RA messages, 51

RS messages, 51–52

Service Unreachable messages, 48

Time Exceeded messages, 49

traceroute command, 49–50

icons, networking, 143–144

identity stores, 251

IEEE 802.11 standards, 107–108

ifconfig command, 194–195

Linux, 129–130

macOS, 132–133

IGP (Interior Gateway Protocols),
159, 163

impersonation, 241

in-person exams, 269

inside global addresses, 65

inside local addresses, 65

integrity, CIA Triad, 245, 248

interfaces

show interface status command, 219, 224

show ip interface brief command, 226

show ip interface command, 219,

221–222

interference, 93, 108–109

Internet connections

SOHO, 26–27

speed tests, 16–17

Internet layer, TCP/IP, 3, 6–7

inventories, show inventory command,
219, 225

iOS, 117, 134–136

IoT (Internet of Things), 117–119

IP (Internet Protocol)

attacks, 241–242

multicast traffic, 174

show ip interface brief command, 226

show ip interface command, 219,

221–222

show ip route command, 219, 222

telephony traffic, 173

ip addr add command, 196–197

ip addr command, 195–196

ip address command, 130

**IP addressing. See also specific IPv4
addressing and IPv6 addressing
entries below**

configuration information

verifying in Linux, 129–130

verifying in macOS, 132–134

viewing in Windows 11, 124–125

Linux devices

ping command, 198–199, 200

viewing settings, 194–195

macOS devices

ping command, 198–199, 200

viewing settings, 194–195

NAT, 64

benefits of, 68

dynamic NAT, 66–67

example of, 66

inside global addresses, 65

inside local addresses, 65

limitations of, 68

outside global addresses, 65

outside local addresses, 65

overloading, 67

PAT, 67

static NAT, 67

terminology, 65–66

topologies, 63–64

- netstat command, 203
- private addressing, 63
- public IP addresses, finding with
 - Linux, 132
- reserved addresses, 63–64
- spoofing attacks, 237
- TTL fields, IP headers, 164
- verifying new addresses were added to
 - interfaces, 196–197
- Windows devices
 - ping* command, 197–198, 199
 - releasing settings, 193–194
 - renewing settings, 193–194
 - tracert* command, 202–203
 - viewing settings, 191–192

ip command, 195**ip route command, 197****ipconfig command, 124–125, 191–194****iPerf tool, 17–20****iptables, 232****IPv4 addressing, 69**

- address classes, 70–71
- ANDing, 71
- dual-stacking, 89–90
- embedded addresses in IPv6, 84–85
- headers, 69
- IPv6 addressing
 - comparisons*, 78
 - migrating to*, 89–90
- subnetting
 - addressing schemes*, 74
 - borrowing bits*, 72–73
 - examples*, 74–76
 - methodology*, 72–74
 - multipliers, determining*, 74
 - octet binary values*, 73
 - octet decimal values*, 73
 - subnet masks*, 70–71
 - subnet masks, ANDing*, 71
 - subnet masks, binary values*, 72
 - subnet masks, determining new*, 73–74
- tunneling, 89

IPv6 addressing

- anycast addresses, 87
- benefits of, 77–78
- dual-stacking, 89–90
- headers, 78–79
- IPv4 addressing
 - comparisons*, 78
 - migrating from*, 89–90

- migrating to*, 89–90
- multicast addresses, 85
 - assigned multicast addresses*, 85–86
 - FF02:0:0:0:0:FF00::/104 multicast prefix*, 87
 - FF02::1 All-nodes multicast group*, 85
 - FF02::2 All-routers multicast group*, 85–86
 - ipv6 unicast-routing global configuration command*, 85–86
 - least significant 24 bits*, 87
 - solicited-node multicast addresses*, 86–87
- overview, 77–78
- prefixes, 88–89
- tunneling, 89
- unicast addresses, 80
 - 3–1-4 (pi) rule*, 80
 - global unicast addresses*, 80–82
 - IPv4 embedded addresses*, 84–85
 - link-local addresses*, 82–83
 - loopback addresses*, 83
 - ULA*, 84
 - unspecified addresses*, 83
- writing conventions
 - addresses*, 88
 - prefixes*, 88–89

ipv6 unicast-routing global configuration command, 85–86

J**jitter, 15–16****K****key attacks, compromised, 238****L****LAN (Local Area Networks)**

- cabling standards, 92–93
- components of, 21
- device connectivity guidelines, 145–146
- switching
 - broadcast domains*, 171
 - collision domains*, 171
 - Ethernet switches*, 170
 - evolution to*, 169–170
 - forwarding*, 170
 - Layer 2 switching*, 172
 - Layer 3 switching*, 172

logic, 170–171

MAC addresses, 170–171

topologies, 21–22, 24–26

VLAN

benefits of, 173

black hole VLAN, 174

data VLAN, 174

default VLAN, 174

IP multicast traffic, 174

IP telephony traffic, 173

management traffic, 173

management VLAN, 174

native VLAN, 174

normal data traffic, 174

reasons for using, 172–173

scavenger class traffic, 174

traffic, types of, 173–174

types of, 174

voice VLAN, 174–175

WLAN, 26

Layer 2 switching, 172

Layer 3 switching, 172

least significant 24 bits, multicast addresses, 87

lights, device status, 139–140

link-local addresses, 82–83

link-state routing protocols, 159–160

building databases, 164–165

convergence, 166–167

Dijkstra algorithm, 165–166

features of, 164

LSA, 164–165, 166–167

SPF algorithm, 165–166

Linux

connectivity/access, verifying, 130–132

curl command, 132

file permissions, Linux, 250

firewalls, 232

HTTPS connectivity/access, 131–132

ifconfig command, 129–130

ip address command, 130

ip command options, 195

IP configuration information, verifying, 129–130

IP settings, viewing, 194–195

iptables, 232

nc command/Ncat, 131–132

netstat -rn command, 132

nftables, 232

ping command, 130–131, 198–199, 200

public IP addresses, finding, 132

routing tables, viewing, 132

speedtest command, 131

LLDP (Link Layer Discovery Protocol), 218

log files, accounting, 250

logical access control, 249

logical topologies, 24–25, 147, 148–149

logins

SSH, 206

wireless routers, 258–259

logs, network device, 250

loop prevention, routing, 163–164

loopback addresses, 83

LSA (Link-State Advertisements), 164–165, 166–167

M

MAC addresses

filtering, 255–256

show mac address-table command, 219, 225

switches, 170–171

macOS

configuration information, verifying, 132–134

connectivity/access, 132–134

ifconfig command, 132–133

ip command options, 195

IP settings, viewing, 194–195

networksetup -getinfo <network service> command, 133–134

networksetup -listallnetworkservices command, 133–134

ping command, 198–199, 200

maintenance, security, 249

malware

adware, 238

ransomware, 239

rootkits, 239

spyware, 239

Trojan horses, 238

viruses, 238

worms, 238

MAN (Metropolitan Area Networks), 26

management network ports, Cisco 4461 ISR, 152

management VLAN, 174**managing**

- cabling, 91, 149–150
 - advantages of, 92*
 - coaxial cable, 95–96*
 - copper cable, 92, 93, 104*
 - disadvantages of, 92*
 - fiber patch cords, 101–103*
 - fiber-optic cable, 91, 92, 98*
 - fiber-optic cable, connectors, 100–101*
 - fiber-optic cable, MMF, 99*
 - fiber-optic cable, SMF, 98–99*
 - fiber-optic cable versus copper cable, 104*
- LAN cabling standards, 92–93*
- STP cable, 95*
- UTP cable, 94–95*
- UTP cable, categories, 96–97*
- UTP cable, connectors, 97*
- UTP cable, crossover, 97–98*
- UTP cable, straight-through, 97–98*

cloud computing, 212–213

devices

- console ports, 209–210*
- Meraki cloud management, 212–213*
- NMS, 210–211*
- RDP, 205*
- SSH, 206*
- Telnet, 207*
- terminal emulators, 208–209*
- VPN, 207–208*

man-in-the-middle attacks. See MITM attacks**McCumber (cybersecurity) cube, 245**

- CIA Triad, 247
 - availability, 245, 249*
 - confidentiality, 245, 248*
 - defined, 245–246*
 - integrity, 245, 248*
- data states, 246
- principles of, 245–246
- safeguards, 246–247

memory

- buffering, switches, 172
- port-based memory, 172
- shared memory, 172

Meraki cloud management, 212–213**MFA (Multifactor Authentication), 250****mitigation, defined, 236****MITM attacks, 238, 240, 242, 254–255****MMF cable, 99****mobile cores, 111****mobile devices**

- connectivity/access, activating, 134–135
- development of, 116
- OS, 117
- RAN, 111
- smartphones, 116
- tablets/phablets, 117
- verifying connectivity/access, 135–137

modification attacks, data, 237**monitoring networks, Wireshark**

- downloading, 186
- features of, 185
- installing, 186
- overview, 185
- packet capturing, 186
 - opening captures, 189*
 - saving captures, 187–189*
- users, 186

Moran, Matthew, 271–272**multicast addresses, 85**

- assigned multicast addresses, 85–86
- FF02:0:0:0:FF00::/104 multicast prefix, 87
- FF02::1 All-nodes multicast group, 85
- FF02::2 All-routers multicast group, 85–86
- ipv6 unicast-routing global configuration command, 85–86
- least significant 24 bits, 87
- solicited-node multicast addresses, 86–87

multicast traffic, IP, 174**multipliers, subnetting, 74****N****NA messages, 52–53****NAT (Network Address Translation), 64**

- benefits of, 68
- dynamic NAT, 66–67
- example of, 66
- inside global addresses, 65
- inside local addresses, 65
- limitations of, 68
- outside global addresses, 65
- outside local addresses, 65
- overloading, 67
- PAT, 67
- static NAT, 67

- terminology, 65–66
- topologies, 63–64
- native VLAN, 174**
- nc command/Ncat, 131–132**
- neighbor discovery**
 - NDP, 86–87
 - SLAAC, 59–60
- NetFlow, 211**
- netstat command, 203**
- netstat -rn command, 132**
- network access layer, TCP/IP, 7–8**
- network device logs, 250**
- network layer, OSI model, 2**
- network media/connectivity, 91**
 - advantages of, 92
 - coaxial cable, 95–96
 - copper cable, 92, 93
 - fiber-optic cable versus, 104*
 - crosstalk, 93
 - disadvantages of, 92
 - EMI, 93
 - fiber patch cords, 101–103
 - fiber-optic cable, 91, 92, 98
 - connectors, 100–101*
 - copper cable versus, 104*
 - MMF cable, 99*
 - SMF cable, 98–99*
 - interference, 93, 108–109
 - LAN cabling standards, 92–93
 - RFI, 93
 - STP cable, 95
 - UTP cable, 94–95
 - categories, 96–97*
 - connectors, 97*
 - crossover UTP cable, 97–98*
 - straight-through UTP cable, 97–98*
 - wireless connectivity, 91, 92
- networking models**
 - OSI model, 1–3
 - All People Seem To Need Data Processing memorization technique, 3*
 - application layer, 2*
 - data link layer, 2*
 - network layer, 2*
 - physical layer, 2*
 - presentation layer, 2*
 - session layer, 2*
 - transportation layer, 2*
 - TCP/IP model, 1, 7
 - application layer, 3, 5*
 - Internet layer, 3, 6–7*
 - network access layer, 7–8*
 - PDU, 9–10*
 - protocols, 8*
 - transport layer, 3, 5–6*
- networks**
 - 5G cellular networks, 109–110
 - attacks
 - access attacks, 240*
 - reconnaissance attacks, 239*
 - basic setups, 259–262
 - CAN, 26
 - cellular networks, 109–110
 - configuring
 - basic setups, 259–262*
 - wireless setups, 262–266*
 - connectivity/access
 - access layer switches, 144*
 - cable management, 149–150*
 - core layer switches, 145*
 - distribution layer switches, 145*
 - Linux, 129–132*
 - logical topologies, 24–25, 147, 148–149*
 - macOS, 132–134*
 - mobile devices, 134–137*
 - networking icons, 143–144*
 - physical topologies, 24–25, 146, 147–148*
 - switches, overview, 143*
 - Windows 11, 121–128*
 - firewalls, 227
 - application gateway (proxy) firewalls, 229–230*
 - Cisco IOS firewall example, 230–231*
 - host-based firewalls, 231–233*
 - iptables, 232*
 - nftables, 232*
 - NGFW, 229–230*
 - stateful firewalls, 229*
 - stateless firewalls, 227–228*
 - TCP Wrappers, 233*
 - Windows Defender Firewall, 231–232*
 - hierarchical campus design, 27–29
 - home networks, configuring, 267–268
 - icons, 143–144
 - LAN
 - broadcast domains, 171*
 - cabling standards, 92–93*
 - collision domains, 171*
 - components of, 21*
 - device connectivity guidelines, 145–146*

- Layer 2 switching*, 172
 - Layer 3 switching*, 172
 - switching, Ethernet switches*, 170
 - switching, evolution to*, 169–170
 - switching, forwarding*, 170
 - switching, logic*, 170–171
 - switching, MAC addresses*, 170–171
 - topologies*, 21–22, 24–26
 - WLAN*, 26
- MAN, 26
- management traffic, VLAN, 173
- monitoring, Wireshark
 - downloading*, 186
 - features of*, 185
 - installing*, 186
 - overview*, 185
 - packet capturing*, 186–189
 - users*, 186
- PAN, 26
- performance
 - bandwidth*, 13, 14
 - delays*, 15–16
 - end-to-end bandwidth*, 14
 - goodput*, 14
 - iPerf tool*, 17–20
 - jitter*, 15–16
 - physical path lengths*, 15
 - queueing delays*, 15
 - serialization delays*, 15
 - speed tests*, 16–17
 - throughput*, 13–14
- RAN, 111
- scanning tools, 237
- SOHO
 - Internet connections*, 26–27
 - routers*, 27
- three-tiered campus design, 28
- topologies, 24–25
 - CAN, 26
 - full mesh topologies*, 23–24
 - hub-and-spoke topologies*, 23
 - hybrid topologies*, 24
 - LAN, 21–22, 24–26
 - logical topologies*, 24–25, 147, 148–149
 - MAN, 26
 - PAN, 26
 - physical topologies*, 24–25, 146, 147–148
 - point-to-point topologies*, 23
 - variations of*, 26
 - WAN, 23–26
 - WLAN, 26
- two-tiered campus design, 28–29
- VLAN
 - benefits of*, 173
 - black hole VLAN*, 174
 - data VLAN*, 174
 - default VLAN*, 174
 - IP multicast traffic*, 174
 - IP telephony traffic*, 173
 - management traffic*, 173
 - management VLAN*, 174
 - native VLAN*, 174
 - normal data traffic*, 174
 - reasons for using*, 172–173
 - scavenger class traffic*, 174
 - traffic, types of*, 173–174
 - types of*, 174
 - voice VLAN*, 174–175
- VPN, 207
 - automating connections*, 207–208
 - scripting connections*, 207–208
 - tunnels*, 10–11
 - Windows configurations*, 207–208
- WAN
 - connecting to*, 22–23
 - topologies*, 23–26
- Wi-Fi networks, 105, 109–110
- wireless security
 - attacks (overview)*, 253
 - basic setups*, 262–266
 - DoS attacks*, 253–254
 - encryption*, 257
 - home router configurations*, 258
 - home user authentication*, 256–257
 - MAC address filtering*, 255–256
 - MITM attacks*, 254–255
 - passphrases*, 266
 - rogue AP*, 254
 - shared key authentication*, 256
 - SSID cloaking*, 255
 - verifying connectivity/access*, 266
 - WEP, 256
 - wireless router logins*, 258–259
 - WPA, 256, 257
 - WPA2, 256–257
 - WPA3, 256
- Wireshark network monitoring
 - downloading*, 186
 - features of*, 185
 - installing*, 186
 - overview*, 185
 - packet capturing*, 186–189
 - users*, 186
- WLAN, 26

networksetup -getinfo <network service> command, 133–134

networksetup -listallnetworkservices command, 133–134

nftables, 232

NGFW (Next-Generation Firewalls), 229–230

NIM (Network Interface Modules), 152

NIST, cloud computing services, 33

NMS (Network Management Systems)

CLI, 211

defined, 210

functions, 210–211

NetFlow, 211

REST API, 211

SNMP, 211

Syslog, 211

normal data traffic, 174

NS messages, 52, 59–60

nslookup command, 203

NTP (Network Time Protocol)

configuring, 47–48

Stratums, 46–47

verifying, 47–48

O

octet binary values, subnetting, 73

octet decimal values, subnetting, 73

Ookla, speed tests, 16–17

on-premises computing

advantages of, 31

disadvantages of, 31–32

opening packet captures, 189

OS (Operating Systems)

Android OS, 117, 134–137

Cisco IOS

firewall configuration example, 230–231

help facility, 215–216

hacking tools, 237

iOS, 117, 134–136

Linux

connectivity/access, 129–132

curl command, 132

finding public IP addresses, 132

firewalls, 232

HTTPS connectivity/access, 131–132

ifconfig command, 129–130

ip address command, 130

ip command options, 195

nc command/Ncat, 131–132

netstat -rn command, 132

nftables, 232

ping command, 198–199, 200, 130–131

speedtest command, 131

verifying connectivity/access, 130–132

verifying IP configuration information, 129–130

viewing IP settings, 194–195

viewing routing tables, 132

macOS

connectivity/access, 132–134

ifconfig command, 132–133

ip command options, 195

networksetup -getinfo <network service> command, 133–134

networksetup -listallnetworkservices command, 133–134

ping command, 198–199, 200

verifying configuration information, 132–134

viewing IP settings, 194–195

mobile devices, 117

activating connectivity/access, 134–135

connectivity/access, 134–137

verifying connectivity/access, 135–137

Windows 11

arp -a command, 125–126

command line, 124–127

connectivity/access, 121–128

Control Panel, 122–124

firewalls, 231–232

getmac /v command, 124

Get-NetRoute command, 126–127

ipconfig command, 124–125

netstat command, 203

ping command, 197–198, 199, 127

PowerShell, 124–127

releasing IP settings, 193–194

renewing IP settings, 193–194

route print command, 127

Settings app, 121–122

tracert command, 128, 202–203

verifying connectivity/access, 127–128

viewing ARP caches, 125–126

viewing host routing tables, 126–127

viewing IP configuration information, 124–125

viewing IP settings, 191–192

Windows Defender Firewall, 231–232

OSI model, 1–3

- All People Seem To Need Data
 - Processing memorization technique, 3
- application layer, 2
- data link layer, 2
- network layer, 2
- physical layer, 2
- presentation layer, 2
- session layer, 2
- stateless firewalls, 227–228
- transportation layer, 2

OSPF (Open Shortest Path First), 163**OU (Organizational Units), 251****outside global addresses, 65****outside local addresses, 65****overloading NAT, 67****P****PaaS (Platform as a Service), 33****packets**

- capturing with Wireshark, 186
 - opening captures, 189
 - saving captures, 187–189
- crafting tools, 237
- delays
 - jitter*, 15–16
 - physical path lengths*, 15
 - queueing delays*, 15
 - serialization delays*, 15
- forwarding, 155
 - path determination*, 156
 - switching*, 156
- sending, 114
- sniffers, 237, 238

PAN (Personal Area Networks), 26**passphrases, wireless security, 266****passwords, 250**

- attacks, 238, 240
- crackers, 237

PAT (Port Address Translation), 67**path determination, packet**

- forwarding, 156

path lengths, network performance/delays, 15**PDU (Protocol Data Units), 9–10****penetration testing tools, 236–237****performance, networks**

- bandwidth, 13, 14

delays, 15–16

end-to-end bandwidth, 14

goodput, 14

iPerf tool, 17–20

jitter, 15–16

physical path lengths, 15

queueing delays, 15

serialization delays, 15

speed tests, 16–17

throughput, 13–14

permissions (Linux), file, 250**phablets/tablets, 117****phishing, 240****physical access control, 249, 252****physical layer, OSI model, 2****physical path lengths, network performance/delays, 15****physical topologies, 24–25, 146, 147–148****pi (3–1–4) rule, 80****ping command, 49, 197–200**

IP addressing

- Linux devices*, 198–199, 200

- macOS devices*, 198–199, 200

- Windows devices*, 197–198, 199

reconnaissance attacks, 239

verifying Linux connectivity, 130–131

verifying Windows 11 connectivity, 127

point-to-point topologies, 23**poisoning/poison reverse, route, 164****policies/procedures, help desks, 180****ports**

Cisco 4461 ISR, 151

- auxiliary ports*, 152

- console ports*, 152

- fixed ports*, 151–153

- Gigabit Ethernet 0/0/0 and 0/0/1 ports*, 152

- Gigabit Ethernet 0/0/2 and 0/0/3 ports*, 152

- management network ports*, 152

- NIM*, 152

- SM-X slots*, 153–154

- Ten Gigabit Ethernet 0/0/4 and 0/0/5 ports*, 152

- USB ports*, 152

console ports, 209–210

memory, 172

numbers, TCP/UDP, 38–39

redirection attacks, 240

POST messages, 55**post-exam information**

- career options, 271
- certificates/badges, 271
- certification options, 272
- failing exams, 272

PowerShell (Windows 11), 124–127**prefixes, IPv6 addressing, 88–89****presentation layer, OSI model, 2****pretexting, 240****prioritization/escalation, help desks, 180–181****privacy**

- private addressing, 63
- private clouds, 33
- WEP, 256

privileges

- command syntax, 217
- levels of, 216–217

processing data, 246**protocols**

- ARP. add ARP entries
- CDP, 218
- connectionless protocols, 37–38, 41
- connection-oriented protocols, 37–38
- DHCPv4, 57–58
- DHCPv6, 58
 - SLAAC, 58–61
 - stateful operations, 58–61
- discovery protocols, 218
- distance vector protocols, 159
- DNS
 - operation of, 61–62
 - process of, 61–62
 - resource records, 61–62
 - URI, 61
- EGP, 157–158
- EIGRP, 163
- FTP, 43, 45
 - commands, 43–45
 - SFTP, 43, 45
 - TFTP, 43, 46
- HTTP, 55
 - DELETE messages, 56
 - GET messages, 55
 - HEAD messages, 56
 - operation of, 56–57
 - POST messages, 55
 - PUT messages, 56
- ICMPv4, 48

Destination Unreachable messages, 48

Echo messages, 48

host reachability messages, 48

ping command, 49

Service Unreachable messages, 48

Time Exceeded messages, 49

traceroute command, 49–50

ICMPv6, 48

Destination Unreachable messages, 48

Echo messages, 48

host reachability messages, 48

messaging (overview), 51

NA messages, 52–53

NS messages, 52

ping command, 49

RA messages, 51

RS messages, 51–52

Service Unreachable messages, 48

Time Exceeded messages, 49

traceroute command, 49–50

IGP, 159, 163**link-state routing protocols, 159–160**

building databases, 164–165

convergence, 166–167

Dijkstra algorithm, 165–166

features of, 164

LSA, 164–165, 166–167

SPF algorithm, 165–166

LLDP, 218**NDP, 86–87****NTP**

configuring, 47–48

Stratums, 46–47

verifying, 47–48

OSPF, 163**RIPv2, 163****SFTP, 43, 45**

show protocols command, 219, 223

SNMP, 211**TCP, 37**

connection establishment/termination, 40–41

error recovery (reliability), 39–40

flow control, 40

headers, 38, 41

port numbers, 38–39

windowing, 40

TCP/IP model, 8**TFTP, 43, 46****UDP, 37**

headers, 41

port numbers, 38–39

proxy (application gateway) firewalls,
229–230

public clouds, 33

public IP addresses, finding with
Linux, 132

PUT messages, 56

Q

queueing delays, 15

quid pro quo (“something for
something”), 241

R

R2 routing tables, 161

RA messages, 51, 59

RAN (Radio Access Networks), 111

ransomware, 239

RBAC, 250

RDP (Remote Desktop Protocol), 205

reconnaissance attacks, 239

redirection attacks, ports, 240

redundancy, 171–172, 249

reflection/amplification attacks, 242

regular maintenance, security, 249

releasing IP settings in Windows
devices, 193–194

reliability (error recovery), TCP, 39–40

remote access

RDP, 205

SSH, 206

Telnet, 207

remote exams, 269–270

removable media as data loss vector, 236

renewing IP settings in Windows
devices, 193–194

reserved addresses, 63–64

reset attacks, TCP, 242

resource records, DNS, 61–62

REST API, 211

RF spectrum, 105–106

RFI (Radio Frequency Interference), 93

RIPv2 (Routing Information Protocol
version 2), 163

risks, security, 236

rogue AP, 254

rootkit detectors, 237

rootkits, 239

route print command, 127

routers/routing

AD, 161–163

Cisco 4461 ISR, ports, 151

auxiliary ports, 152

console ports, 152

fixed ports, 151–153

Gigabit Ethernet 0/0/0 and 0/0/1
ports, 152

Gigabit Ethernet 0/0/2 and 0/0/3
ports, 152

management network ports, 152

NIM, 152

SM-X slots, 153–154

Ten Gigabit Ethernet 0/0/4 and 0/0/5
ports, 152

USB ports, 152

directly connected routing, 157

dynamic routing, 157–158

classful routing protocols, 160

classless routing protocols, 160

distance vector protocols, 159

EGP, 157–158

EIGRP, 163

IGP, 159, 163

link-state routing protocols, 159–160,
164–167

metrics, 160–161

OSPF, 163

R2 routing tables, 161

RIPv2, 163

show ip route command, 219, 222,
160–161

home routers

access, 267–268

configuring, 258

loop prevention, 163–164

packet forwarding, 155

path determination, 156

switching, 156

poisoning/poison reverse, 164

RA messages, 59

routing tables

R2 routing tables, 161

triggered updates, 164

viewing, 197

viewing in Linux, 132

RS messages, 58–59

show ip interface brief command, 226
 show ip route command, 219, 222
 SOHO, 27
 split horizon rule, 164
 SSID cloaking, 255
 static routing, 157–158
 triggered updates, 164
 TTL fields, IP headers, 164
 wireless routers, logins, 258–259

RS messages, 51–52, 58–59

S

SaaS (Software as a Service), 33

safeguards, cybersecurity (McCumber) cube, 246–247

saving packet captures, 187–189

scanning tools, 237, 237, 239

scavenger class traffic, 174

scoring exams, 270

scripting VPN connections, 207–208

security

AAA, 250

access control, 248

administrative access control, 249–250

logical access control, 249

physical access control, 249, 252

accounting, 250

ACL, 250

AD, 251

administration, 251

authentication, 251

authorization, 251

components of, 251

directory services, 251

domains, 251

forests, 251

functions, 251

OU, 251

trees, 251

assets, 235

attacks

access attacks, 240

amplification/reflection attacks, 242

baiting, 241

buffer overflow attacks, 240

compromised key attacks, 238

data modification attacks, 237

DDoS attacks, 241

DoS attacks, 238, 241, 253

dumpster diving, 241

eavesdropping attacks, 237

ICMP attacks, 242

impersonation, 241

IP attacks, 241–242

MITM attacks, 238, 240, 242, 254–255

password attacks, 238, 240

phishing, 240

port redirection attacks, 240

pretexting, 240

reconnaissance attacks, 239

session hijacking, 242

shoulder surfing, 241

sniffer attacks, 238

social engineering attacks, 240–241

“something for something” (quid pro quo), 241

spam, 241

spear phishing, 240

spoofing attacks, 237, 240, 242

tailgating, 241

TCP reset attacks, 242

TCP session hijacking, 242

TCP SYN flood attacks, 242

transport layer attacks, 242–243

trust exploitation attacks, 240

UDP flood attacks, 243

audit trails, 248

authentication, 250

authorization, 250

awareness, 251

billing systems, 250

biometric security, 250

CIA Triad, 247

availability, 245, 249

confidentiality, 245, 248

defined, 245–246

integrity, 245, 248

communication protocols, 248

cybersecurity (McCumber) cube, 245

CIA Triad, 245–246, 247–249

data states, 246

principles of, 245–246

safeguards, 246–247

data exfiltration, 236

data loss vectors, 236

debuggers, 237

digital certificates, 248

encryption, 237, 248

exploits, 235, 237

failover mechanisms, 249

file permissions, Linux, 250

- firewalls, 227
 - application gateway (proxy) firewalls*, 229–230
 - Cisco IOS firewall example*, 230–231
 - host-based firewalls*, 231–233
 - iptables*, 232
 - nftables*, 232
 - NGFW*, 229–230
 - stateful firewalls*, 229
 - stateless firewalls*, 227–228
 - TCP Wrappers*, 233
 - Windows Defender Firewall*, 231–232
- forensic tools, 237
- hacking tools
 - network scanning/hacking*, 237
 - OS hacks*, 237
 - wireless hacking*, 237
- hashing algorithms, 248
- identity stores, 251
- log files, 250
- maintenance, 249
- malware
 - adware*, 238
 - ransomware*, 239
 - rootkits*, 239
 - spyware*, 239
 - Trojan horses*, 238
 - viruses*, 238
 - worms*, 238
- mitigation, 236
- network device logs, 250
- packets
 - crafting tools*, 237
 - sniffers*, 237, 238
- passwords, 250
 - attacks*, 238, 240
 - crackers*, 237
- penetration testing tools, 236–237
- programs, 251–252
- RBAC, 250
- redundancy, 249
- risks, 236
- rootkit detectors, 237
- scanning tools
 - network scanning/hacking*, 237
 - vulnerability scanners*, 237, 239
- smartcards, 250
- threats, defined, 235
- training, 251
- user awareness/training, 251
- vulnerabilities, 235
 - exploiting*, 237
 - scanners*, 237, 239
- wireless security
 - attacks (overview)*, 253
 - basic setups*, 262–266
 - DoS attacks*, 253–254
 - encryption*, 257
 - home router configurations*, 258
 - home user authentication*, 256–257
 - MAC address filtering*, 255–256
 - MITM attacks*, 254–255
 - passphrases*, 266
 - rogue AP*, 254
 - shared key authentication*, 256
 - SSID cloaking*, 255
 - verifying connectivity/access*, 266
 - WEP*, 256
 - wireless router logs*, 258–259
 - WPA*, 256, 257
 - WPA2*, 256–257
 - WPA3*, 256
- sending packets, 114**
- serialization delays, 15**
- server virtualization, 34–35**
- Service Unreachable messages, 48**
- session hijacking, 242**
- session layer, OSI model, 2**
- setting up networks**
 - basic setups, 259–262
 - wireless setups, 262–266
- Settings app (Windows 11), 121–122**
- SFTP (Secure FTP), 43, 45**
- shared key authentication, 256**
- shared memory, 172**
- shoulder surfing, 241**
- show commands**
 - defined, 219
 - show arp command, 219, 222
 - show interface status command, 219, 224
 - show interfaces command, 219, 220–221
 - show inventory command, 219, 225
 - show ip interface brief command, 226
 - show ip interface command, 219, 221–222
 - show ip route command, 131, 160–161, 219, 222
 - show mac address-table command, 219, 225
 - show protocols command, 219, 223
 - show running-config command, 219–220
 - show version command, 219, 223–224

- SLAAC (Stateless Address Autoconfiguration), 58–59**
 - neighbor discovery, 59–60
 - NS messages, 59–60
 - operation of, 60–61
 - RA messages, 59
 - RS messages, 58–59
 - smartcards, 250**
 - smartphones, 116**
 - SMF cable, 98–99**
 - SM-X slots, 153–154**
 - sniffers, packet, 237, 238**
 - SNMP (Simple Network Management Protocol), 211**
 - social engineering attacks, 240–241**
 - social networking as data loss vector, 236**
 - SOHO (Small Offices/Home Offices)**
 - Internet connections, 26–27
 - routers, 27
 - solicited-node multicast addresses, 86–87**
 - “something for something” (quid pro quo), 241**
 - spam, 241**
 - spear phishing, 240**
 - speed tests, 16–17**
 - speedtest command, 131**
 - SPF algorithm, 165–166**
 - split horizon rule, 164**
 - spoofing attacks, 237, 240, 242**
 - spyware, 239**
 - SSH (Secure Shell), 206**
 - SSID (Service Set Identifiers)**
 - cloaking, 255
 - configuring, 264
 - stateful firewalls, 229**
 - stateful operations, DHCPv6, 58–61**
 - stateless firewalls, 227–228**
 - states of data, cybersecurity (McCumber) cube, 246**
 - static NAT, 67**
 - static routing, 157–158**
 - status lights, devices, 139–140**
 - storage**
 - cloud storage as a data loss vector, 236
 - data storage, 246
 - store-and-forward switching, 171–172**
 - STP cable, 95**
 - straight-through UTP cable, 97–98**
 - Stratums, NTP, 46–47**
 - structured troubleshooting methods, 178–179**
 - subnetting**
 - addressing schemes, 74
 - borrowing bits, 72–73
 - examples, 74–76
 - methodology, 72–74
 - multipliers, determining, 74
 - octet binary values, 73
 - octet decimal values, 73
 - subnet masks, 70–71
 - ANDing, 71*
 - binary values, 72*
 - determining new masks, 73–74*
 - substitution troubleshooting method, 179**
 - switches/switching**
 - access layer switches, 144
 - asymmetric switching, 172
 - broadcast domains, 171
 - collision domains, 171
 - core layer switches, 145
 - cut-through switching, 172
 - distribution layer switches, 145
 - Ethernet switches, 170
 - evolution to, 169–170
 - forwarding, 170
 - fragment-free switching, 172
 - frame forwarding, 171
 - Layer 2 switching, 172
 - Layer 3 switching, 172
 - logic, 170–171
 - MAC addresses, 170–171
 - memory buffering, 172
 - overview, 143
 - packet forwarding, 156
 - show ip interface brief command, 226
 - store-and-forward switching, 171–172
 - symmetric switching, 172
 - syntax help, commands, 215**
 - Syslog, 211**
- ## T
- tablets/phablets, 117**
 - tailgating, 241**
 - TCP (Transport Control Protocol), 37**

- attacks
 - reset attacks*, 242
 - session hijacking*, 242
 - TCP SYN flood attacks*, 242
- connection establishment/termination, 40–41
- error recovery (reliability), 39–40
- flow control, 40
- headers, 38, 41
- port numbers, 38–39
- TCP Wrappers, 233
- windowing, 40
- TCP/IP model**, 1, 7
 - application layer, 3, 5
 - Internet layer, 3, 6–7
 - network access layer, 7–8
 - PDU, 9–10
 - protocols, 8
 - transport layer, 3, 5–6
 - transport layer attacks, 242–243
- telephony traffic, IP**, 173
- Telnet**, 207
- Ten Gigabit Ethernet 0/0/4 and 0/0/5 ports**, 152
- terminal emulators**, 208–209
- terminating TCP connections**, 40–41
- testing, penetration testing tools**, 236–237
- TFTP (Trivial FTP)**, 43, 46
- threats, security**, 235
- three-tiered campus design**, 28
- throughput**, 13–14
- ticketing systems**, 181–182
- Time Exceeded messages**, 49
- timers, hold-down**, 164
- TKIP (Total Key Integrity Protocol)**, 257
- top-down troubleshooting method**, 178
- topologies**
 - NAT, 65
 - networks
 - CAN, 26
 - full mesh topologies*, 23–24
 - hub-and-spoke topologies*, 23
 - hybrid topologies*, 24
 - LAN, 21–22
 - logical topologies*, 24–25, 147, 148–149
 - MAN, 26
 - PAN, 26
 - physical topologies*, 24–25, 146, 147–148
 - point-to-point topologies*, 23
 - variations of*, 26
 - WAN, 23–24
 - WLAN, 26
- traceroute command**, 49–50
- tracert command**, 128, 201–203
- traffic, VLAN**
 - IP
 - multicast traffic*, 174
 - telephony traffic*, 173
 - management traffic, 173
 - normal data traffic, 174
 - scavenger class traffic, 174
- training, security**, 251
- transmitting data**, 246
- transport layer, TCP/IP**, 3, 5–6, 242–243
- transport protocols**
 - connectionless protocols, 37–38
 - connection-oriented protocols, 37–38
 - TCP, 37
 - connection establishment/termination*, 40–41
 - error recovery (reliability)*, 39–40
 - flow control*, 40
 - headers*, 38, 41
 - port numbers*, 38–39
 - windowing*, 40
 - UDP, 37
 - headers*, 41
 - port numbers*, 38–39
- transportation layer**, 2
- trees, AD**, 251
- triggered updates, routing tables**, 164
- Trojan horses**, 238
- trouble tickets**
 - fields, 182
 - ticketing process, 181
- troubleshooting**
 - bottom-up troubleshooting method, 178
 - comparison troubleshooting method, 179
 - divide-and-conquer troubleshooting method, 178
 - educated guess troubleshooting method, 179
 - follow-the-path troubleshooting method, 178

- help desks, 180
 - policies/procedures, 180*
 - prioritization/escalation, 180–181*
 - ticketing systems, 181–182*
 - trouble tickets, 181–182*
- methodologies (overview), 177
- selecting a troubleshooting method, 179
- structured troubleshooting methods, 178–179
- substitution troubleshooting method, 179
- top-down troubleshooting method, 178

trust exploitation attacks, 240

TTL fields, IP headers, 164

tunnels

- data encapsulation, 10–11
- IPv6 addressing, 89

two-tiered campus design, 28–29

U

UDP (User Datagram Protocol), 37

- flood attacks, 243
- headers, 41
- port numbers, 38–39

ULA (Unique Local Addresses), 84

unencrypted devices as a data loss vector, 236

unicast addresses, 80

- 3–1-4 (pi) rule, 80
- global unicast addresses, 80–82
- IPv4 embedded addresses, 84–85
- link-local addresses, 82–83
- loopback addresses, 83
- ULA, 84
- unspecified addresses, 83

unspecified unicast addresses, 83

updates (routing tables), triggered, 164

URI (Uniform Resource Identifiers), 61

USB ports, Cisco 4461 ISR, 152

users

- home user authentication, 256–257
- security awareness/training, 251

UTP cable, 94–95

- categories, 96–97
- connectors, 97
- crossover UTP cable, 97–98
- straight-through UTP cable, 97–98

V

verifying

- connectivity/access
 - Android, 135–136*
 - iOS, 135–136*
 - Linux, 130–132*
 - mobile devices, 135–137*
 - Windows 11, 127–128*
 - wireless security, 266*
- new IP addresses were added to interfaces, 196–197
- NTP, 47–48

versioning, show version command, 219, 223–224

viewing

- ARP caches in Windows 11, 125–126
- ARP tables, 197
- host routing tables in Windows 11, 126–127
- IP configuration information in Windows 11, 124–125
- IP settings
 - Linux devices, 194–195*
 - macOS devices, 194–195*
 - Windows devices, 191–192*
- routing tables, 197
- routing tables in Linux, 132

virtualization

- hosts, 114–116
- servers, 34–35

viruses, 238

VLAN (Virtual LAN)

- benefits of, 173
- black hole VLAN, 174
- data VLAN, 174
- default VLAN, 174
- IP
 - multicast traffic, 174*
 - telephony traffic, 173*
- management traffic, 173
- management VLAN, 174
- native VLAN, 174
- normal data traffic, 174
- reasons for using, 172–173
- scavenger class traffic, 174
- traffic, types of, 173–174
- types of, 174
- voice VLAN, 174–175

VPN (Virtual Private Networks), 207

- automating connections, 207–208

- scripting connections, 207–208
- tunnels, 10–11
- Windows configurations, 207–208

vulnerabilities

- exploits, 237
- scanners, 237, 239
- security, 235

W**WAN (Wide Area Networks)**

- connecting to, 22–23
- topologies, 23–26

WEP (Wired Equivalent Privacy), 256**Wi-Fi networks, 105, 109–110****windowing, TCP, 40****Windows 11**

- arp -a command, 125–126
- command line, 124–127
- connectivity/access, verifying, 127–128
- Control Panel, 122–124
- getmac /v command, 124
- Get-NetRoute command, 126–127
- ipconfig command, 124–125
- IP settings
 - releasing, 193–194*
 - renewing, 193–194*
 - viewing, 191–192*
- netstat command, 203
- ping command, 127, 197–198, 199
- PowerShell, 124–127
- route print command, 127
- Settings app, 121–122
- tracert command, 128, 202–203
- viewing
 - ARP caches, 125–126*
 - host routing tables, 126–127*
 - IP configuration information, 124–125*
- VPN configurations, 207–208
- Windows Defender Firewall, 231–232

Windows Defender Firewall, 231–232

wireless hacking tools, 237

wireless router logins, 258–259

wireless security

- attacks
 - DoS attacks, 253–254*
 - MITM attacks, 254–255*
 - overview, 253*
 - rogue AP, 254*

- configuring
 - basic setups, 262–266*
 - home routers, 258*
- encryption, 257
- home user authentication, 256–257
- MAC address filtering, 255–256
- passphrases, 266
- shared key authentication, 256
- SSID cloaking, 255
- verifying connectivity/access, 266
- WEP, 256
- wireless router logins, 258–259
- WPA, 256, 257
- WPA2, 256–257
- WPA3, 256

wireless technologies

- 802.11 standards, 107–108
- cellular networks, 109–110
- channels, 105–106
- crosstalk, 93
- EMI, 93
- interference, 93, 108–109
- mobile cores, 111
- network connectivity, 91, 92
- RAN, 111
- RF spectrum, 105–106
- RFI, 93
- Wi-Fi, 105
- Wi-Fi networks, 109–110

Wireshark network monitoring

- downloading, 186
- features of, 185
- installing, 186
- overview, 185
- packet capturing, 186
 - opening captures, 189*
 - saving captures, 187–189*
- users, 186

WLAN (Wireless LAN), 26**Word help, 215****worms, 238****WPA (Wi-Fi Protected Access), 256, 257****WPA2, 256–257****WPA3, 256****writing conventions, IPv6 addressing**

- addresses, 88
- prefixes, 88–89