CCNAv7:
Intoduction to Network (ITN)

Companion Guide

Networking Academy

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Introduction to Networks Companion Guide (CCNAv7)

Cisco Networking Academy

Cisco Press

Introduction to Networks Companion Guide (CCNAv7)

Cisco Networking Academy

Published by:
Cisco Press

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020935402

ISBN-13: 978-0-13-663366-2
ISBN-10: 0-13-663366-8

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Introduction to Networks (CCNAv7) course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

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

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.

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

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

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

Editor-in-Chief
Mark Taub

Alliances Manager, Cisco Press
Arezou Gol

Director, ITP Product Management
Brett Bartow

Senior Editor
James Manly

Managing Editor
Sandra Schroeder

Development Editor
Christopher Cleveland

Senior Project Editor
Tonya Simpson

Copy Editor
Kitty Wilson

Technical Editor
Bob Vachon

Editorial Assistant
Cindy Teeters

Cover Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Erika Millen

Proofreader
Abigail Manheim

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 screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

About the Contributing Authors

Rick Graziani teaches computer science and computer networking courses at Cabrillo College and University of California, Santa Cruz in Santa Cruz, California. Prior to teaching, Rick worked in the information technology field for Santa Cruz Operation, Tandem Computers, and Lockheed Missiles and Space Corporation, and he served in the U.S. Coast Guard. He holds an M.A. in computer science and systems theory from California State University, Monterey Bay. Rick also works as a curriculum developer for the Cisco Networking Academy Curriculum Engineering team. When Rick is not working, he is most likely surfing at one of his favorite Santa Cruz surf breaks.

Allan Johnson entered the academic world in 1999, after 10 years as a business owner/operator, to dedicate his efforts to his passion for teaching. He holds both an M.B.A. and an M.Ed. 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 works full time for Cisco Networking Academy as Curriculum Lead.

Contents at a Glance

Introduction xxx

Chapter 1 Networking Today 1

Chapter 2 Basic Switch and End Device Configuration 45

Chapter 3 Protocols and Models 85

Chapter 4 Physical Layer 137

Chapter 5 Number Systems 175

Chapter 6 Data Link Layer 203

Chapter 7 Ethernet Switching 233

Chapter 8 Network Layer 267

Chapter 9 Address Resolution 297

Chapter 10 Basic Router Configuration 319

Chapter 11 IPv4 Addressing 341

Chapter 12 IPv6 Addressing 397

Chapter 13 ICMP 443

Chapter 14 Transport Layer 461

Chapter 15 Application Layer 507

Chapter 16 Network Security Fundamentals 541

Chapter 17 Build a Small Network 571

Appendix A Answers to “Check Your Understanding” Questions 631

Key Terms Glossary 645

Index 669

Contents

Introduction xxx

Chapter 1 Networking Today 1

Objectives 1

Key Terms 1

Introduction (1.0) 3

Networks Affect Our Lives (1.1) 3

Networks Connect Us (1.1.1) 3

No Boundaries (1.1.3) 3

Network Components (1.2) 4

Host Roles (1.2.1) 4

Peer-to-Peer (1.2.2) 5

End Devices (1.2.3) 6

Intermediary Devices (1.2.4) 6

Network Media (1.2.5) 7

Network Representations and Topologies (1.3) 8

Network Representations (1.3.1) 8

Topology Diagrams (1.3.2) 10

Physical Topology Diagrams 10

Logical Topology Diagrams 10

Common Types of Networks (1.4) 11

Networks of Many Sizes (1.4.1) 11

LANs and WANs (1.4.2) 12

LANs 13

WANs 14

The Internet (1.4.3) 15

Intranets and Extranets (1.4.4) 16

Internet Connections (1.5) 17

Internet Access Technologies (1.5.1) 17

Home and Small Office Internet Connections (1.5.2) 18

Businesses Internet Connections (1.5.3) 19

The Converging Network (1.5.4) 20

Reliable Networks (1.6) 23
Network Architecture (1.6.1) 23
Fault Tolerance (1.6.2) 24
Scalability (1.6.3) 24
Quality of Service (1.6.4) 25
Network Security (1.6.5) 26
Network Trends (1.7) 27
Recent Trends (1.7.1) 28
Bring Your Own Device (BYOD) (1.7.2) 28
Online Collaboration (1.7.3) 28
Video Communications (1.7.4) 29
Cloud Computing (1.7.6) 29
Technology Trends in the Home (1.7.7) 31
Powerline Networking (1.7.8) 31
Wireless Broadband (1.7.9) 32
Wireless Internet Service Providers 32
Wireless Broadband Service 32
Network Security (1.8) 33
Security Threats (1.8.1) 33
Security Solutions (1.8.2) 34
The IT Professional (1.9) 35
CCNA (1.9.1) 35
Networking Jobs (1.9.2) 36
Summary (1.10) 37
Networks Affect Our Lives 37
Network Components 37
Network Representations and Topologies 37
Common Types of Networks 37
Internet Connections 38
Reliable Networks 38
Network Trends 38
Network Security 39
The IT Professional 40
Practice 40
Check Your Understanding Questions 40

Chapter 2 Basic Switch and End Device Configuration 45

Objectives 45

Key Terms 45

Introduction (2.0) 46

Cisco IOS Access (2.1) 46

Operating Systems (2.1.1) 46

GUI (2.1.2) 47

Purpose of an OS (2.1.3) 48

Access Methods (2.1.4) 49

Terminal Emulation Programs (2.1.5) 50

IOS Navigation (2.2) 52

Primary Command Modes (2.2.1) 52

Configuration Mode and Subconfiguration Modes (2.2.2) 53

Navigate Between IOS Modes (2.2.4) 54

A Note About Syntax Checker Activities (2.2.6) 55

The Command Structure (2.3) 56

Basic IOS Command Structure (2.3.1) 56

IOS Command Syntax Check (2.3.2) 57

IOS Help Features (2.3.3) 58

Hot Keys and Shortcuts (2.3.5) 58

Basic Device Configuration (2.4) 61

Device Names (2.4.1) 61

Password Guidelines (2.4.2) 62

Configure Passwords (2.4.3) 63

Encrypt Passwords (2.4.4) 64

Banner Messages (2.4.5) 65

Save Configurations (2.5) 66

Configuration Files (2.5.1) 67

Alter the Running Configuration (2.5.2) 68

Capture Configuration to a Text File (2.5.4) 68

Ports and Addresses (2.6) 71

IP Addresses (2.6.1) 71

Interfaces and Ports (2.6.2) 73

Configure IP Addressing (2.7) 74
Manual IP Address Configuration for End Devices (2.7.1) 75
Automatic IP Address Configuration for End Devices (2.7.2) 76
Switch Virtual Interface Configuration (2.7.4) 77
Verify Connectivity (2.8) 78
Summary (2.9) 79
Cisco IOS Access 79
IOS Navigation 79
The Command Structure 79
Basic Device Configuration 79
Save Configurations 80
Ports and Addresses 80
Configure IP Addressing 80
Verify Connectivity 80
Practice 81
Check Your Understanding Questions 81

Chapter 3 Protocols and Models 85
Objectives 85
Key Terms 85
Introduction (3.0) 86
The Rules (3.1) 86
Communications Fundamentals (3.1.2) 86
Communication Protocols (3.1.3) 87
Rule Establishment (3.1.4) 88
Network Protocol Requirements (3.1.5) 88
Message Encoding (3.1.6) 89
Message Formatting and Encapsulation (3.1.7) 90
Message Size (3.1.8) 91
Message Timing (3.1.9) 92
Message Delivery Options (3.1.10) 92
A Note About the Node Icon (3.1.11) 94
Protocols 94
Network Protocol Overview (3.2.1) 94
Network Protocol Functions (3.2.2) 95
Protocol Interaction (3.2.3) 96

Protocol Suites (3.3) 97

Network Protocol Suites (3.3.1) 97

Evolution of Protocol Suites (3.3.2) 98

TCP/IP Protocol Example (3.3.3) 99

TCP/IP Protocol Suite (3.3.4) 99

Application Layer 101
Transport Layer 102
Internet Layer 102
Network Access Layer 103

TCP/IP Communication Process (3.3.5) 103

Standards Organizations (3.4) 108

Open Standards (3.4.1) 108

Internet Standards (3.4.2) 108

Electronic and Communications Standards (3.4.3) 111

Reference Models (3.5) 111

The Benefits of Using a Layered Model (3.5.1) 112

The OSI Reference Model (3.5.2) 112

The TCP/IP Protocol Model (3.5.3) 114

OSI and TCP/IP Model Comparison (3.5.4) 115

Data Encapsulation (3.6) 116

Segmenting Messages (3.6.1) 116

Sequencing (3.6.2) 118

Protocol Data Units (3.6.3) 118

Encapsulation Example (3.6.4) 120

De-encapsulation Example (3.6.5) 120

Data Access (3.7) 121

Addresses (3.7.1) 121

Layer 3 Logical Address (3.7.2) 122

Devices on the Same Network (3.7.3) 123

Role of the Data Link Layer Addresses: Same IP Network (3.7.4) 124

Devices on a Remote Network (3.7.5) 125

Role of the Network Layer Addresses (3.7.6) 125

Role of the Data Link Layer Addresses: Different IP Networks (3.7.7) 126

Data Link Addresses (3.7.8) 127

Summary (3.8) 130
The Rules 130
Protocols 130
Protocol Suites 130
Standards Organizations 131
Reference Models 131
Data Encapsulation 132
Data Access 132
Practice 133
Check Your Understanding Questions 133

Chapter 4 Physical Layer 137
Objectives 137
Key Terms 137
Introduction (4.0) 138
Purpose of the Physical Layer (4.1) 138
The Physical Connection (4.1.1) 138
The Physical Layer (4.1.2) 139
Physical Layer Characteristics (4.2) 141
Physical Layer Standards (4.2.1) 141
Physical Components (4.2.2) 142
Encoding (4.2.3) 142
Signaling (4.2.4) 143
Bandwidth (4.2.5) 145
Bandwidth Terminology (4.2.6) 145
Latency 146
Throughput 146
Goodput 146
Copper Cabling (4.3) 146
Characteristics of Copper Cabling (4.3.1) 147
Types of Copper Cabling (4.3.2) 148
Unshielded Twisted-Pair (UTP) (4.3.3) 148
Shielded Twisted-Pair (STP) (4.3.4) 150
Coaxial Cable (4.3.5) 151

UTP Cabling (4.4) 152
Properties of UTP Cabling (4.4.1) 152
UTP Cabling Standards and Connectors (4.4.2) 153
Straight-Through and Crossover UTP Cables (4.4.3) 157

Fiber-Optic Cabling (4.5) 158
Properties of Fiber-Optic Cabling (4.5.1) 158
Types of Fiber Media (4.5.2) 159
Single-Mode Fiber 159
Multimode Fiber 160
Fiber-Optic Cabling Usage (4.5.3) 160
Fiber-Optic Connectors (4.5.4) 161
Fiber Patch Cords (4.5.5) 162
Fiber Versus Copper (4.5.6) 163

Wireless Media (4.6) 164
Properties of Wireless Media (4.6.1) 164
Types of Wireless Media (4.6.2) 165
Wireless LAN (4.6.3) 166

Summary (4.7) 168
Purpose of the Physical Layer 168
Physical Layer Characteristics 168
Copper Cabling 168
UTP Cabling 169
Fiber-Optic Cabling 169
Wireless Media 169

Practice 170

Check Your Understanding Questions 170

Chapter 5 Number Systems 175

Objectives 175

Key Terms 175

Introduction (5.0) 176

Binary Number System (5.1) 176
Binary and IPv4 Addresses (5.1.1) 176
Binary Positional Notation (5.1.3) 178

Convert Binary to Decimal (5.1.5) 180
Decimal to Binary Conversion (5.1.7) 182
Decimal to Binary Conversion Example (5.1.8) 186
IPv4 Addresses (5.1.11) 193

Hexadecimal Number System (5.2) 194
Hexadecimal and IPv6 Addresses (5.2.1) 194
Decimal to Hexadecimal Conversions (5.2.3) 196
Hexadecimal to Decimal Conversion (5.2.4) 196

Summary (5.3) 198
Binary Number System 198
Hexadecimal Number System 198

Practice 198

Check Your Understanding Questions 198

Chapter 6 Data Link Layer 203

Objectives 203

Key Terms 203

Introduction (6.0) 204

Purpose of the Data Link Layer (6.1) 204
The Data Link Layer (6.1.1) 204
IEEE 802 LAN/MAN Data Link Sublayers (6.1.2) 206
Providing Access to Media (6.1.3) 207
Data Link Layer Standards (6.1.4) 209

Topologies (6.2) 209
Physical and Logical Topologies (6.2.1) 209
WAN Topologies (6.2.2) 211
Point-to-Point 211
Hub and Spoke 211
Mesh 212
Point-to-Point WAN Topology (6.2.3) 213
LAN Topologies (6.2.4) 213
Legacy LAN Topologies 214
Half-Duplex and Full-Duplex Communication (6.2.5) 215
Half-Duplex Communication 215
Full-Duplex Communication 215

Access Control Methods (6.2.6) 216
Contention-Based Access 216
Controlled Access 217
Contention-Based Access—CSMA/CD (6.2.7) 217
Contention-Based Access—CSMA/CA (6.2.8) 219

Data Link Frame (6.3) 221
The Frame (6.3.1) 221
Frame Fields (6.3.2) 222
Layer 2 Addresses (6.3.3) 223
LAN and WAN Frames (6.3.4) 225

Summary (6.4) 228
Purpose of the Data Link Layer 228
Topologies 228
Data Link Frame 229

Practice 229

Check Your Understanding Questions 229

Chapter 7 Ethernet Switching 233

Objectives 233

Key Terms 233

Introduction (7.0) 234

Ethernet Frames (7.1) 234
Ethernet Encapsulation (7.1.1) 234
Data Link Sublayers (7.1.2) 235
MAC Sublayer (7.1.3) 236
Data Encapsulation 236
Accessing the Media 237
Ethernet Frame Fields (7.1.4) 237

Ethernet MAC Address (7.2) 239
MAC Address and Hexadecimal (7.2.1) 240
Ethernet MAC Address (7.2.2) 241
Frame Processing (7.2.3) 243
Unicast MAC Address (7.2.4) 244
Broadcast MAC Address (7.2.5) 246
Multicast MAC Address (7.2.6) 247

The MAC Address Table (7.3) 248
Switch Fundamentals (7.3.1) 248
Switch Learning and Forwarding (7.3.2) 250
Examine the Source MAC Address 250
Find the Destination MAC Address 250
Filtering Frames (7.3.3) 252
Switch Speeds and Forwarding Methods (7.4) 254
Frame Forwarding Methods on Cisco Switches (7.4.1) 254
Cut-Through Switching (7.4.2) 255
Memory Buffering on Switches (7.4.3) 257
Duplex and Speed Settings (7.4.4) 257
Auto-MDIX (7.4.5) 259
Summary (7.5) 261
Ethernet Frame 261
Ethernet MAC Address 261
The MAC Address Table 261
Switch Speeds and Forwarding Methods 262
Practice 262
Check Your Understanding Questions 262
Chapter 8 Network Layer 267
Objectives 267
Key Terms 267
Introduction (8.0) 268
Network Layer Characteristics (8.1) 268
The Network Layer (8.1.1) 268
IP Encapsulation (8.1.2) 270
Characteristics of IP (8.1.3) 271
Connectionless (8.1.4) 271
Best Effort (8.1.5) 272
Media Independent (8.1.6) 273
IPv4 Packet (8.2) 274
IPv4 Packet Header (8.2.1) 274
IPv4 Packet Header Fields (8.2.2) 274
IPv6 Packet (8.3) 276
Limitations of IPv4 (8.3.1) 277
IPv6 Overview (8.3.2) 277

IPv4 Packet Header Fields in the IPv6 Packet Header (8.3.3) 278
IPv6 Packet Header (8.3.4) 280

How a Host Routes (8.4) 281
Host Forwarding Decision (8.4.1) 281
Default Gateway (8.4.2) 282
A Host Routes to the Default Gateway (8.4.3) 283
Host Routing Tables (8.4.4) 283

Introduction to Routing (8.5) 285
Router Packet Forwarding Decision (8.5.1) 285
IP Router Routing Table (8.5.2) 286
Static Routing (8.5.3) 287
Dynamic Routing (8.5.4) 288
Introduction to an IPv4 Routing Table (8.5.6) 290

Summary (8.6) 292
Network Layer Characteristics 292
IPv4 Packet 292
IPv6 Packet 292
How a Host Routes 293
Introduction to Routing 293

Practice 294

Check Your Understanding Questions 294

Chapter 9 Address Resolution 297

Objectives 297

Key Terms 297

Introduction (9.0) 298

MAC and IP (9.1) 298
Destination on Same Network (9.1.1) 298
Destination on Remote Network (9.1.2) 299

ARP (9.2) 301
ARP Overview (9.2.1) 301
ARP Functions (9.2.2) 302
Removing Entries from an ARP Table (9.2.6) 306
ARP Tables on Networking Devices (9.2.7) 306
ARP Issues—ARP Broadcasts and ARP Spoofing (9.2.8) 307

IPv6 Neighbor Discovery (9.3) 309
IPv6 Neighbor Discovery Messages (9.3.2) 309
IPv6 Neighbor Discovery—Address Resolution (9.3.3) 311
Summary (9.4) 313
MAC and IP 313
ARP 313
Neighbor Discovery 314
Practice 314
Check Your Understanding Questions 314

Chapter 10 Basic Router Configuration 319
Objectives 319
Introduction (10.0) 320
Configure Initial Router Settings (10.1) 320
Basic Router Configuration Steps (10.1.1) 320
Basic Router Configuration Example (10.1.2) 321
Configure Interfaces (10.2) 323
Configure Router Interfaces (10.2.1) 323
Configure Router Interfaces Example (10.2.2) 324
Verify Interface Configuration (10.2.3) 325
Configuration Verification Commands (10.2.4) 326
Configure the Default Gateway (10.3) 330
Default Gateway on a Host (10.3.1) 331
Default Gateway on a Switch (10.3.2) 332
Summary (10.4) 335
Configure Initial Router Settings 335
Configure Interfaces 335
Configure the Default Gateway 335
Practice 336
Check Your Understanding Questions 337

Chapter 11 IPv4 Addressing 341
Objectives 341
Key Terms 341
Introduction (11.0) 342

IPv4 Address Structure (11.1) 342

Network and Host Portions (11.1.1) 342

The Subnet Mask (11.1.2) 343

The Prefix Length (11.1.3) 344

Determining the Network: Logical AND (11.1.4) 345

Network, Host, and Broadcast Addresses (11.1.6) 347

Network Address 347

Host Addresses 348

Broadcast Address 349

IPv4 Unicast, Broadcast, and Multicast (11.2) 349

Unicast (11.2.1) 349

Broadcast (11.2.2) 350

IP Directed Broadcasts 351

Multicast (11.2.3) 352

Types of IPv4 Addresses (11.3) 353

Public and Private IPv4 Addresses (11.3.1) 353

Routing to the Internet (11.3.2) 354

Special Use IPv4 Addresses (11.3.4) 356

Loopback Addresses 356

Link-Local Addresses 357

Legacy Classful Addressing (11.3.5) 357

Assignment of IP Addresses (11.3.6) 358

Network Segmentation (11.4) 359

Broadcast Domains and Segmentation (11.4.1) 359

Problems with Large Broadcast Domains (11.4.2) 360

Reasons for Segmenting Networks (11.4.3) 362

Subnet an IPv4 Network (11.5) 364

Subnet on an Octet Boundary (11.5.1) 364

Subnet Within an Octet Boundary (11.5.2) 366

Subnet a Slash 16 and a Slash 8 Prefix (11.6) 367

Create Subnets with a Slash 16 Prefix (11.6.1) 367

Create 100 Subnets with a Slash 16 Prefix (11.6.2) 369

Create 1000 Subnets with a Slash 8 Prefix (11.6.3) 372

Subnet to Meet Requirements (11.7) 374

Subnet Private Versus Public IPv4 Address Space (11.7.1) 374

What About the DMZ? 377

Minimize Unused Host IPv4 Addresses and Maximize Subnets (11.7.2) 377
Example: Efficient IPv4 Subnetting (11.7.3) 378

VLSM (11.8) 381
IPv4 Address Conservation (11.8.3) 381
VLSM (11.8.4) 383
VLSM Topology Address Assignment (11.8.5) 386

Structured Design (11.9) 387
IPv4 Network Address Planning (11.9.1) 388
Device Address Assignment (11.9.2) 389

Summary (11.10) 390
IPv4 Addressing Structure 390
IPv4 Unicast, Broadcast, and Multicast 390
Types of IPv4 Addresses 390
Network Segmentation 391
Subnet an IPv4 Network 391
Subnet a /16 and a /8 Prefix 391
Subnet to Meet Requirements 391
Variable-Length Subnet Masking 392
Structured Design 392

Practice 393

Check Your Understanding Questions 393

Chapter 12 IPv6 Addressing 397

Objectives 397

Key Terms 397

Introduction (12.0) 398

IPv4 Issues (12.1) 398
Need for IPv6 (12.1.1) 398
Internet of Things 399
IPv4 and IPv6 Coexistence (12.1.2) 399
Dual Stack 399
Tunneling 400
Translation 401

IPv6 Address Representation (12.2) 401

IPv6 Addressing Formats (12.2.1) 401

Preferred Format 402

Rule 1—Omit Leading Zeros (12.2.2) 403

Rule 2—Double Colon (12.2.3) 404

IPv6 Address Types (12.3) 406

Unicast, Multicast, Anycast (12.3.1) 406

IPv6 Prefix Length (12.3.2) 406

Types of IPv6 Unicast Addresses (12.3.3) 407

A Note About the Unique Local Address (12.3.4) 408

IPv6 GUA (12.3.5) 408

IPv6 GUA Structure (12.3.6) 409

Global Routing Prefix 410

Subnet ID 410

Interface ID 410

IPv6 LLA (12.3.7) 411

GUA and LLA Static Configuration (12.4) 413

Static GUA Configuration on a Router (12.4.1) 413

Static GUA Configuration on a Windows Host (12.4.2) 414

Static Configuration of a Link-Local Unicast Address (12.4.3) 415

Dynamic Addressing for IPv6 GUAs (12.5) 417

RS and RA Messages (12.5.1) 417

Method 1: SLAAC (12.5.2) 418

Method 2: SLAAC and Stateless DHCPv6 (12.5.3) 419

Method 3: Stateful DHCPv6 (12.5.4) 420

EUI-64 Process vs. Randomly Generated (12.5.5) 421

EUI-64 Process (12.5.6) 422

Randomly Generated Interface IDs (12.5.7) 424

Dynamic Addressing for IPv6 LLAs (12.6) 425

Dynamic LLAs (12.6.1) 425

Dynamic LLAs on Windows (12.6.2) 425

Dynamic LLAs on Cisco Routers (12.6.3) 426

Verify IPv6 Address Configuration (12.6.4) 427

IPv6 Multicast Addresses (12.7) 430
Assigned IPv6 Multicast Addresses (12.7.1) 430
Well-Known IPv6 Multicast Addresses (12.7.2) 430
Solicited-Node IPv6 Multicast Addresses (12.7.3) 432

Subnet an IPv6 Network (12.8) 432
Subnet Using the Subnet ID (12.8.1) 432
IPv6 Subnetting Example (12.8.2) 433
IPv6 Subnet Allocation (12.8.3) 434
Router Configured with IPv6 Subnets (12.8.4) 435

Summary (12.9) 436
IPv4 Issues 436
IPv6 Address Representation 436
IPv6 Address Types 436
GUA and LLA Static Configuration 437
Dynamic Addressing for IPv6 GUAs 437
Dynamic Addressing for IPv6 LLAs 437
IPv6 Multicast Addresses 438
Subnet an IPv6 Network 438

Practice 439

Check Your Understanding Questions 439

Chapter 13 ICMP 443

Objectives 443

Introduction (13.0) 444

ICMP Messages (13.1) 444
ICMPv4 and ICMPv6 Messages (13.1.1) 444
Host Reachability (13.1.2) 444
Destination or Service Unreachable (13.1.3) 445
Time Exceeded (13.1.4) 446
ICMPv6 Messages (13.1.5) 446

Ping and Traceroute Tests (13.2) 449
Ping—Test Connectivity (13.2.1) 449
Ping the Loopback (13.2.2) 450
Ping the Default Gateway (13.2.3) 450
Ping a Remote Host (13.2.4) 451

Traceroute—Test the Path (13.2.5) 452
Round-Trip Time (RTT) 453
IPv4 TTL and IPv6 Hop Limit 453

Summary (13.3) 454

ICMP Messages 454

Ping and Traceroute Testing 454

Practice 455

Check Your Understanding Questions 456

Chapter 14 Transport Layer 461

Objectives 461

Key Terms 461

Introduction (14.0) 462

Transportation of Data (14.1) 462

Role of the Transport Layer (14.1.1) 462

Transport Layer Responsibilities (14.1.2) 463

Transport Layer Protocols (14.1.3) 467

Transmission Control Protocol (TCP) (14.1.4) 467

User Datagram Protocol (UDP) (14.1.5) 468

The Right Transport Layer Protocol for the Right Application (14.1.6) 469

TCP Overview (14.2) 470

TCP Features (14.2.1) 470

TCP Header (14.2.2) 471

TCP Header Fields (14.2.3) 471

Applications That Use TCP (14.2.4) 472

UDP Overview (14.3) 473

UDP Features (14.3.1) 473

UDP Header (14.3.2) 474

UDP Header Fields (14.3.3) 474

Applications that use UDP (14.3.4) 475

Port Numbers (14.4) 476

Multiple Separate Communications (14.4.1) 476

Socket Pairs (14.4.2) 477

Port Number Groups (14.4.3) 478

The netstat Command (14.4.4) 479

TCP Communication Process (14.5) 480
TCP Server Processes (14.5.1) 480
TCP Connection Establishment (14.5.2) 483
Session Termination (14.5.3) 484
TCP Three-Way Handshake Analysis (14.5.4) 485
Reliability and Flow Control (14.6) 486
TCP Reliability—Guaranteed and Ordered Delivery (14.6.1) 486
TCP Reliability—Data Loss and Retransmission (14.6.3) 488
TCP Flow Control—Window Size and Acknowledgments (14.6.5) 490
TCP Flow Control—Maximum Segment Size (MSS) (14.6.6) 491
TCP Flow Control—Congestion Avoidance (14.6.7) 493
UDP Communication (14.7) 494
UDP Low Overhead Versus Reliability (14.7.1) 494
UDP Datagram Reassembly (14.7.2) 494
UDP Server Processes and Requests (14.7.3) 495
UDP Client Processes (14.7.4) 495
Summary (14.8) 499
Transportation of Data 499
TCP Overview 499
UDP Overview 499
Port Numbers 499
TCP Communications Process 500
Reliability and Flow Control 500
UDP Communication 501
Practice 501
Check Your Understanding Questions 502

Chapter 15 Application Layer 507
Objectives 507
Key Terms 507
Introduction (15.0) 508
Application, Presentation, and Session (15.1) 508
Application Layer (15.1.1) 508
Presentation and Session Layer (15.1.2) 508
TCP/IP Application Layer Protocols (15.1.3) 510

Peer-to-Peer (15.2) 511

Client-Server Model (15.2.1) 511

Peer-to-Peer Networks (15.2.2) 512

Peer-to-Peer Applications (15.2.3) 513

Common P2P Applications (15.2.4) 514

Web and Email Protocols (15.3) 515

Hypertext Transfer Protocol and Hypertext Markup Language (15.3.1) 515

HTTP and HTTPS (15.3.2) 516

Email Protocols (15.3.3) 518

SMTP, POP, and IMAP (15.3.4) 519

SMTP 519

POP 520

IMAP 521

IP Addressing Services (15.4) 521

Domain Name Service (15.4.1) 522

DNS Message Format (15.4.2) 524

DNS Hierarchy (15.4.3) 525

The nslookup Command (15.4.4) 526

Dynamic Host Configuration Protocol (15.4.6) 527

DHCP Operation (15.4.7) 528

File Sharing Services (15.5) 530

File Transfer Protocol (15.5.1) 530

Server Message Block (15.5.2) 531

Summary 534

Application, Presentation, and Session 534

Peer-to-Peer 534

Web and Email Protocols 534

IP Addressing Services 535

File Sharing Services 535

Practice 536

Check Your Understanding Questions 536

Chapter 16 Network Security Fundamentals 541

Objectives 541

Key Terms 541

Introduction (16.0) 542

Security Threats and Vulnerabilities (16.1) 542

Types of Threats (16.1.1) 542

Types of Vulnerabilities (16.1.2) 543

Physical Security (16.1.3) 545

Network Attacks (16.2) 546

Types of Malware (16.2.1) 546

Viruses 546
Worms 547
Trojan Horses 547

Reconnaissance Attacks (16.2.2) 547

Access Attacks (16.2.3) 548

Password Attacks 548
Trust Exploitation 548
Port Redirection 549
Man-in-the-Middle 549

Denial of Service Attacks (16.2.4) 551

DoS Attack 551
DDoS Attack 551

Network Attack Mitigations (16.3) 552

The Defense-in-Depth Approach (16.3.1) 553

Keep Backups (16.3.2) 553

Upgrade, Update, and Patch (16.3.3) 554

Authentication, Authorization, and Accounting (16.3.4) 555

Firewalls (16.3.5) 555

Types of Firewalls (16.3.6) 557

Endpoint Security (16.3.7) 558

Device Security (16.4) 558

Cisco AutoSecure (16.4.1) 558

Passwords (16.4.2) 559

Additional Password Security (16.4.3) 560

Enable SSH (16.4.4) 561

Disable Unused Services (16.4.5) 563

Summary 565
Security Threats and Vulnerabilities 565
Network Attacks 565
Network Attack Mitigation 565
Device Security 566
Practice 567
Check Your Understanding Questions 567

Chapter 17 Build a Small Network 571
Objectives 571
Key Terms 571
Introduction (17.0) 572
Devices in a Small Network (17.1) 572
Small Network Topologies (17.1.1) 572
Device Selection for a Small Network (17.1.2) 573
Cost 573
Speed and Types of Ports/Interfaces 573
Expandability 573
Operating System Features and Services 574
IP Addressing for a Small Network (17.1.3) 574
Redundancy in a Small Network (17.1.4) 576
Traffic Management (17.1.5) 577
Small Network Applications and Protocols (17.2) 578
Common Applications (17.2.1) 578
Network Applications 578
Application Layer Services 579
Common Protocols (17.2.2) 579
Voice and Video Applications (17.2.3) 582
Scale to Larger Networks (17.3) 583
Small Network Growth (17.3.1) 583
Protocol Analysis (17.3.2) 583
Employee Network Utilization (17.3.3) 584
Verify Connectivity (17.4) 586
Verify Connectivity with Ping (17.4.1) 586
Extended Ping (17.4.2) 588
Verify Connectivity with Traceroute (17.4.3) 590

Extended Traceroute (17.4.4) 592
Network Baseline (17.4.5) 593

Host and IOS Commands (17.5) 596

IP Configuration on a Windows Host (17.5.1) 596
IP Configuration on a Linux Host (17.5.2) 599
IP Configuration on a macOS Host (17.5.3) 600
The arp Command (17.5.4) 601
Common show Commands Revisited (17.5.5) 602
The show cdp neighbors Command (17.5.6) 609
The show ip interface brief Command (17.5.7) 610
Verify Switch Interfaces 611

Troubleshooting Methodologies (17.6) 611

Basic Troubleshooting Approaches (17.6.1) 612
Resolve or Escalate? (17.6.2) 613
The debug Command (17.6.3) 613
The terminal monitor Command (17.6.4) 615

Troubleshooting Scenarios (17.7) 616

Duplex Operation and Mismatch Issues (17.7.1) 617
IP Addressing Issues on IOS Devices (17.7.2) 618
IP Addressing Issues on End Devices (17.7.3) 619
Default Gateway Issues (17.7.4) 619
Troubleshooting DNS Issues (17.7.5) 621

Summary (17.8) 624

Devices in a Small Network 624
Small Network Applications and Protocols 624
Scale to Larger Networks 624
Verify Connectivity 625
Host and IOS Commands 625
Troubleshooting Methodologies 626
Troubleshooting Scenarios 626

Practice 627

Check Your Understanding Questions 628

Appendix A Answers to "Check Your Understanding" Questions 631

Key Terms Glossary 645

Index 669

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

Introduction to Networks Companion Guide (CCNAv7) is the official supplemental textbook for the Cisco Network Academy CCNA Introduction to Networks Version 7 course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application and provides opportunities to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small business, medium-sized business as well as enterprise and service provider environments.

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

Topic Coverage

The following list gives you a thorough overview of the features provided in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the *Companion Guide* encourages you to think about finding the answers as you read the chapter.

- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Summary:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of chapter is a full list of all the labs, class activities, and Packet Tracer activities to refer to at study time.

Readability

The following features are provided to help you understand networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference to find the term used inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Key Terms Glossary defines all the key terms.
- **Key Terms Glossary:** This book contains an all-new Key Terms Glossary that defines more than 1000 terms.

Practice

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

- **Check Your Understanding questions and answer key:** Review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions in the online course. Appendix A, "Answers to 'Check Your Understanding' Questions," provides an answer key to all the questions and includes an explanation of each answer.

Interactive Graphic

- **Labs and activities:** Throughout each chapter, you are directed back to the online course to take advantage of the activities provided to reinforce concepts. In addition, at the end of each chapter is a "Practice" section that lists all the labs and activities to provide practice with the topics introduced in this chapter.

Video

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

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy CCNA IT Essential v7 course and is divided into 17 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "Networking Today":** This chapter introduces the concept of a network and provides an overview of the different types of networks encountered. It examines how networks impact the way we work, learn, and play. This chapter also examines recent trends in networks, such as video, cloud computing, and BYOD and how to help ensure robust, reliable, secure networks to support these trends.
- **Chapter 2, "Basic Switch and End Device Configuration":** This chapter introduces the operating system used with most Cisco devices: Cisco IOS. The basic purpose and functions of IOS are described, as are methods to access IOS. The chapter also describes how to maneuver through the IOS command-line interface as well as basic IOS device configuration.
- **Chapter 3, "Protocols and Models":** This chapter examines the importance of rules or protocols for network communication. It explores the OSI reference model and the TCP/IP communication suite and examines how these models provide the necessary protocols to allow communication to occur on a modern converged network.
- **Chapter 4, "Physical Layer":** This chapter introduces the lowest layer of the OSI model: the physical layer. This chapter explains the transmission of bits over the physical medium.
- **Chapter 5, "Number Systems":** This chapter explains how to convert between decimal, binary, and hexadecimal number systems. Understanding these number systems is essential to understanding IPv4, IPv6, and Ethernet MAC addressing.

- **Chapter 6, "Data Link Layer":** This chapter discusses how the data link layer prepares network layer packets for transmission, controls access to the physical media, and transports data across various media. This chapter includes a description of the encapsulation protocols and processes that occur as data travels across the LAN and the WAN.
- **Chapter 7, "Ethernet Switching":** This chapter examines the functionality of the Ethernet LAN protocols. It explores how Ethernet functions, including how devices use Ethernet MAC addresses to communicate in a multiaccess network. The chapter discusses how Ethernet switches build MAC address tables and forward Ethernet frames.
- **Chapter 8, "Network Layer":** This chapter introduces the function of the network layer—routing—and the basic device that performs this function—the router. It presents important routing concepts related to addressing, path determination, and data packets for both IPv4 and IPv6. The chapter also introduces how routers perform packet forwarding, static and dynamic routing, and the IP routing table.
- **Chapter 9, "Address Resolution":** This chapter discusses how host computers and other end devices determine the Ethernet MAC address for a known IPv4 or IPv6 address. This chapter examines the ARP protocol for IPv4 address resolution and the Neighbor Discovery Protocol for IPv6.
- **Chapter 10, "Basic Router Configuration":** This chapter explains how to configure a Cisco router, including IPv4 and IPv6 addressing on an interface.
- **Chapter 11, "IPv4 Addressing":** This chapter focuses on IPv4 network addressing, including the types of addresses and address assignment. It describes how to use subnet masks to determine the number of subnetworks and hosts in a network. It examines how to improve network performance by optimally dividing the IPv4 address space based on network requirements. It explores the calculation of valid host addresses and the determination of both subnet and broadcast addresses.
- **Chapter 12, "IPv6 Addressing":** This chapter focuses on IPv6 network addressing, including IPv6 address representation, types of addresses, and the structure of different types of IPv6 address. The chapter introduces the different methods that an end device can receive an IPv6 address automatically.
- **Chapter 13, "ICMP":** This chapter introduces Internet Control Message Protocol (ICMP) tools, such as **ping** and **trace**.

- **Chapter 14, "Transport Layer":** This chapter introduces Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) and examines how each of these protocols transports information across the network. It explores how TCP uses segmentation, the three-way handshake, and expectational acknowledg ments to ensure reliable delivery of data. It also examines the best-effort delivery mechanism provided by UDP and describes when its use would be preferred over the use of TCP.
- **Chapter 15, "Application Layer":** This chapter introduces some protocols of the TCP/IP application layer, which also relates to the top three layers of the OSI model. The chapter focuses on the role of the application layer and how the applications, services, and protocols in the application layer make robust communication across data networks possible. This will be demonstrated by examining some key protocols and services, including HTTP, HTTPS, DNS, DHCP, SMTP/POP, and FTP.
- **Chapter 16, "Network Security Fundamentals":** This chapter introduces network security threats and vulnerabilities. Various network attacks and mitigation techniques are discussed, along with how to secure network devices.
- **Chapter 17, "Build a Small Network":** This chapter reexamines the various components in a small network and describes how they work together to allow network growth. It examines network configuration and troubleshooting issues, along with different troubleshooting methodologies.
- **Appendix A, "Answers to 'Check Your Understanding' Questions":** This appendix lists the answers to the "Check Your Understanding" review questions that are included at the end of each chapter.
- **Key Terms Glossary:** The Key Terms Glossary provides definitions for all the key terms identified in each chapter.

Figure Credits

Figure 2-2, screen shot of Windows 10 GUI © Microsoft 2020

Figure 2-4, screen shot of PuTTY © 1997-2020 Simon Tatham

Figure 2-5, screen shot of Tera Term © 2004-2019 TeraTerm Project

Figure 2-6, screen shot of SecureCRT © 1995-2020 VanDyke Software, Inc.

Figure 2-9, screen shot of PuTTY startup screen © 1997-2020 Simon Tatham

Figure 2-10, screen shot of setting PuTTY to log a session to a text file © 1997-2020 Simon Tatham

Figure 2-11, screen shot of turn off session logging © 1997-2020 Simon Tatham

Figure 2-12, screen shot of configuring or verifying IPv4 addressing on a Windows host © Microsoft 2020

Figure 2-13, screen shot of configuring or verifying IPv6 addressing on a Windows host © Microsoft 2020

Figure 2-15, screen shot of accessing IPv4 properties on a Windows host © Microsoft 2020

Figure 2-16, screen shot of manually configuring IPv4 addressing on a Windows host © Microsoft 2020

Figure 2-17, screen shot of setting a Windows host to obtain IPv4 addressing automatically © Microsoft 2020

Figure 3-21A, © 2020 IEEE

Figure 3-21B, © Internet Engineering Task Force

Figure 3-21C, © Internet Assigned Numbers Authority

Figure 3-21D, © 2020 Internet Corporation for Assigned Names and Numbers

Figure 3-21E, © ITU 2020

Figure 3-21F, © Telecommunications Industry Association

Figure 3-22A, © 2020 Internet Society

Figure 3-22B, © Internet Engineering Task Force

Figure 3-22C, © Internet Engineering Task Force

Figure 3-22D, © Internet Research Task Force

Figure 11-2, screen shot of IPv4 addressing on a Windows PC © Microsoft 2020

Figure 11-13A, © 1997–2020, American Registry for Internet Numbers

Figure 11-13B, © 1992-2020 the Réseaux IP Européens Network Coordination Centre RIPE NCC

Figure 11-13C, © Latin America and Caribbean Network Information Centre

Figure 11-13D, © 2020 African Network Information Centre (AFRINIC)

Figure 11-13E, © 2020 APNIC

Figure 12-1A, © 1997–2020, American Registry for Internet Numbers

Figure 12-1B, © 1992-2020 the Réseaux IP Européens Network Coordination Centre RIPE NCC

Figure 12-1C, © Latin America and Caribbean Network Information Centre

Figure 12-1D, © 2020. All Rights Reserved - African Network Information Centre (AFRINIC)

Figure 12-1E, © 2020 APNIC

Figure 12-13, screen shot of Manually Configuring IPv6 Addressing on a Windows Host © Microsoft 2020

Figure 16-8, screen shot of Windows 10 Update © Microsoft 2020

Figure 17-6, screen shot of Windows Task Manager © Microsoft 2020

Figure 17-8, screen shot of Wireshark capture showing packet statistics © Microsoft 2020

Figure 17-9, screen shot of Windows 10 usage details for a Wi-Fi network connection © Microsoft 2020

Figure 17-17, screen shot of Windows 10 network connection details © Microsoft 2020

Figure 17-18, screen shot of Linux Ubuntu connection information © Canonical Ltd

Figure 17-19, screen shot of configuration information on a macOS host © Microsoft 2020

CHAPTER 7

Ethernet Switching

Objectives

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

- How are the Ethernet sublayers related to the frame fields?
- What is an Ethernet MAC address?
- How does a switch build its MAC address table and forward frames?
- What are the available switch forwarding methods and port settings on Layer 2 switch ports?

Key Terms

This chapter uses the following key terms. You can find the definitions in the glossary at the end of the book.

contention-based access method page 237

collision fragment page 238

runt frame page 238

jumbo frame page 238

baby giant frame page 238

cyclic redundancy check (CRC) page 239

organizationally unique identifier (OUI) page 242

burned-in address (BIA) page 243

Address Resolution Protocol (ARP) page 245

Neighbor Discovery (ND) page 245

MAC address table page 249

unknown unicast page 250

store-and-forward switching page 254

cut-through switching page 255

fast-forward switching page 256

fragment-free switching page 256

automatic medium-dependent interface crossover (auto-MDIX) page 259

Introduction (7.0)

If you are planning to become a network administrator or a network architect, you definitely need to know about Ethernet and Ethernet switching. The two most prominent LAN technologies in use today are Ethernet and WLANs. Ethernet supports bandwidths of up to 100 Gbps, which explains its popularity. This chapter contains a lab in which you will use Wireshark to look at Ethernet frames and another lab where you will view network device MAC addresses. There are also some instructional videos to help you better understand Ethernet. By the time you have finished this chapter, you will be able to create a switched network that uses Ethernet!

Ethernet Frames (7.1)

Ethernet operates in the data link layer and the physical layer. It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards.

Ethernet Encapsulation (7.1.1)

This chapter starts with a discussion of Ethernet technology, including an explanation of MAC sublayer and the Ethernet frame fields.

Two LAN technologies are used today: Ethernet and wireless LANs (WLANs). Ethernet uses wired communications, including twisted-pair, fiber-optic links, and coaxial cables.

Ethernet operates in the data link layer and the physical layer. It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards. Ethernet supports the following data bandwidths:

- 10 Mbps
- 100 Mbps
- 1000 Mbps (1 Gbps)
- 10,000 Mbps (10 Gbps)
- 40,000 Mbps (40 Gbps)
- 100,000 Mbps (100 Gbps)

As shown in Figure 7-1, Ethernet standards define both Layer 2 protocols and Layer 1 technologies.

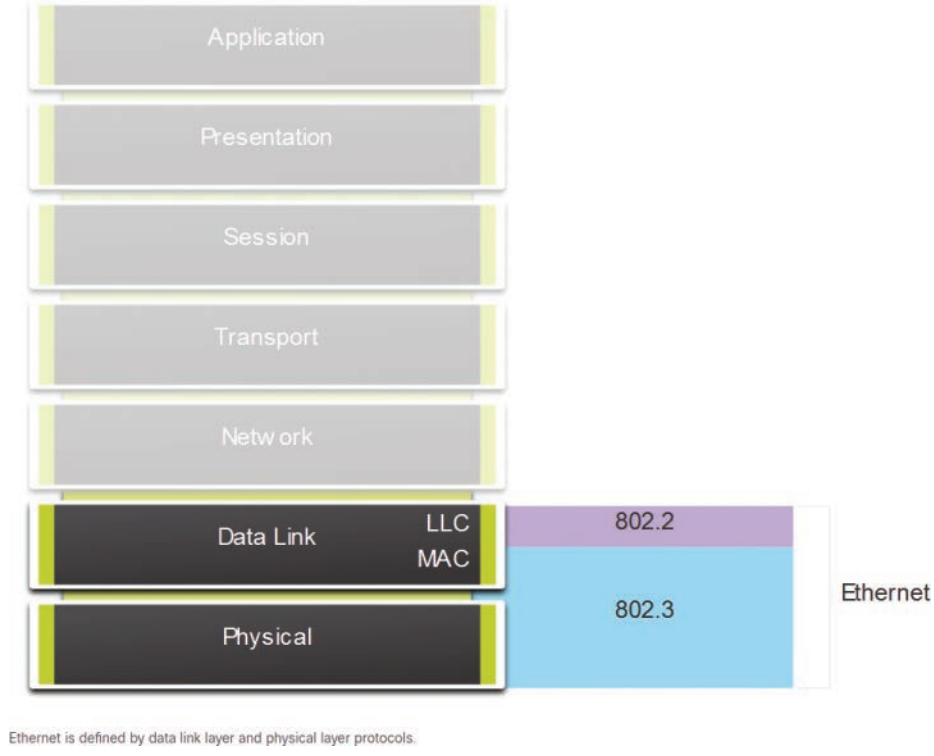


Figure 7-1 Ethernet in the OSI Model

Data Link Sublayers (7.1.2)

IEEE 802 LAN/MAN protocols, including Ethernet, use the two sublayers of the data link layer to operate: the Logical Link Control (LLC) and the Media Access Control (MAC) layers (see Figure 7-2).

Recall that the LLC and MAC sublayers have the following roles in the data link layer:

- **LLC sublayer:** This IEEE 802.2 sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers. It places information in the frame to identify which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to use the same network interface and media.
- **MAC sublayer:** This sublayer (specified in IEEE 802.3, 802.11, and 802.15), which is implemented in hardware, is responsible for data encapsulation and media access control. It provides data link layer addressing and is integrated with various physical layer technologies.

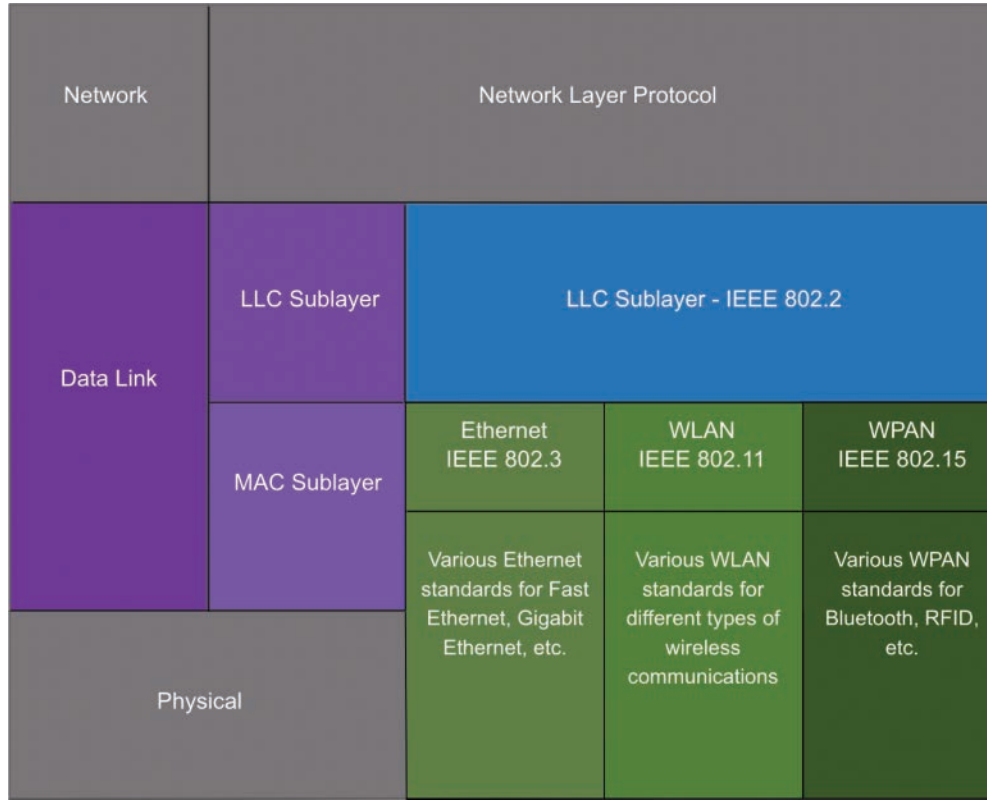


Figure 7-2 IEEE Ethernet Standards in the OSI Model

MAC Sublayer (7.1.3)

The MAC sublayer is responsible for data encapsulation and accessing the media.

Data Encapsulation

IEEE 802.3 data encapsulation includes the following:

- **Ethernet frame:** This is the internal structure of the Ethernet frame.
- **Ethernet addressing:** An Ethernet frame includes both source and destination MAC addresses to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
- **Ethernet error detection:** The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

Accessing the Media

As shown in Figure 7-3, the IEEE 802.3 MAC sublayer includes the specifications for different Ethernet communications standards over various types of media, including copper and fiber.

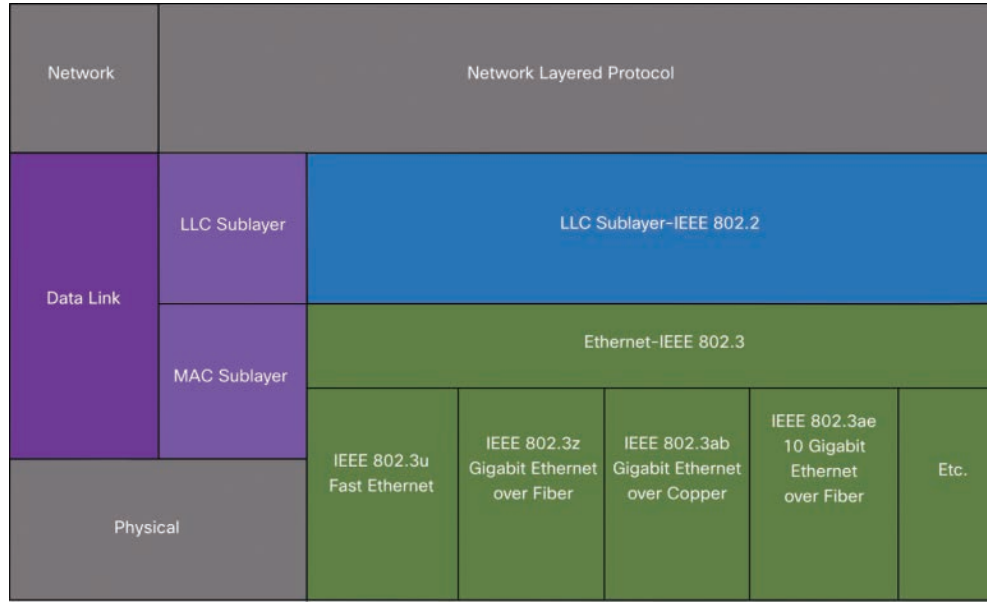


Figure 7-3 Details of the MAC Sublayer

Recall that legacy Ethernet using a bus topology or hubs is a shared, half-duplex medium. Ethernet over a half-duplex medium uses a *contention-based access method*, Carrier Sense Multiple Access/Collision Detect (CSMA/CD) to ensure that only one device is transmitting at a time. CSMA/CD allows multiple devices to share the same half-duplex medium and detects a collision when more than one device attempts to transmit simultaneously. It also provides a back-off algorithm for retransmission.

Ethernet LANs today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD.

Ethernet Frame Fields (7.1.4)

The minimum Ethernet frame size is 64 bytes, and the expected maximum is 1518 bytes. The frame size might be larger than that if additional requirements are included, such as VLAN tagging. (VLAN tagging is beyond the scope of this book.)

The frame includes all bytes from the destination MAC address field through the FCS field. The Preamble field is not included when describing the size of a frame.

Any frame less than 64 bytes in length is considered a *collision fragment* or *runt frame* and is automatically discarded by receiving stations. Frames with more than 1500 bytes of data are considered *jumbo frames* or *baby giant frames*.

If the size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device drops the frame. Dropped frames are likely to result from collisions or other unwanted signals. They are considered invalid. Jumbo frames are supported by most Fast Ethernet and Gigabit Ethernet switches and NICs.

Figure 7-4 shows the fields in the Ethernet frame.

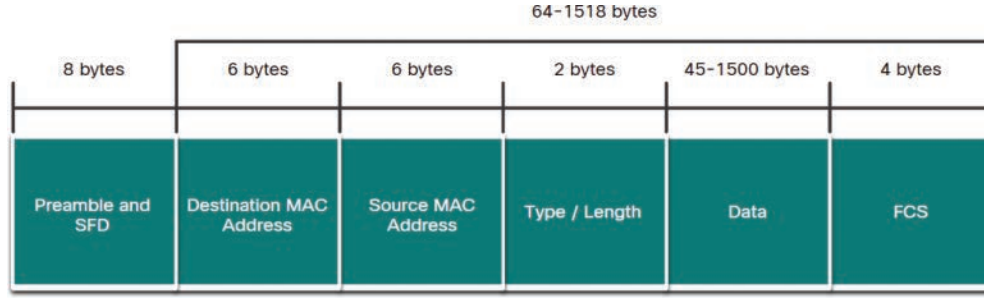


Figure 7-4 Ethernet Frame Structure and Field Size

Table 7-1 provides more information about the function of each field.

Table 7-1 Ethernet Frame Fields Detail

Field	Description
Preamble and Start Frame Delimiter fields	The preamble (7 bytes) and start frame delimiter (SFD), also called the start of frame (1 byte), fields are used for synchronization between the sending and receiving devices. These first 8 bytes of the frame are used to get the attention of the receiving nodes. Essentially, the first few bytes tell the receivers to get ready to receive a new frame.
Destination MAC Address field	This 6-byte field is the identifier for the intended recipient. Recall that Layer 2 uses this address to assist devices in determining if a frame is addressed to them. The address in a frame is compared to the MAC address in a device. If there is a match, the device accepts the frame. It can be a unicast, multicast, or broadcast address.
Source MAC Address field	This 6-byte field identifies the originating NIC or interface of the frame.

Field	Description
Type/Length field	This 2-byte field identifies the upper-layer protocol encapsulated in the Ethernet frame. Common values are, in hexadecimal, 0x800 for IPv4, 0x86DD for IPv6, and 0x806 for ARP. **Note:** You may also see this field referred to as EtherType, Type, or Length.
Data field	This field (which can range from 46 to 1500 bytes) contains the encapsulated data from a higher layer, which is a generic Layer 3 PDU or, more commonly, an IPv4 packet. All frames must be at least 64 bytes long. If a small packet is encapsulated, additional bits called a pad are used to increase the size of the frame to this minimum size.
Frame Check Sequence field	The frame check sequence (FCS) field (4 bytes) is used to detect errors in a frame. It uses a *cyclic redundancy check (CRC)*. The sending device includes the results of a CRC in the FCS field of the frame. The receiving device receives the frame and generates a CRC to look for errors. If the calculations match, no error occurred. Calculations that do not match indicate that the data has changed; in such a case, the frame is dropped. A change in the data could be the result of a disruption of the electrical signals that represent the bits.

Interactive Graphic

Check Your Understanding—Ethernet Switching (7.1.5)

Refer to the online course to complete this activity.

Lab—Use Wireshark to Examine Ethernet Frames (7.1.6)

In this lab, you will complete the following objectives:

- Part 1: Examine the Header Fields in an Ethernet II Frame
- Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

Ethernet MAC Address (7.2)

Ethernet technology relies on MAC addresses to function. MAC addresses are used to identify the frame source and destination.

MAC Address and Hexadecimal (7.2.1)

As discussed in detail in Chapter 5, "Number Systems," in networking, IPv4 addresses are represented using the decimal (base 10) number system and the binary (base 2) number system. IPv6 addresses and Ethernet addresses are represented using the hexadecimal (base 16) number system. To understand hexadecimal, you must first be very familiar with binary and decimal.

The hexadecimal numbering system uses the numbers 0 to 9 and the letters A to F.

An Ethernet MAC address consists of a 48-bit binary value. Hexadecimal is used to identify an Ethernet address because a single hexadecimal digit represents 4 binary bits. Therefore, a 48-bit Ethernet MAC address can be expressed using only 12 hexadecimal values.

Figure 7-5 compares the equivalent decimal and hexadecimal values for binary 0000 to 1111.

Figure 7-5 Decimal to Binary to Hexadecimal Conversion

Given that 8 bits (1 byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF, as shown in the Figure 7-6.

Decimal	Binary	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

Figure 7-6 Selected Examples of Decimal to Binary to Hexadecimal Conversions

When using hexadecimal, leading zeros are always displayed to complete the 8-bit representation. For example, in Figure 7-6, the binary value 0000 1010 is shown to be 0A in hexadecimal.

Hexadecimal numbers are often represented by a value preceded by 0x (for example, 0x73) to distinguish between decimal and hexadecimal values in documentation.

Hexadecimal may also be represented using a subscript 16 or by using the hex number followed by an H (for example, 73H).

You might have to convert between decimal and hexadecimal values. If such conversions are required, convert the decimal or hexadecimal value to binary and then to convert the binary value to either decimal or hexadecimal as appropriate. See Chapter 5 for more information.

Ethernet MAC Address (7.2.2)

In an Ethernet LAN, every network device is connected to the same shared medium. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. MAC addressing provides a method for device identification at the data link layer of the OSI model.

An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, as shown in Figure 7-7. Because 1 byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.

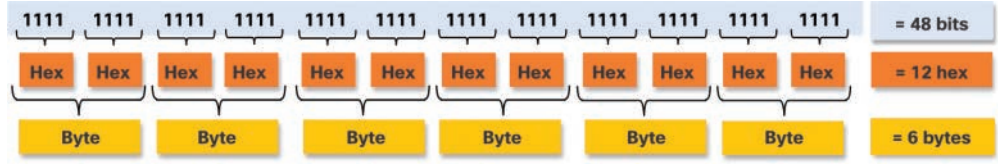


Figure 7-7 Ethernet MAC Address in Bits, Hextets, and Bytes

All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure uniqueness, every vendor that sells Ethernet devices must register with the IEEE to obtain a unique 6-digit hexadecimal (that is, 24-bit or 3-byte) code called an *organizationally unique identifier (OUI)*.

When a vendor assigns a MAC address to a device or to an Ethernet interface, the vendor must do as follows:

- Use its assigned OUI as the first 6 hexadecimal digits.
- Assign a unique value in the last 6 hexadecimal digits.

Therefore, an Ethernet MAC address consists of a 6-digit hexadecimal vendor OUI code followed by a 6-digit hexadecimal vendor-assigned value, as shown in Figure 7-8.

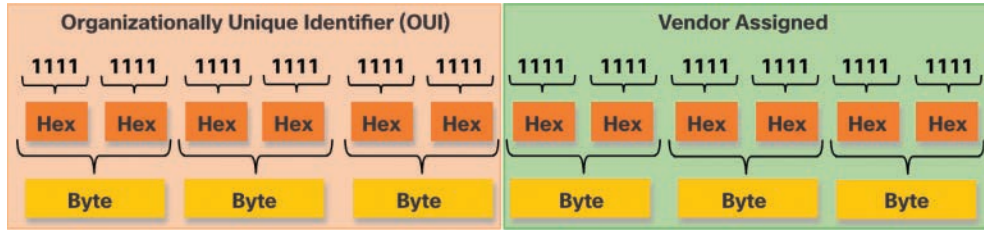


Figure 7-8 The Ethernet MAC Address Structure

For example, say that Cisco needs to assign a unique MAC address to a new device, and the IEEE has assigned Cisco the OUI 00-60-2F. Cisco would configure the device with a unique vendor code such as 3A-07-BC. Therefore, the Ethernet MAC address of that device would be 00-60-2F-3A-07-BC.

It is the responsibility of a vendor to ensure that no two of its devices are assigned the same MAC address. However, it is possible for duplicate MAC addresses to exist because of mistakes made during manufacturing, mistakes made in some virtual machine implementation methods, or modifications made using one of several

software tools. In such a case, it is necessary to modify the MAC address with a new NIC or make modifications by using software.

Frame Processing (7.2.3)

Sometimes a MAC address is referred to as a *burned-in address (BIA)* because the address is hard coded into read-only memory (ROM) on the NIC. This means that the address is permanently encoded into the ROM chip.

Note

With modern PC operating systems and NICs, it is possible to change the MAC address in software. This is useful when attempting to gain access to a network that filters based on BIA. Consequently, filtering or controlling traffic based on the MAC address is no longer as secure as it once was.

When the computer boots up, the NIC copies its MAC address from ROM into RAM. When a device is forwarding a message to an Ethernet network, as shown in Figure 7-9, the Ethernet header includes the following:

- **Source MAC address:** This is the MAC address of the source device NIC.
- **Destination MAC address:** This is the MAC address of the destination device NIC.

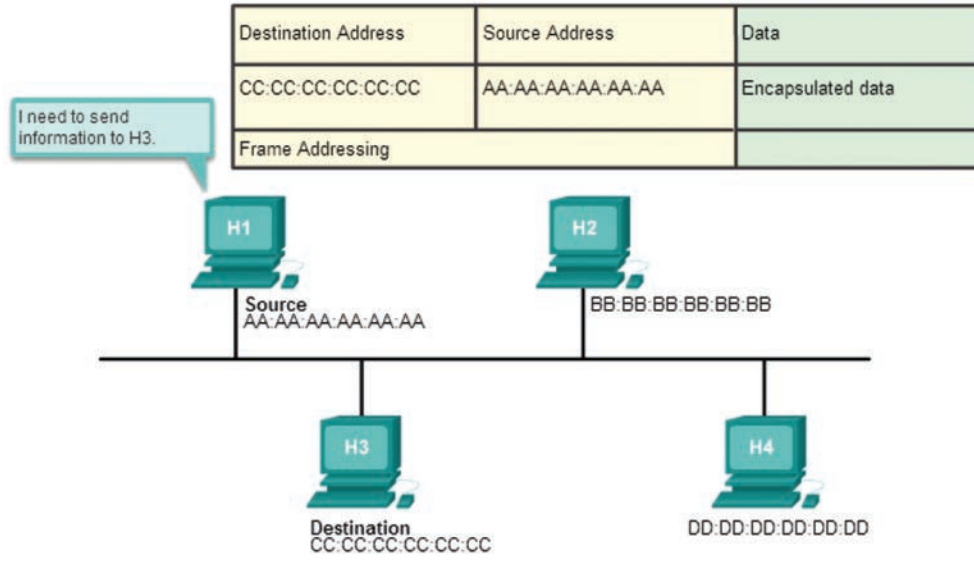


Figure 7-9 The Source Prepares a Frame to Send to the Destination

When a NIC receives an Ethernet frame, it examines the destination MAC address to see if it matches the physical MAC address that is stored in RAM. If there is no match, the device discards the frame. In Figure 7-10, H2 and H4 discard the frame. The MAC address matches for H4, so H4 passes the frame up the OSI layers, where the de-encapsulation process takes place.

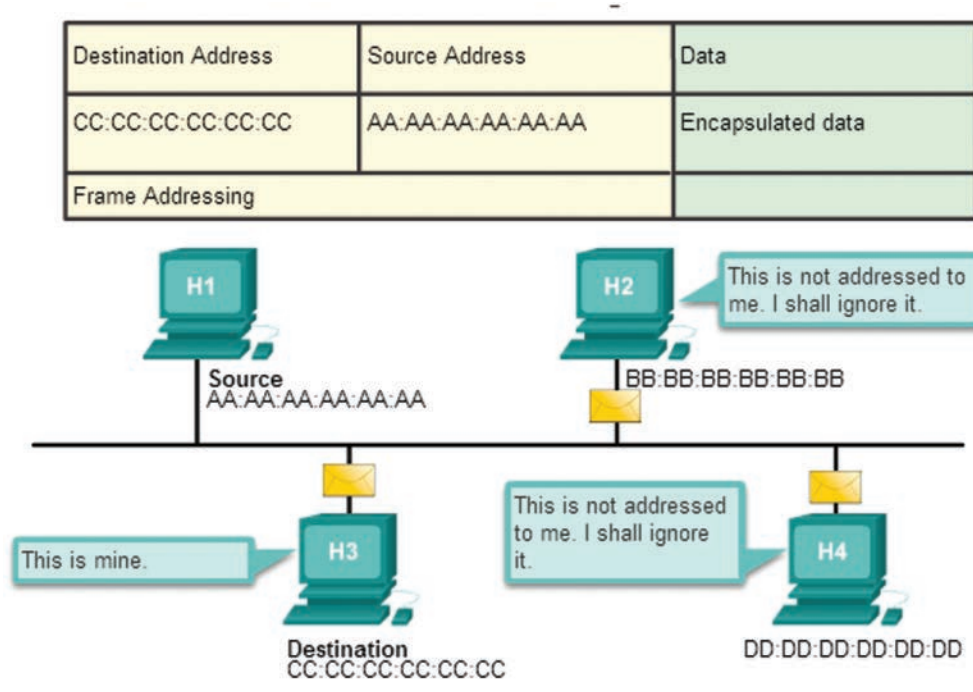


Figure 7-10 All Devices Receive the Frame, but Only the Destination Processes It

Note

Ethernet NICs also accept frames if the destination MAC address is a broadcast or a multicast group of which the host is a member.

Any device that is the source or destination of an Ethernet frame will have an Ethernet NIC and, therefore, a MAC address. This includes workstations, servers, printers, mobile devices, and routers.

Unicast MAC Address (7.2.4)

In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

A unicast MAC address is a unique address that is used when a frame is sent from a single transmitting device to a single destination device.

In Figure 7-11, the destination MAC address and the destination IP address are both unicast.

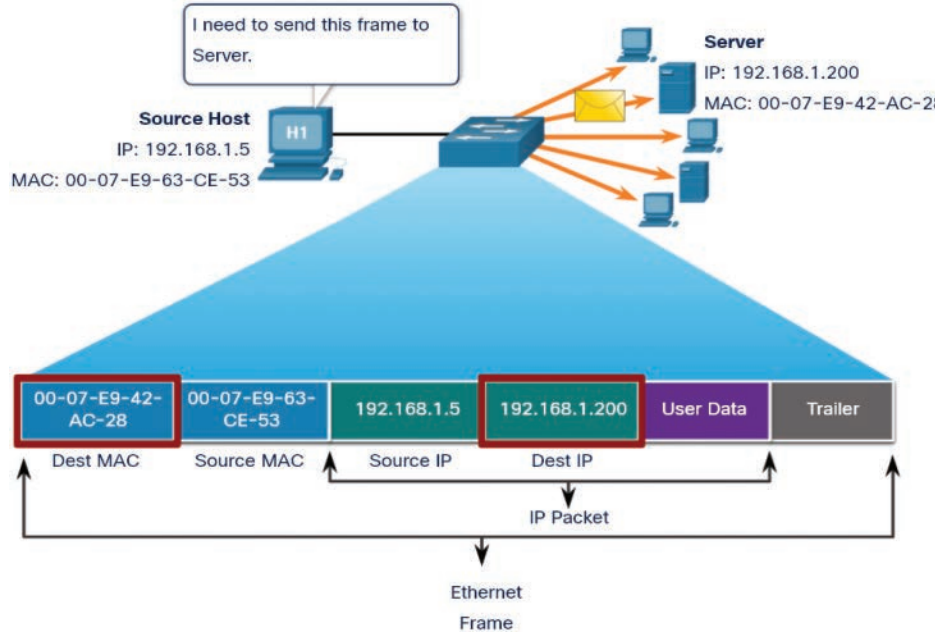


Figure 7-11 Unicast Frame Transmission

A host with IPv4 address 192.168.1.5 (source) requests a web page from the server at IPv4 unicast address 192.168.1.200. For a unicast packet to be sent and received, a destination IP address must be in the IP packet header. A corresponding destination MAC address must also be present in the Ethernet frame header. The IP address and MAC address combine to deliver data to one specific destination host.

The process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as *Address Resolution Protocol (ARP)*. The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as *Neighbor Discovery (ND)*.

Note

The source MAC address must always be a unicast address.

Broadcast MAC Address (7.2.5)

An Ethernet broadcast frame is received and processed by every device on an Ethernet LAN. The features of an Ethernet broadcast are as follows:

- It has the destination MAC address FF-FF-FF-FF-FF-FF in hexadecimal (or 48 1s in binary).
- It is flooded out all Ethernet switch ports except the incoming port.
- It is not forwarded by a router.

If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 address that has all 1s in the host portion. This numbering in the address means that all hosts on that local network (broadcast domain) receive and process the packet.

In Figure 7-12, the destination MAC address and destination IP address are both broadcast addresses.

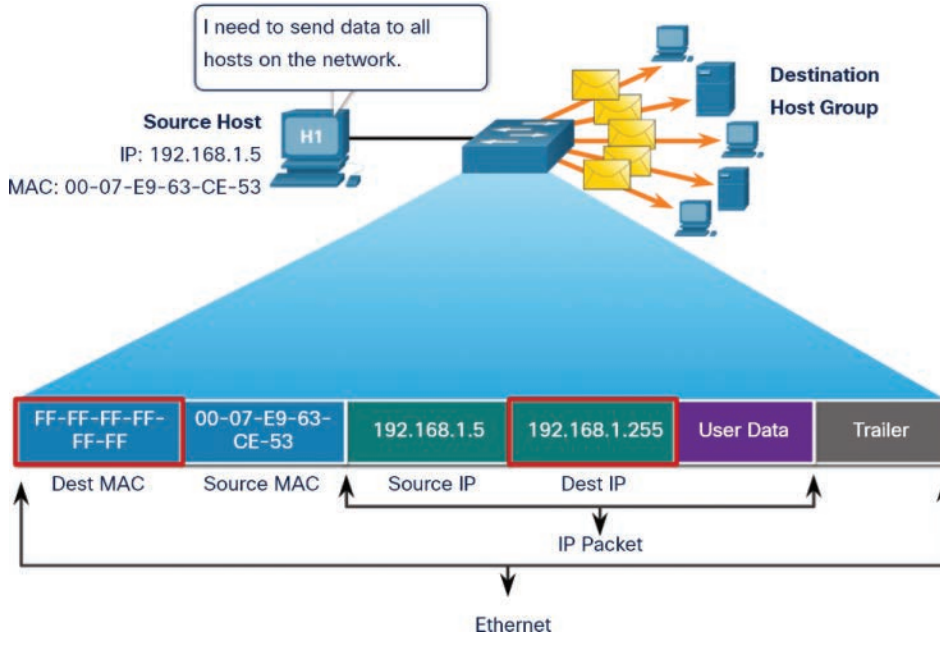


Figure 7-12 Broadcast Frame Transmission

The source host sends an IPv4 broadcast packet to all devices on its network. The IPv4 destination address is a broadcast address, 192.168.1.255. When the IPv4 broadcast packet is encapsulated in the Ethernet frame, the destination MAC address is the broadcast MAC address FF-FF-FF-FF-FF-FF in hexadecimal (or 48 1s in binary).

DHCP for IPv4 is an example of a protocol that uses Ethernet and IPv4 broadcast addresses. However, not all Ethernet broadcasts carry IPv4 broadcast packets. For example, ARP requests do not use IPv4, but the ARP message is sent as an Ethernet broadcast.

Multicast MAC Address (7.2.6)

An Ethernet multicast frame is received and processed by a group of devices on the Ethernet LAN that belong to the same multicast group. The features of an Ethernet multicast frame are as follows:

- It has destination MAC address 01-00-5E when the encapsulated data is an IPv4 multicast packet and destination MAC address 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (STP) and Link Layer Discovery Protocol (LLDP).
- It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping.
- It is not forwarded by a router unless the router is configured to route multicast packets.

If the encapsulated data is an IP multicast packet, the devices that belong to a multicast group are assigned a multicast group IP address. The range of IPv4 multicast addresses is 224.0.0.0 to 239.257.257.257. The range of IPv6 multicast addresses begins with ff00::/8. Because a multicast address represents a group of addresses (sometimes called a host group), it can only be used as the destination of a packet. The source is always a unicast address.

As with the unicast and broadcast addresses, a multicast IP address requires a corresponding multicast MAC address to deliver frames on a local network. The multicast MAC address is associated with, and uses addressing information from, the IPv4 or IPv6 multicast address.

In Figure 7-13, the destination MAC address and destination IP address are both multicast addresses.

Routing protocols and other network protocols use multicast addressing. Applications such as video and imaging software may also use multicast addressing, although multicast applications are not as common.

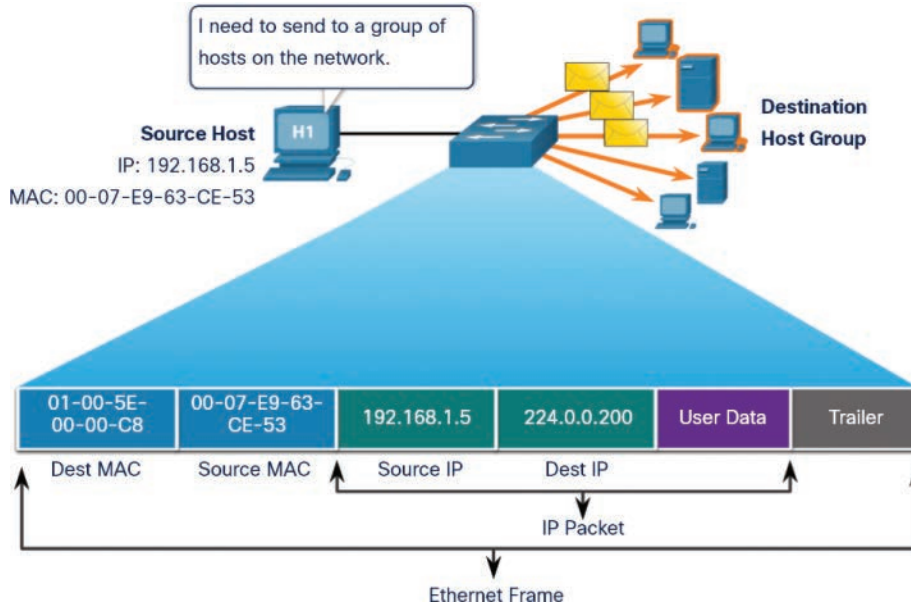


Figure 7-13 Multicast Frame Transmission

Lab—View Network Device MAC Addresses (7.2.7)

In this lab, you will complete the following objectives:

- Part 1: Set Up the Topology and Initialize Devices
- Part 2: Configure Devices and Verify Connectivity
- Part 3: Display, Describe, and Analyze Ethernet MAC Addresses

The MAC Address Table (7.3)

Compared to legacy Ethernet hubs, Ethernet switches improve efficiency and overall network performance. Although traditionally most LAN switches have operated at Layer 2 of the OSI model, an increasing number of Layer 3 switches are now being implemented. This section focuses on Layer 2 switches. Layer 3 switches are beyond the scope of this book.

Switch Fundamentals (7.3.1)

Now that you know all about Ethernet MAC addresses, it is time to talk about how a switch uses these addresses to forward (or discard) frames to other devices

on a network. If a switch just forwarded every frame it received out all ports, your network would be so congested that it would probably come to a complete halt.

A Layer 2 Ethernet switch uses Layer 2 MAC addresses to make forwarding decisions. It is completely unaware of the data (protocol) being carried in the data portion of the frame, such as an IPv4 packet, an ARP message, or an IPv6 ND packet. The switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses.

An Ethernet switch examines its *MAC address table* to make a forwarding decision for each frame. In contrast, a legacy Ethernet hub repeats bits out all ports except the incoming port. In Figure 7-14, the four-port switch was just powered on. The table shows the MAC address table, which has not yet learned the MAC addresses for the four attached PCs.

Note

MAC addresses are shortened throughout this section for demonstration purposes.

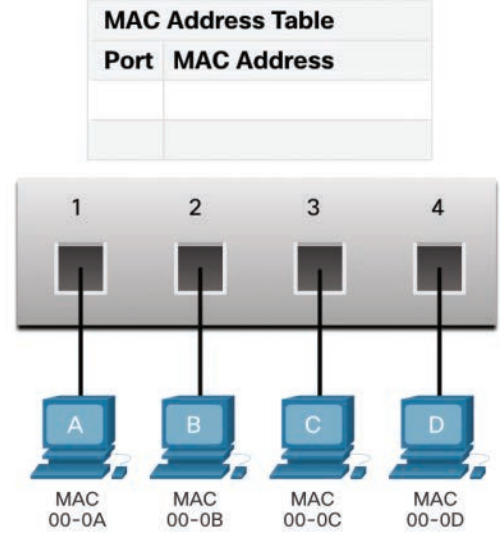


Figure 7-14 Switch Powers Up with an Empty MAC Address Table

Note

The MAC address table is sometimes referred to as a content-addressable memory (CAM) table. While the term CAM table is fairly common, for the purposes of this course, we refer to it as a MAC address table.

Switch Learning and Forwarding (7.3.2)

A switch dynamically builds its MAC address table by examining the source MAC addresses of the frames received on a port. The switch forwards frames by searching for a match between the destination MAC address in a frame and an entry in the MAC address table.

Examine the Source MAC Address

Every frame that enters a switch is checked for new information to learn. It does this by examining the source MAC address of the frame and the port number where the frame entered the switch. If the source MAC address does not exist, it is added to the table, along with the incoming port number. If the source MAC address does exist, the switch updates the refresh timer for that entry. By default, most Ethernet switches keep an entry in the table for 5 minutes.

In Figure 7-15, for example, PC-A is sending an Ethernet frame to PC-D. The table shows that the switch adds the MAC address for PC-A to the MAC address table.

Note

If the source MAC address exists in the table but on a different port, the switch treats this as a new entry. The entry is replaced using the same MAC address but with the more current port number.

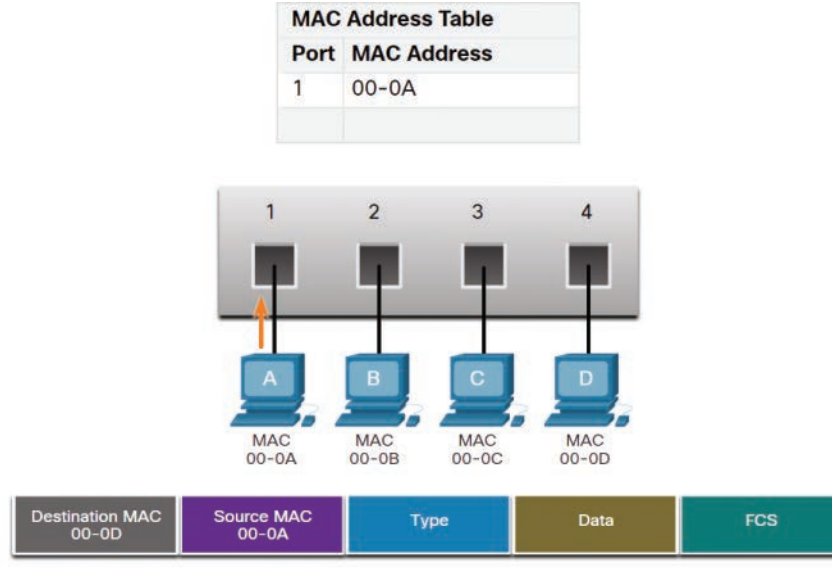
Find the Destination MAC Address

If the destination MAC address is a unicast address, the switch looks for a match between the destination MAC address of the frame and an entry in its MAC address table. If the destination MAC address is in the table, the switch forwards the frame out the specified port. If the destination MAC address is not in the table, the switch forwards the frame out all ports except the incoming port. This is called an ***unknown unicast***.

As shown in Figure 7-16, the switch does not have the destination MAC address in its table for PC-D, so it sends the frame out all ports except port 1.

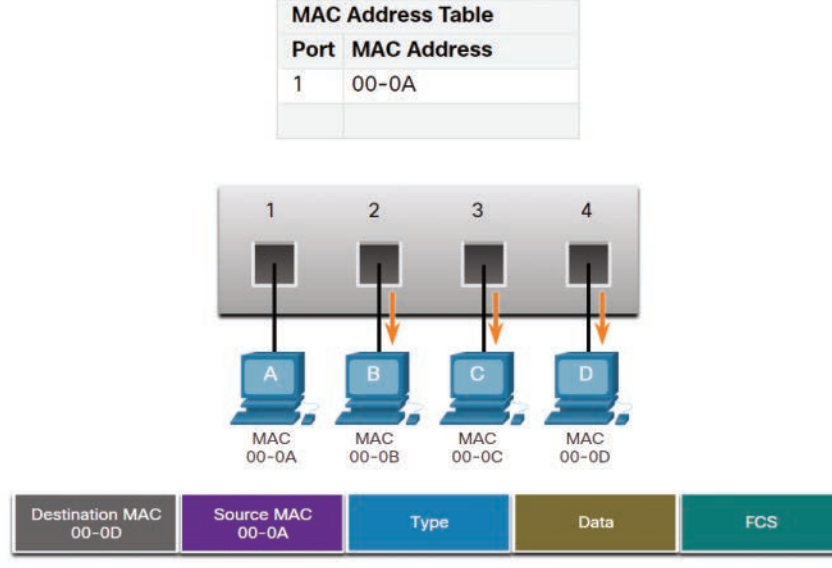
Note

If the destination MAC address is a broadcast or a multicast address, the frame is flooded out all ports except the incoming port.



1. PC-A sends an Ethernet frame.
2. The switch adds the port number and MAC address for PC-A to the MAC Address Table.

Figure 7-15 Switch Learns the MAC Address for PC-A



1. The destination MAC address is not in the table.
2. The switch forwards the frame out all other ports.

Figure 7-16 Switch Forwards the Frame Out All Other Ports

Filtering Frames (7.3.3)

As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, the switch is able to filter the frame and forward out a single port.

In Figure 7-17, PC-D is replying to PC-A. The switch sees the MAC address of PC-D in the incoming frame on port 4. The switch then puts the MAC address of PC-D into the MAC address table associated with port 4.

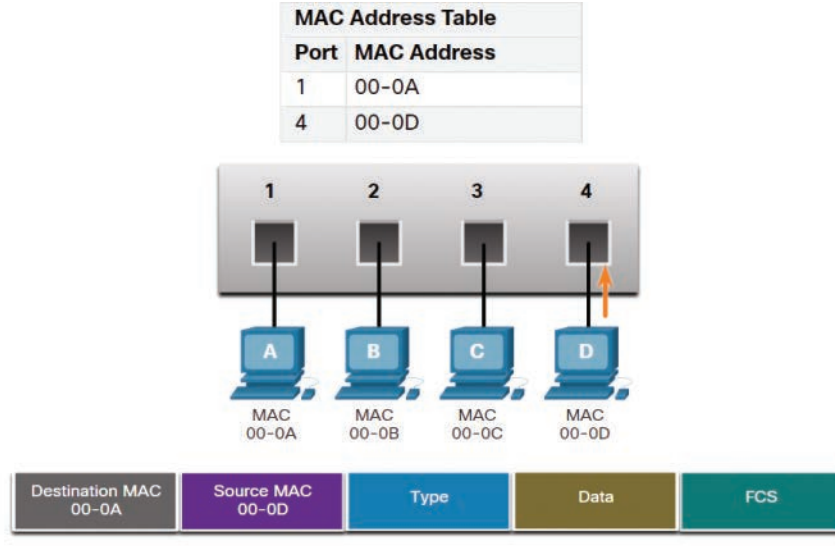


Figure 7-17 Switch Learns the MAC Address for PC-D

Next, because the switch has the destination MAC address for PC-A in the MAC address table, it sends the frame only out port 1, as shown in Figure 7-18.

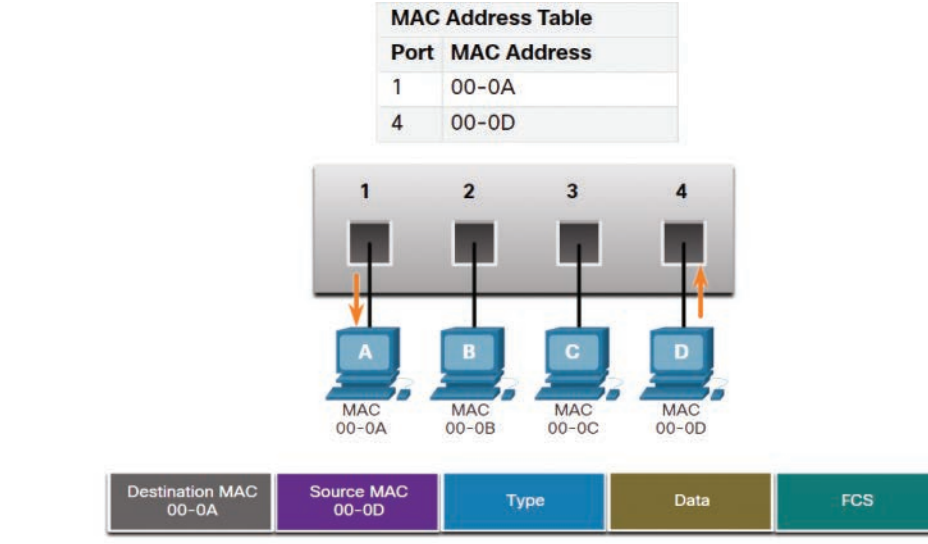
Next, PC-A sends another frame to PC-D, as shown in Figure 7-19. The MAC address table already contains the MAC address for PC-A; therefore, the 5-minute refresh timer for that entry is reset. Next, because the switch table contains the destination MAC address for PC-D, it sends the frame out only port 4.

Video

Video—MAC Address Tables on Connected Switches (7.3.4)

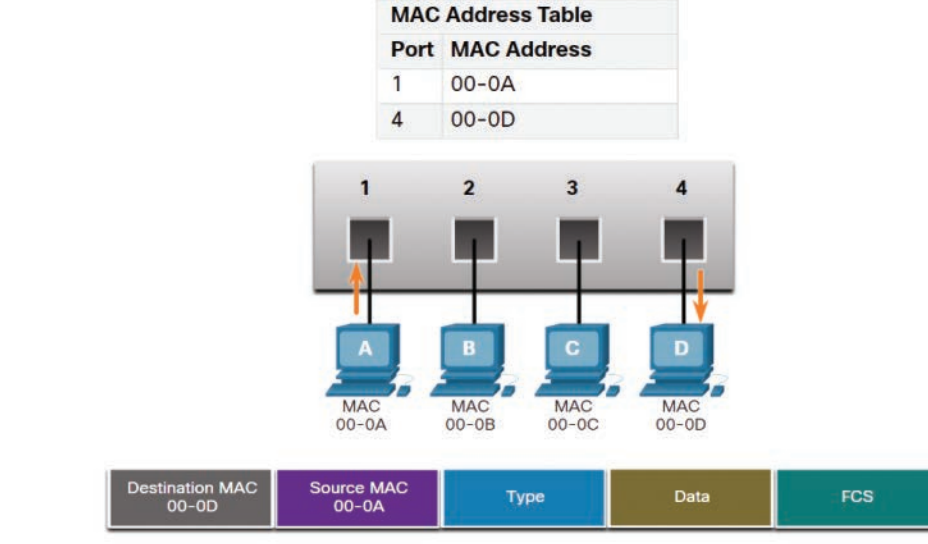
A switch can have multiple MAC addresses associated with a single port. This is common when the switch is connected to another switch. The switch will have a separate MAC address table entry for each frame received with a different source MAC address.

Refer to the online course to view this video.



1. The switch has a MAC address entry for the destination.
2. The switch filters the frame, sending it only out port 1.

Figure 7-18 Switch Forwards the Frame Out the Port Belonging to PC-A



1. The switch receives another frame from PC-A and refreshes the timer for the MAC address entry for port 1.
2. The switch has a recent entry for the destination MAC address and filters the frame, forwarding it only out port 4.

Figure 7-19 Switch Forwards the Frame Out the Port Belonging to PC-D

Video

Video—Sending the Frame to the Default Gateway (7.3.5)

When a device has an IP address that is on a remote network, the Ethernet frame cannot be sent directly to the destination device. Instead, the Ethernet frame is sent to the MAC address of the default gateway, the router.

Refer to the online course to view this video.

Interactive Graphic

Activity—Switch It! (7.3.6)

Use this activity to check your understanding of how a switch learns and forwards frames.

Refer to the online course to complete this activity.

Lab—View the Switch MAC Address Table (7.3.7)

In this lab, you will complete the following objectives:

- Part 1: Build and Configure the Network
- Part 2: Examine the Switch MAC Address Table

Switch Speeds and Forwarding Methods (7.4)

Switches may have the capability to implement various forwarding methods to increase performance in a network.

Frame Forwarding Methods on Cisco Switches (7.4.1)

As you learned in the previous section, a switch uses its MAC address table to determine which port to use to forward frames. With Cisco switches, there are actually two frame forwarding methods, and there are good reasons to use one instead of the other, depending on the situation.

Switches use one of the following forwarding methods for switching data between network ports:

- *Store-and-forward switching*: With this frame forwarding method, the switch receives the entire frame and computes the CRC. The switch uses a mathematical formula, based on the number of bits (1s) in the frame, to determine whether the received frame has an error. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. Then the frame is forwarded out the correct port.

- *Cut-through switching*: With this frame forwarding method, the switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

A big advantage of store-and-forward switching is that the switch determines whether a frame has errors before propagating the frame. When an error is detected in a frame, the switch discards the frame. Discarding frames with errors reduces the amount of bandwidth consumed by corrupt data. Store-and-forward switching is required for quality of service (QoS) analysis on converged networks where frame classification for traffic prioritization is necessary. For example, voice over IP (VoIP) data streams need to have priority over web-browsing traffic.

Figure 7-20 shows the store-and-forward process.

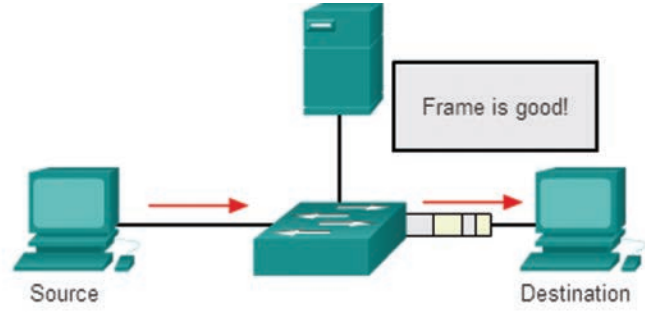


Figure 7-20 Store-and-Forward Switching

Cut-Through Switching (7.4.2)

In cut-through switching, the switch acts on the data as soon as it is received, even if the transmission is not complete. The switch buffers just enough of the frame to read the destination MAC address so that it can determine which port to use to forward the data. The destination MAC address is located in the first 6 bytes of the frame, following the preamble. The switch looks up the destination MAC address in its switching table, determines the outgoing interface port, and forwards the frame on to its destination through the designated switch port. The switch does not perform any error checking on the frame.

Figure 7-21 shows the cut-through switching process.

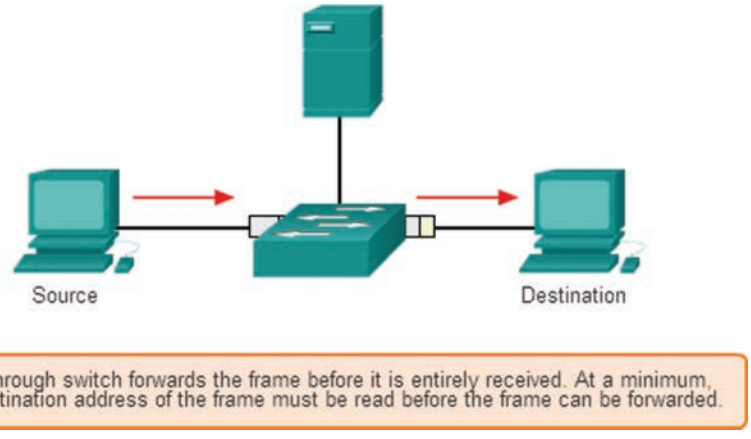


Figure 7-21 Cut-Through Switching

There are two variants of cut-through switching:

- *Fast-forward switching*: Fast-forward switching offers the lowest level of latency. With fast-forward switching, the switch immediately forwards a packet after reading the destination address. Because with fast-forward switching the switch starts forwarding before the entire packet has been received, there may be times when packets are relayed with errors. This occurs infrequently, and the destination NIC discards the faulty packet upon receipt. In fast-forward mode, latency is measured from the first bit received to the first bit transmitted. Fast-forward switching is the typical cut-through method of switching.
- *Fragment-free switching*: In fragment-free switching, the switch stores the first 64 bytes of the frame before forwarding. Fragment-free switching can be viewed as a compromise between store-and-forward switching and fast-forward switching. The reason the switch stores only the first 64 bytes of the frame is that most network errors and collisions occur during the first 64 bytes. Fragment-free switching tries to enhance fast-forward switching by performing a small error check on the first 64 bytes of the frame to ensure that a collision has not occurred before forwarding the frame. Fragment-free switching is a compromise between the high latency and high integrity of store-and-forward switching and the low latency and reduced integrity of fast-forward switching.

Some switches are configured to perform cut-through switching on a per-port basis until a user-defined error threshold is reached, and then they automatically change to store-and-forward. When the error rate falls below the threshold, the port automatically changes back to cut-through switching.

Memory Buffering on Switches (7.4.3)

An Ethernet switch may use a buffering technique to store frames before forwarding them. Buffering may also be used when the destination port is busy due to congestion. The switch stores the frame until it can be transmitted.

As shown in Table 7-2, there are two methods of memory buffering.

Table 7-2 Memory Buffering Methods

Method	Description
Port-based memory buffering	Frames are stored in queues that are linked to specific incoming and outgoing ports.
	A frame is transmitted to the outgoing port only when all the frames ahead in the queue have been successfully transmitted.
	It is possible for a single frame to delay the transmission of all the frames in memory because a destination port is busy. This delay occurs even if the other frames could be transmitted to open destination ports.
Shared memory buffering	All frames are deposited into a common memory buffer shared by all switch ports, and the amount of buffer memory required by a port is dynamically allocated.
	The frames in the buffer are dynamically linked to the destination port, enabling a packet to be received on one port and then transmitted on another port, without moving it to a different queue.

Shared memory buffering results in the ability to store larger frames with potentially fewer dropped frames. This is important with asymmetric switching, which allows for different data rates on different ports, such as when connecting a server to a 10 Gbps switch port and PCs to 1 Gbps ports.

Duplex and Speed Settings (7.4.4)

Two of the most basic settings on a switch are the bandwidth (sometimes referred to as *speed*) and duplex settings for each individual switch port. It is critical that the duplex and bandwidth settings match between the switch port and the connected devices, such as computers or other switches.

Two types of duplex settings are used for communications on an Ethernet network:

- **Full-duplex:** Both ends of the connection can send and receive simultaneously.
- **Half-duplex:** Only one end of the connection can send at a time.

Autonegotiation is an optional function on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities. Full-duplex is chosen if both devices have the capability, along with their highest common bandwidth.

In Figure 7-22, the Ethernet NIC for PC-A can operate in full-duplex or half-duplex and at 10 Mbps or 100 Mbps. PC-A is connected to switch S1 on port 1, which can operate in full-duplex or half-duplex and at 10 Mbps, 100 Mbps, or 1000 Mbps (1 Gbps). If both devices are using autonegotiation, the operating mode is full-duplex, at 100 Mbps.

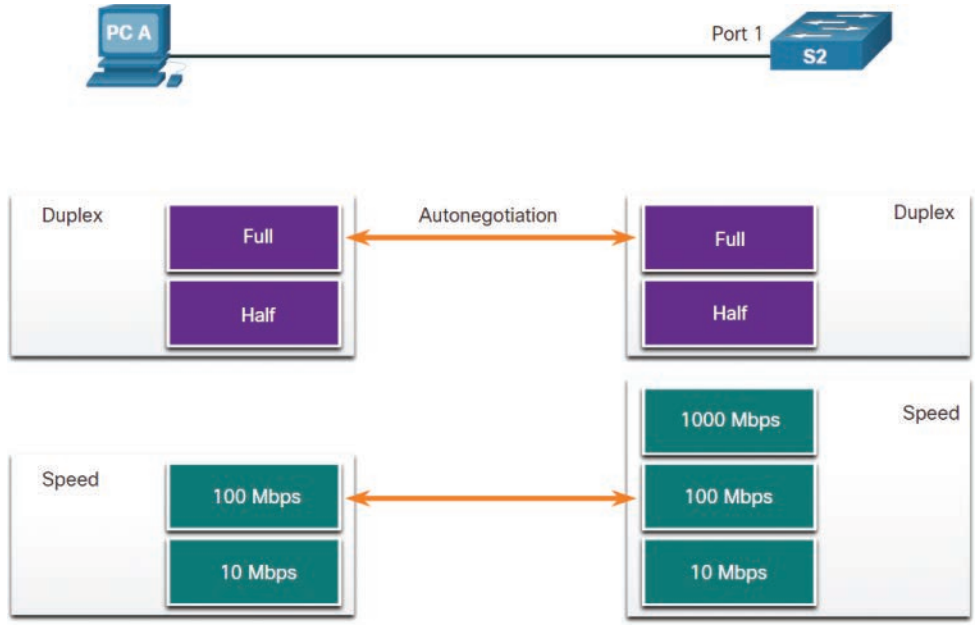


Figure 7-22 Duplex and Speed Settings

Note

Most Cisco switches and Ethernet NICs default to autonegotiation for speed and duplexing. Gigabit Ethernet ports operate only in full-duplex.

Duplex mismatch is one of the most common causes of performance issues on 10/100 Mbps Ethernet links. It occurs when one port on the link operates at half-duplex while the other port operates at full-duplex, as shown in Figure 7-23. In this scenario, S2 will continually experience collisions because S1 keeps sending frames any time it has something to send.

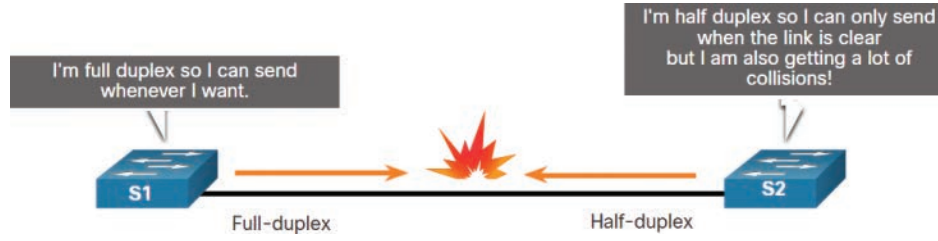


Figure 7-23 Duplex Mismatch

Duplex mismatch occurs when one or both ports on a link are reset, and the autonegotiation process does not result in the two link partners having the same configuration. It also can occur when users reconfigure one side of a link and forget to reconfigure the other. Both sides of a link should have autonegotiation on, or both sides should have it off. Best practice is to configure both Ethernet switch ports as full-duplex.

Auto-MDIX (7.4.5)

At one time, connections between devices required the use of either a crossover cable or a straight-through cable. The type of cable required depended on the type of interconnecting devices. For example, Figure 7-24 identifies the correct cable types required to interconnect a switch to a switch, a switch to a router, a switch to a host, or a router to a host. A crossover cable is used for connecting like devices, and a straight-through cable is used for connecting unlike devices.

Note

A direct connection between a router and a host requires a crossover connection.

Most switch devices now support the *automatic medium-dependent interface crossover (auto-MDIX)* feature. When this feature is enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly. Therefore, you can use either a crossover cable or a straight-through cable for connections to a copper 10/100/1000 port on a switch, regardless of the type of device on the other end of the connection.

The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. However, the feature can be disabled. For this reason, you should always use the correct cable type and should not rely on the auto-MDIX feature. Auto-MDIX can be re-enabled using the **mdix auto** interface configuration command.

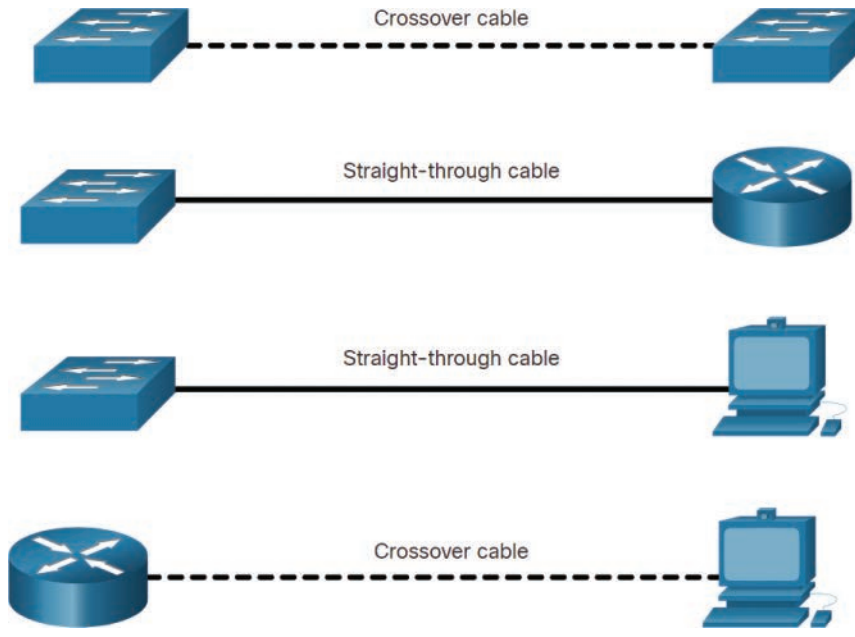


Figure 7-24 Cable Types

Interactive Graphic

Check Your Understanding—Switch Speeds and Forwarding Methods (7.4.6)

Refer to the online course to complete this activity.

Summary (7.5)

The following is a summary of the topics in the chapter and their corresponding online modules.

Ethernet Frame

Ethernet operates at the data link layer and the physical layer. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies. Ethernet operates at the LLC and MAC sublayers of the data link layer. Data encapsulation includes the following: Ethernet frame, Ethernet addressing, and Ethernet error detection. Ethernet LANs use switches that operate in full-duplex. The Ethernet frame fields are Preamble and Start Frame Delimiter, Destination MAC Address, Source MAC Address, EtherType, Data, and FCS.

Ethernet MAC Address

The binary number system uses the digits 0 and 1. Decimal uses 0 through 9. Hexadecimal uses 0 through 9 and the letters A through F. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. MAC addressing provides a method for device identification at the data link layer of the OSI model. An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, or 6 bytes. An Ethernet MAC address consists of a 6-digit hexadecimal vendor OUI code followed by a 6-digit hexadecimal vendor-assigned value. When a device is forwarding a message to an Ethernet network, the Ethernet header includes the source and destination MAC addresses. In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

The MAC Address Table

A Layer 2 Ethernet switch makes forwarding decisions based solely on Layer 2 Ethernet MAC addresses. The switch dynamically builds its MAC address table by examining the source MAC addresses of the frames received on a port. The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table. As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of each frame. When the MAC address table of the switch contains the destination MAC address, the switch is able to filter the frame and forward it out a single port.

Switch Speeds and Forwarding Methods

Switches use one of two forwarding methods for switching data between network ports: store-and-forward switching or cut-through switching. Two variants of cut-through switching are fast-forward and fragment-free switching. Two methods of memory buffering are port-based memory buffering and shared memory buffering. Two types of duplex settings are used for communications on an Ethernet network: full-duplex and half-duplex. Autonegotiation is an optional function on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities. Full-duplex is chosen if both devices have the capability, and their highest common bandwidth is chosen. Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When this feature is enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly.

Practice

The following activities provide practice with the topics introduced in this chapter. The lab is available in the companion *Introduction to Networks Labs & Study Guide (CCNAv7)* (ISBN 9780136634454). The Packet Tracer activity instructions are also provided in the *Labs & Study Guide*. The PKA files are available in the online course.

Labs

Lab 7.1.6: Use Wireshark to Examine Ethernet Frames

Lab 7.2.7: View Network Device MAC Addresses

Lab 7.3.7: View the Switch MAC Address Table

Check Your Understanding Questions

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

1. Which network device makes forwarding decisions based only on the destination MAC address that is contained in a frame?

   a. repeater
   b. hub
   c. Layer 2 switch
   d. router

2. For which network device is the primary function to send data to a specific destination based on the information found in the MAC address table?

   a. hub
   b. router
   c. Layer 2 switch
   d. modem

3. What does the LLC sublayer do?

   a. It performs data encapsulation.
   b. It communicates with upper protocol layers.
   c. It is responsible for media access control.
   d. It adds a header and trailer to a packet to form an OSI Layer 2 PDU.

4. Which statement is true about MAC addresses?

   a. MAC addresses are implemented by software.
   b. A NIC needs a MAC address only if it is connected to a WAN.
   c. The first 3 bytes are used by the vendor-assigned OUI.
   d. The ISO is responsible for MAC address regulations.

5. What happens to a runt frame received by a Cisco Ethernet switch?

   a. The frame is dropped.
   b. The frame is returned to the originating network device.
   c. The frame is broadcast to all other devices on the same network.
   d. The frame is sent to the default gateway.

6. What are the minimum and maximum sizes of an Ethernet frame? (Choose two.)

   a. 56 bytes
   b. 64 bytes
   c. 128 bytes
   d. 1024 bytes
   e. 1518 bytes

7. What addressing information does a switch record in order to build its MAC address table?

   a. the destination Layer 3 addresses of incoming packets
   b. the destination Layer 2 addresses of outgoing frames
   c. the source Layer 3 addresses of outgoing frames
   d. the source Layer 2 addresses of incoming frames

8. Which two characteristics describe Ethernet technology? (Choose two.)

   a. It is supported by IEEE 802.3 standards.
   b. It is supported by IEEE 802.5 standards.
   c. It typically uses an average of 16 Mbps for data transfer.
   d. It uses unique MAC addresses to ensure that data is sent to and processed by the appropriate destination.
   e. It uses a ring topology.

9. What statement describes MAC addresses?

   a. They are globally unique.
   b. They are routable only within the private network.
   c. They are added as part of a Layer 3 PDU.
   d. They have 32-bit binary values.

10. What is the special value assigned to the first 24 bits of a multicast MAC address?

    a. 01-5E-00
    b. FF-00-5E
    c. FF-FF-FF
    d. 01-00-5E

11. What will a host on an Ethernet network do if it receives a frame with a destination MAC address that does not match its own MAC address?

    a. It will discard the frame.
    b. It will forward the frame to the next host.
    c. It will remove the frame from the media.
    d. It will strip off the data link frame to check the destination IP address.

12. What is auto-MDIX?

    a. a type of Cisco switch
    b. an Ethernet connector type
    c. a feature that automatically determines speed and duplex
    d. a feature that detects Ethernet cable type

13. Which two functions or operations are performed by the MAC sublayer? (Choose two.)

    a. It is responsible for media access control.
    b. It performs the function for NIC driver software.
    c. It adds a header and trailer to form an OSI Layer 2 PDU.
    d. It handles communication between upper and lower layers.
    e. It adds control information to the network protocol header.

14. What type of address is 01-00-5E-0A-00-02?

    a. an address that reaches every host inside a local subnet
    b. an address that reaches one specific host
    c. an address that reaches every host in the network
    d. an address that reaches a specific group of hosts

This page intentionally left blank

Index

Symbols

* (asterisk), 453
: (colon), 404–405
/8 networks, subnetting, 372–373, 391
10BASE-T, 143
/16 networks, subnetting, 367–370, 391
100BASE-TX, 143

A

A records, 524
AAA (authentication, authorization, and accounting), 555
AAA (authentication, authorization, and accounting) x, 645
AAAA records, 524
access, IOS. *See* Cisco IOS
access attacks, 548–549
  brute-force, 646
  definition of, 645
  DoS (denial-of-service), 551–552
  man-in-the-middle attack, 549
  password attacks, 548
  port redirection, 549
  trust exploitation, 548–549
access control, 35, 216–217
access control lists (ACLs), 35
access methods, definition of, 645
access points (APs), 138, 166, 645
access technologies, 17–20, 92
  businesses, 19–20
  small office and home offices, 17–19
  summary of, 38
ACK (Acknowledgement), 472, 484–486, 488
ACK (Acknowledgment), 645
Acknowledgment (ACK), 645
ACLs (access control lists), 35
address conservation, IPv4, 381–383
address resolution, IPv6 ND (Neighbor Discovery), 311
Address Resolution Protocol. *See* ARP (Address Resolution Protocol)
addresses
  ARP (Address Resolution Protocol)
    broadcasts, 307–309
    definition of, 301–302
    examining with Packet Tracer, 309
    maps, 303
    overview of, 302–304
    replies, 305
    requests, 304
    role in remote communications, 305–306
    spoofing, 307–309
    summary of, 313
    tables, 306–307
  data link, 124, 125, 126–129
  devices on same network, 123
  IP. *See* IP (Internet Protocol) addresses
  Layer 2, 223–225
  Layer 3 logical, 122–123
  MAC (media access control), 239–248
    address structure, 241–243
    address table, 248–254
    broadcast, 246–247
    destinations on remote network, 299–301
    destinations on same network, 298–299
    frame processing, 243–244
    hexadecimal number system, 240–241
    multicast, 247–248
    summary of, 313
    unicast, 244–245
  types of, 121
adjacency tables, 645
ADVERTISE messages, 529
adware, 33
AfriNIC (African Network Information Centre), 358
alternating current, 645

American National Standards Institute (ANSI), 141, 209
American Registry for Internet Numbers (ARIN), 358
American Standard Code for Information Interchange (ASCII), 645
analog telephones, 645
AND, logical, 345–346
ANSI (American National Standards Institute), 141, 209
Anti-Spam Research Group (ASRG), 109
antispyware, 34
antivirus software, 34
anycast, 406, 436–437
APIPA (Automatic Private IP Addressing), 357, 619
APNIC (Asia Pacific Network Information Centre), 358
AppleTalk, 99
application filtering, 557
application layer. *See also* specific protocols
client-server model, 511–512
definition of, 113, 114, 508
email protocols, 518–521
IMAP (Internet Message Access Protocol), 521
POP (Post Office Protocol), 520
SMTP (Simple Mail Transfer Protocol), 519–520
summary of, 534
file sharing services, 530–533
FTP (File Transfer Protocol), 530
SMB (Server Message Block), 531–533
summary of, 535–536
functions of, 508
IP addressing services, 521–530
DHCP (Dynamic Host Configuration Protocol), 527–529
DNS (Domain Name System), 522–525
nslookup command, 526–527
summary of, 535
overview of, 101–102, 508–511
peer-to-peer applications, 513–515
peer-to-peer networks, 512–513, 534
services in, 579
summary of, 534
web protocols, 515–518
HTML (Hypertext Markup Language), 515–517
HTTP (Hypertext Transfer Protocol), 516–518
HTTPS (HTTP Secure), 516–518
summary of, 534
applications
peer-to-peer, 513–515
small business networks
common applications, 578–579
voice/video applications, 582
summary of, 624
APs (access points), 138, 166, 645
architecture, network, 23
fault tolerance, 24
QoS (quality of service), 25–26
scalability, 24–25
security design, 26–27
ARCNET, 217
ARIN (American Registry for Internet Numbers), 358
ARP (Address Resolution Protocol), 103, 245, 360
broadcasts, 307–309
definition of, 103, 245, 301–302, 360, 645
examining with Packet Tracer, 309
maps, 303
overview of, 302–304
replies, 305
requests, 304
role in remote communications, 305–306
spoofing, 307–309
summary of, 313
tables
displaying, 306–307
removing entries from, 306–307
arp -a command, 307
arp command, 601–602
ASCII (American Standard Code for Information Interchange), 645
Asia Pacific Network Information Centre (APNIC), 358
ASRG (Anti-Spam Research Group), 109
assigned multicast, 646
asterisk (*), 453
asymmetric switching, 646
ATM (Asynchronous Transfer Mode), 225
attacks, 546–552
access, 548–549
brute-force, 646
DoS (denial-of-service), 551–552

man-in-the-middle attack, 549
password attacks, 548
port redirection, 549
trust exploitation, 548–549
malware, 546–547
Trojan horses, 33, 547, 665
viruses, 546
worms, 547, 668
mitigation of, 552–558
AAA (authentication, authorization, and accounting), 555
backups, 553–554
defense-in-depth approach, 553
endpoint security, 558
firewalls, 555–557
summary of, 565
updates and patches, 554
reconnaissance, 547–548, 660
summary of, 565
attenuation, signal, 147
.au domain, 525
authentication, authorization, and accounting (AAA), 555, 645
auto secure command, 558–559
automatic medium-dependent interface crossover (auto-MDIX), 259–260, 646
Automatic Private IP Addressing (APIPA), 357, 619
auto-MDIX, 259–260, 646
AutoSecure, 558–559
availability, data, 27, 646

B

baby giant frames, 238, 646
backups, 553–554
bandwidth, 234
definition of, 646
goodput, 146, 653
latency, 146
throughput, 146, 665
units of, 145
banner messages, 65–66
banner motd command, 65–66, 321, 322
best-effort delivery, 272, 468, 646. ***See also*** **UDP (User Datagram Protocol)**
BGP (Border Gateway Protocol), 103
BIA (burned-in address), 243, 647
binary number systems, 176–194
binary game, 193
binary positional notation, 178–180
binary to decimal conversion, 180–181
decimal to binary conversion
binary positional value tables, 182–186
example of, 186–193
IPv4 addresses, 176–178, 193–194
summary of, 198
binary positional notation, 178–180
binary positional value tables, 182–186
BitTorrent, 514
blocking IPv4 addresses, 356
Bluetooth, 166, 169–170, 646
BOOTP (Bootstrap Protocol), 510, 646
Bootstrap Protocol (BOOTP), 646
Border Gateway Protocol (BGP), 103
bring your own device (BYOD), 28, 646
broadcast addresses, 349, 646
broadcast domains, segmentation and, 359–362
broadcast MAC (media access control) addresses, 246–247
broadcast transmission, 93
ARP (Address Resolution Protocol), 307–309
definition of, 646
IPv4, 350–352, 390
brute-force attacks, 548, 560, 646
buffered memory, 257, 647
burned-in address (BIA), 243, 647
bus topology, 214, 647
businesses. ***See*** **small business network management**
BYOD (bring your own device), 28, 646

C

cable internet connections, 18, 647
cable testers, 647
cabling, copper, 7, 146–152, 168–169
characteristics of, 147–148
coaxial cable, 151–152
fiber-optic cabling versus, 163–164
rollover cables, 157
STP (shielded twisted pair), 150–151, 662

UTP (unshielded twisted pair), 152–158
connectors, 153–156
crossover, 157
definition of, 148–150
properties of, 152–153
standards, 153–156
straight-through, 157
T568A/T68B standards, 157–158
cabling, fiber-optic, 158–164
copper cabling versus, 163–164
definition of, 652
fiber patch cords, 162–163
fiber-optic connectors, 161–162
industry applications of, 160
multimode fiber, 160
properties of, 158–159
single-mode fiber, 159
summary of, 169
CAM (content addressable memory) table, 649
Canadian Standards Association (CSA), 141
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), 165–166, 216, 219–220, 647
Carrier Sense Multiple Access/Collision Detect (CSMA/CD), 216, 217–219, 647
categories, UTP cabling, 154
CCNA (Cisco Certified Network Associate) certification, 35–36
CDP (Cisco Discovery Protocol), 609–610
CEF (Cisco Express Forwarding), 647
cellular internet, 18–19, 647
CENELEC (European Committee for Electrotechnical Standardization), 141
certifications, CCNA (Cisco Certified Network Associate), 35–36
CFRG (Crypto Forum Research Group), 109
channels, 87, 647
Checksum field
TCP headers, 472
UDP headers, 474
circuit switched systems, 647
Cisco AutoSecure, 558–559
Cisco Certified Network Associate (CCNA) certification, 35–36
Cisco Discovery Protocol (CDP), 609–610
Cisco Express Forwarding (CEF), 647
Cisco IOS
access, 46–52
access methods, 49–50
GUIs (graphical user interfaces), 47–48
operating systems, 46–47
OSs (operating systems), 48–49
summary of, 79
terminal emulation programs, 50–52
commands, 56–60
basic structure of, 56
hot keys and shortcuts for, 58–60
summary of, 79
syntax of, 57–58
definition of, 648
device configuration, 61–66
banner messages, 65–66
capturing to text file, 68–71
configuration files, 67–68
device names, 61–62, 321
with Packet Tracer, 71
password configuration, 63–64
password encryption, 64–65
password guidelines, 62–63
running configuration, altering, 68
small business network management, 573–574, 624
summary of, 79–80
with Syntax Checker, 66
help, 58
interfaces, 73–74
IP (Internet Protocol) addresses, 618
automatic configuration for end devices, 76–77
manual configuration for end devices, 75–76
structure of, 71–73
summary of, 80
switch virtual interface configuration, 77–78
verification of, 77
navigation, 52–56
configuration mode, 53–54
moving between modes, 54–55
Packet Tracer, 60
primary command modes, 52–53
subconfiguration mode, 53–54
summary of, 79
Syntax Checker, 55–56
Tera Term, 60

ports, 73–74
verifying connectivity of, 78, 80
Cisco Packet Tracer. ***See*** **Packet Tracer**
Cisco routers. ***See*** **router configuration**
Cisco Webex Teams, 29
Class A addresses, 357
Class B addresses, 357
Class C addresses, 357
Class D addresses, 357
Class E addresses, 357
classful addressing, legacy, 357–358, 648
clients
definition of, 4, 648
multicast, 352
UDP (User Datagram Protocol), 495–498
client-server model, 511–512
clock command, 60
cloud computing
definition of, 648
impact on daily life, 4
types of, 29–30
CnC (command-and-control) programs, 551
.co domain, 525
coaxial cable, 151–152, 648
collaboration, 28–29, 648
collision fragments, 238
colon (:), 404–405
.com domain, 525
command modes, Cisco IOS
configuration mode, 53–54
moving between modes, 54–55
primary command modes, 52–53
subconfiguration mode, 53–54
Syntax Checker, 55–56
command syntax check, 58
command-and-control (CnC) programs, 551
command-line interface (CLI). ***See*** **specific commands**
communications, network. ***See*** **network communications**
communities, definition of, 648
community cloud, 30
confidentiality, 27, 648
configuration. ***See also*** **verification**
Cisco IOS devices, 61–66. *See also* IP (Internet Protocol) addresses
banner messages, 65–66
capturing to text file, 68–71
configuration files, 67–68
device names, 61–62, 321
with Packet Tracer, 71, 336
password encryption, 64–65
password guidelines, 62–64
passwords, 62–65
running configuration, altering, 68
small business network management, 573–574, 624
summary of, 79–80
with Syntax Checker, 66
verifying connectivity of, 78, 80
default gateways, 330–334
on host, 331–332
router connections, 334
on switch, 332–334
with Syntax Checker, 334
default route propagation, 335–336
GUAs (global unicast addresses)
dynamic addressing, 417–425
static, 413–416
IP (Internet Protocol) addresses
automatic configuration for end devices, 76–77
IPv6, 427–430
manual configuration for end devices, 75–76
switch virtual interface configuration, 77–78
IPv4 subnets
/8 networks, 372–373, 391
/16 networks, 367–370, 391
corporate example of, 378–380
DMZ (demilitarized zone), 377
efficiency of, 377–380
maximizing subnets, 377–378
on an octet boundary, 364–366
within an octet boundary, 366–367
with Packet Tracer, 367, 381
private versus public address space, 374–377
summary of, 391–392
unused host IPv4 addresses, minimizing, 377–378
VLSM (variable-length subnet masking), 381–387
IPv6 subnets, 432–435
example of, 433–434

router configuration, 435
subnet allocation, 433–434
subnet IDs, 432–433
LLAs (link-local addresses)
dynamic addressing, 425–430
static, 413–416
password security, 559–561
passwords, 63–64
router interfaces, 323–330
basic configuration, 323–324
dual stack addressing, 324–325
summary of, 335
verification commands, 325–330
routers, 336–337
ARP tables, displaying, 306–307
basic configuration example, 321–323
basic configuration steps, 320–321, 335
default gateways, 330–334
dynamic LLAs (link-local addresses) on, 426–427
host/router communications, 223–225
interfaces, 323–330
switch and router network build, 336–337
SSH (Secure Shell), 561–562
vulnerabilities, 544
configuration mode, 53–54
configure command, 58
configure terminal command, 54, 62, 321, 324
congestion, definition of, 649
congestion avoidance, 493
connected switches, MAC (media access control) address tables on, 252
connectionless, definition of, 649
connectionless IP (Internet Protocol), 271–272
connection-oriented protocols, 468, 649. ***See also*** **TCP (Transmission Control Protocol)**
connectivity, verification of, 586–596
Cisco IOS devices, 78, 80
network baselines, 593–596
ping command, 586–590
summary of, 624
traceroute command, 590–594
tracert command, 590–593
connectors
fiber-optic, 161–162
UTP (unshielded twisted pair) cable, 153–156
console, 49, 649
content addressable memory (CAM) table, 649
contention-based access, 217–220
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), 216, 219–220
CSMA/CD (Carrier Sense Multiple Access/Collision Detect), 216, 217–219
definition of, 649
contention-based access method, 237
context-sensitive help, 58
Control Bits field (TCP headers), 472
controlled access, 217
converged networks, 20–21, 649
copper cabling, 7, 146–152
characteristics of, 147–148
coaxial cable, 151–152, 648
fiber-optic cabling versus, 163–164
rollover cables, 157
STP (shielded twisted pair), 150–151, 662
summary of, 168–169
UTP (unshielded twisted pair), 152–158
connectors, 153–156
crossover, 157
definition of, 148–150
properties of, 152–153
standards, 153–156
straight-through, 157
summary of, 169
T568A/T68B standards, 157–158
copy running-config startup-config command, 68, 322
core, optical fiber, 649
CRC (cyclic redundancy check), 222–223, 239, 649
crossover UTP cables, 157
crosstalk, 147, 649
Crypto Forum Research Group (CFRG), 109
crypto key generate rsa general-keys modulus command, 561, 562
CSA (Canadian Standards Association), 141
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), 165–166, 216, 219–220, 647
CSMA/CD (Carrier Sense Multiple Access/Collision Detect), 216, 217–219, 647
custom cloud, 649
cut-through switching, 255–256, 649
cyclic redundancy check (CRC), 222–223, 239, 649

D

DAD (duplicate address detection), 424, 448
daemons, 650
data access, 121–129
data link layer addresses, 124, 125, 126–129
devices on same network, 123
Layer 3 logical addresses, 122–123
overview of, 121
summary of, 132
data availability, 27, 646
data centers, 650
data confidentiality, 27
data encapsulation, 116–121
de-encapsulation, 120–121, 132
example of, 120
IP (Internet Protocol), 270–271
MAC (media access control) sublayer, 236
message segmenting, 116–117
PDUs (protocol data units), 118–120, 132
sequencing, 96, 118–119
summary of, 132
Data field (Ethernet frames), 239
data flow, 6
data integrity, 27, 654
data interception and theft, 33
data link frame, 221–226
frame fields, 222–223
LAN frames, 225–226
Layer 2 addresses, 223–225
overview of, 221
WAN frames, 225–226
data link layer
addresses, 124, 125, 126–129
data link frame, 221–226
frame fields, 222–223
LAN frames, 225–226
Layer 2 addresses, 223–225
overview of, 221
summary of, 229
WAN frames, 225–226
definition of, 114
IEEE 802 LAN/MAN sublayers, 206–207
media access in, 207–208
purpose of, 204–206, 228
standards, 209
topologies, 209–220
access control methods, 216–217
contention-based access, 216–220
controlled access, 217
full-duplex communication, 215–216, 653
half-duplex communication, 215, 653
LAN (local area network), 213–214
physical/logical, 209–211
summary of, 228
WAN (wide area network), 211–213
data link sublayers, 235
data loss, 486–487, 542
data networks, definition of, 650
Data Usage tool, 585
datagrams, 118, 463, 468, 494, 650
debug command, 613–615, 616
debug ip icmp command, 615
debug ip packet command, 615
decapsulation. ***See*** **de-encapsulation**
decimal numbers
binary to decimal conversion, 180–181
decimal positional notation, 178–179
decimal to binary conversion
binary positional value tables, 182–186
example of, 186–193
decimal to hexadecimal conversion, 196
hexadecimal to decimal conversion, 196–197
decoding messages, 89
de-encapsulation, 120–121, 132, 650
default gateways
configuration, 330–334
on host, 331–332
router connections, 334
summary of, 335–336
on switch, 332–334
with Syntax Checker, 334
definition of, 282
host routing to, 282–283
pinging, 450–451
sending frames to, 254
troubleshooting, 334, 619–620
default routes, 650
defense-in-depth approach, 553
delimiting, frame, 207
delivery of messages, 92–93
Deluge, 514

demilitarized zone. ***See*** **DMZ (demilitarized zone)**
denial-of-service (DoS) attacks, 33, 543, 650
description command, 57, 323–324
design, IPv4 structure, 387–389, 392
device address assignment, 389
IPv4 network address planning, 388
with Packet Tracer, 389, 392–393
Destination IPv4 Address field, 276
destination IPv4 addresses, 122, 123, 125, 299
Destination IPv6 Address field, 280
Destination MAC Address field, 238
destination MAC addresses, 124, 126, 243, 299, 301, 305
Destination Port field
TCP headers, 472
UDP headers, 474
destination port numbers, 650
Destination Unreachable messages, 445–446
destinations, definition of, 87
device address assignment, 389
device configuration, 61–66. ***See also*** **IP (Internet Protocol) addresses**
banner messages, 65–66
capturing to text file, 68–71
configuration files, 67–68
device names, 61–62, 321
with Packet Tracer, 71, 336
passwords
configuration, 63–64
encryption, 64–65
guidelines for, 62–63
running configuration, altering, 68
small business network management, 573–574, 624
summary of, 79–80
with Syntax Checker, 66
verifying connectivity of, 78, 80
device identifiers, 422
device security
Cisco AutoSecure, 558–559
passwords, 559–561
SSH (Secure Shell), 561–562
summary of, 566
unused services, disabling, 563–564
DHCP (Dynamic Host Configuration Protocol)
definition of, 101, 651
DHCPv6, 529, 663
dynamic addressing in, 527
IP address configuration with, 75, 360
lease periods, 527–528
operation of, 528–529
overview of, 527–529
pools, 527
port numbers, 479
servers, 581
SLAAC (stateless address autoconfiguration)
stateful DHCPv6, 420–421
and stateless DHCPv6, 419–420
DHCPACK messages, 529
DHCPDISCOVER messages, 528–529
DHCPNAK messages, 529
DHCPOFFER messages, 528–529
DHCPREQUEST messages, 529
diagrams, topology, 8–11
definition of, 10
logical, 10–11
network symbols for, 8–10
physical, 10
dialup internet access, 19
dial-up telephone, 650
DiffServ (DS) field (IPv4), 275
digital cameras, 650
digital subscriber line (DSL), 9, 18
Direct Connect, 514
directed broadcast transmission, 351–352, 651
directly connected networks, 651
disable command, 54
disabling services, 563–564
disruption of service, 543
DMZ (demilitarized zone)
definition of, 651
example of, 354–355
subnetting, 377
DNS (Domain Name System)
definition of, 101, 651
hierarchy, 525
message formats in, 524–525
nslookup command, 526–527, 530
overview of, 510, 522–525
port numbers, 479
servers, 76, 581
troubleshooting, 621–623

domains
broadcast, 359–362
top-level, 525
DoS (denial-of-service) attacks, 33, 543, 551–552, 650
dotted decimal notation
binary to decimal conversion, 180–181
decimal positional notation, 178–179
decimal to binary conversion
binary positional value tables, 182–186
example of, 186–193
decimal to hexadecimal conversion, 196
hexadecimal to decimal conversion, 196–197
double colon (::), 404–405
downloads, 512
DS (DiffServe) field (IPv4), 275
DSL (digital subscriber line), 9, 18, 650
dual stack addressing, 324–325, 399–400, 651
duplex multimode LC (Lucent Connector) connectors, 162, 651
duplex operation
definition of, 651
settings for, 257–259
troubleshooting, 617
duplicate address detection (DAD), 424, 448
dynamic addressing, 527
for GUAs (global unicast addresses), 417–425, 437
EUI-64 process, 422–424
randomly generated interface IDs, 424–425
RS and RA messages, 417–418
SLAAC and stateless DHCPv6, 419–420
stateful DHCPv6, 420–421
for LLAs (link-local addresses), 425–430, 437–438
dynamic LLA creation, 425
dynamic LLA on Cisco routers, 426–427
dynamic LLA on Windows, 425–426
IPv6 address configuration, verification of, 427–430
with Packet Tracer, 430
Dynamic Host Configuration Protocol. *See* DHCP (Dynamic Host Configuration Protocol)
dynamic routing, 288–290
dynamic routing protocols, 651. *See also* specific protocols

E

Echo Reply messages, 444–445
Echo Request messages, 444–445
eDonkey, 514
EHs (extension headers), 280
EIA (Electronic Industries Alliance), 111
EIGRP (Enhanced Interior Gateway Routing Protocol), 103
electrical threats, 545
electromagnetic interference (EMI), 147, 651
Electronic Industries Alliance (EIA), 111
electronic standards, 111
email protocols, 518–521
IMAP (Internet Message Access Protocol), 521
POP (Post Office Protocol), 520
SMTP (Simple Mail Transfer Protocol), 519–520
summary of, 534
email servers, 5, 581
EMI (electromagnetic interference), 147, 651
employee network utilization, 584–586
enable command, 54
enable passwords, 651
enable secret, 64, 320, 322, 651
encapsulation, 116–121
de-encapsulation, 120–121, 132
definition of, 651
Ethernet frames, 234–235
example of, 120
IP (Internet Protocol), 270–271
MAC (media access control) sublayer, 236
message segmenting, 116–117
messages, 90–91
PDUs (protocol data units), 118–120, 132
sequencing, 96, 118–119
summary of, 132
encoding, 88–89, 142–143, 651
encryption, password, 64–65
end command, 55
end devices. *See* hosts
endpoint security, 558
Enhanced Interior Gateway Routing Protocol (EIGRP), 103
enterprise networks, 160
environmental threats, 545
erase startup-config command, 68

error detection, 96, 207, 222–223
escalation, 613
EtherChannel, 651
Ethernet, 254–255
bandwidths, 234
crossover, 157
definition of, 103, 652
encoding, 143
frames, 234–239
baby giant frames, 238, 646
data link sublayers, 235
encapsulation, 234–235
fields in, 237–239
filtering, 252–253
forwarding methods, 254–255, 262
jumbo frames, 238, 655
MAC sublayer, 236–237
runt frames, 238, 661
sending to default gateway, 254
summary of, 261
Gigabit, 323
hubs, 7
MAC (media access control) addresses, 239–248
address structure, 241–243
address table, 248–254, 261
broadcast, 246–247
frame processing, 243–244
hexadecimal number system, 240–241
multicast, 247–248
summary of, 261
unicast, 244–245
Metro Ethernet, 18, 20
straight-through, 157
switches
Auto-MDIX, 259–260
cut-through switching, 255–256, 649
duplex settings, 257–259
fast-forward switching, 256, 652
fragment-free switching, 256, 652–653
frame filtering, 252–253
frame forwarding methods on, 254–255
learning and forwarding, 248–249
memory buffering on, 257
overview of, 248–249
speed settings, 257–259, 262
store-and-forward switching, 254–255, 664
ETSI (European Telecommunications Standards Institute), 141
EUI-64 process, 422–424, 652
EUIs (Extended Unique Identifiers), 422–424
European Committee for Electrotechnical Standardization, 141
European Telecommunications Standards Institute (ETSI), 141
EXEC mode, 53, 666
exec-timeout command, 561
Exit and Logout command (Packet Tracer), 22
exit command, 54–55
expandability, small business networks, 573
expectational acknowledgement, 488, 652
Extended Unique Identifiers (EUIs), 422–424, 652
extension headers (EHs), 280
extranets, 16–17, 652

F

fast-forward switching, 256, 652
fault tolerance, 24, 652
FCC (Federal Communications Commission), 141
FCS (Frame Check Sequence) field, 222–223, 239
FDDI (Fiber Distributed Data Interface), 214
Federal Communications Commission (FCC), 141
ff02::1 all-nodes multicast group, 431
ff02::2 all-routers multicast group, 431
FIB (Forwarding Information Base), 652
Fiber Distributed Data Interface (FDDI), 214
fiber patch cords, 162–163
fiber-optic cabling, 7, 158–164
copper cabling versus, 163–164
definition of, 652
fiber patch cords, 162–163
fiber-optic connectors, 161–162
industry applications of, 160
multimode fiber, 160
properties of, 158–159
single-mode fiber, 159
summary of, 169
fiber-optic connectors, 161–162
fiber-to-the-home (FTTH), 160
fields
data link frame, 222–223
Ethernet frame, 237–239

IPv4 packets, 274–276
IPv6 packets, 280–281
TCP headers, 472
UDP headers, 474
file servers, 5
file sharing services, 530–533
FTP (File Transfer Protocol), 530
SMB (Server Message Block), 531–533
summary of, 535–536
File Transfer Protocol (FTP), 101, 511, 581. ***See also*** **file sharing services**
files, configuration, 67–68
filtering
frame, 252–253
URLs (uniform resource locators), 557
FIN flag, 486
Finish (FIN) control flag, 484–485
firewalls, 34, 555–557
definition of, 652
firmware, 48
flags, 486
flow control, 92, 471, 490–494, 652
Flow Label field (IPv6), 280
formatting messages, 90–91
form-factor pluggable (SFP) devices, 161
forwarding, 248–249, 254–255, 262, 281–282, 285–286
Forwarding Information Base (FIB), 652
fping command, 547
FQDNs (fully qualified domain names), 522
fragment-free switching, 256, 652–653
fragmenting packets, 274, 652
Frame Check Sequence (FCS) field, 222–223, 239
Frame Relay, 225
frames
data link, 221–226
frame fields, 222–223
LAN frames, 225–226
Layer 2 addresses, 223–225
overview of, 221
summary of, 229
WAN frames, 225–226
delimiting, 207
Ethernet, 234–239
baby giant frames, 238, 646
data link sublayers, 235
encapsulation, 234–235
fields in, 237–239
forwarding methods, 254–255, 262
jumbo frames, 238, 655
MAC sublayer, 236–237
runt frames, 238, 661
sending to default gateway, 254
summary of, 261
filtering, 252–253
MAC (media access control) addresses, 243–244
Freenet, 514
FTP (File Transfer Protocol), 101, 479, 511, 530, 581
definition of, 652
FTPS (FTP Secure), 581
FTTH (fiber-to-the-home), 160
full-duplex communication, 215–216, 617, 653
fully qualified domain names (FQDNs), 522

G

gateways, default
configuration, 330–334
on host, 331–332
router connections, 334
summary of, 335–336
on switch, 332–334
with Syntax Checker, 334
definition of, 282
host routing to, 282–283
pinging, 450–451
sending frames to, 254
troubleshooting, 334, 619–620
gateways, definition of, 653
Gbps (gigabits per second), 145
GET requests, 516
GIF (Graphics Interchange Format), 509
Gigabit Ethernet, 323
gigabits per second (Gbps), 145
global configuration mode, 53, 653
global routing prefix, 410, 653
global unicast addresses. ***See*** **GUAs (global unicast addresses)**
Gnutella, 514
goodput, 146, 653
gping command, 547

graphical user interfaces (GUIs), 47–48, 653
Graphics Interchange Format (GIF), 509
groups, port number, 478
GUAs (global unicast addresses)
definition of, 408
dynamic addressing for, 417–425, 437
EUI-64 process, 422–424
randomly generated interface IDs, 424–425
RS and RA messages, 417–418
SLAAC and stateless DHCPv6, 419–420
stateful DHCPv6, 420–421
static configuration of, 413–416
structure of, 408–411
summary of, 437
GUIs (graphical user interfaces), 47–48, 653

H

half-duplex communication, 215, 617, 653
hardware, 47
hardware threats, 545
HDLC (High-Level Data Link Control), 225
Header Checksum field (IPv4 packets), 275
Header Length field (TCP headers), 472
headers
IPv4 (Internet Protocol version 4), 274–276
IPv6 (Internet Protocol version 6), 278–281
TCP (Transmission Control Protocol), 471–472
UDP (User Datagram Protocol), 474
help, Cisco IOS, 58
hexadecimal number systems, 194–197, 240–241
decimal to hexadecimal conversion, 196
definition of, 653
hexadecimal to decimal conversion, 196–197
IPv6 addresses, 194–196
summary of, 198
hextets, 653
High-Level Data Link Control (HDLC), 225
Hop Limit field (IPv6 packets), 280
hops, 269
host commands, for small business networks, 596–611. *See also* specific commands
IP configuration on Linux hosts, 599–600
IP configuration on MacOS hosts, 596–601
IP configuration on Windows hosts, 596–598
summary of, 625–626
hostname command, 62, 320, 321
hosts
Cisco IOS. *See* Cisco IOS
default gateway configuration on, 331–332
definition of, 6
host addresses, 348, 653
host commands, 596–611. *See also* specific commands
IP configuration on Linux hosts, 599–600
IP configuration on MacOS hosts, 596–601
IP configuration on Windows hosts, 596–598
summary of, 625–626
host communication, 281–284
default gateways, host routing to, 282–283
host forwarding decisions, 281–282
host/router communications, 223–225
routing tables, 283–284
IP addresses. *See* IP (Internet Protocol) addresses
Linux, 599–600
MacOS, 596–601
pinging, 451–452
reachability, 444–445
remote, 282
roles of, 4–5
Windows, 596–598
hot keys, 58–60
HTTP (Hypertext Transfer Protocol), 102, 479, 511, 516–518, 580
definition of, 653
HTTPS (HTTP Secure), 102, 479, 511, 515–518, 580
definition of, 653
hub-and-spoke topologies, 211–212
hubs, 653
hubs, Ethernet, 7
hybrid cloud, 30, 654
Hypertext Transfer Protocol (HTTP), 102, 479, 511, 516–518, 580

I

IAB (Internet Architecture Board), 16, 109
IANA (Internet Assigned Numbers Authority), 109, 358, 654
ICANN (Internet Corporation for Assigned Names and Numbers), 16, 109

ICMP (Internet Control Message Protocol)
definition of, 102, 654
messages, 444–448
Destination Unreachable, 445–446
Echo Reply, 444–445
Echo Request, 444–445
Neighbor Advertisement (NA), 446–448
Neighbor Solicitation (NS), 446–448
Router Advertisement (RA), 446–448
Router Solicitation (RS), 446–448
summary of, 454
Time Exceeded, 446
ping tests, 449–452, 455
default gateways, 450–451
loopback addresses, 450
remote hosts, 451–452
summary of, 454–455
testing network connectivity with, 455
traceroute tests, 452–455
identity theft, 33, 543
IDs
device, 422
interface, 410–411
interface IDs, 424, 654
interfaces, 654
randomly generated interface IDs, 424–425
subnet, 410, 432–433, 664
IEEE (Institute of Electrical and Electronics Engineers), 111, 141, 209
definition of, 654
IEEE 802 LAN/MAN sublayers, 206–207
wireless standards, 165–166, 169–170
IETF (Internet Engineering Task Force), 16, 98, 109, 141, 209
ifconfig command, 596–601
IMAP (Internet Message Access Protocol), 101, 479, 510, 521, 581, 654
INFORMATION REQUEST messages, 529
information theft, 542
initial sequence number (ISN), 487, 654
installation, Packet Tracer, 21–22
Institute of Electrical and Electronics Engineers. ***See*** **IEEE (Institute of Electrical and Electronics Engineers)**
Integrated Services Digital Network (ISDN), 654
integrity, data, 27, 654
interface command, 323
interface configuration mode, 54
interface IDs, 410–411, 424, 654
interface vlan 1 command, 77
interfaces
Cisco IOS, 73–74
configuration, 323–330
basic configuration, 323–324
dual stack addressing, 324–325
summary of, 335
verification commands, 325–330
definition of, 9, 654
loopback, 356
randomly generated interface IDs, 424–425
selection of, 573
switch virtual interfaces, 77–78
intermediary devices, 6–7, 654
International Organization for Standardization (ISO), 98, 141, 209, 654
International Telecommunication Union (ITU), 98, 141, 209, 654
International Telecommunications Union-Telecommunication Standardization Sector (ITU-T), 111
internet
definition of, 15–16, 654
impact on daily life, 3–4
internet access technologies for, 17–20
businesses, 19–20
small office and home offices, 17–19
summary of, 38
standards, 109
Internet Architecture Board (IAB), 16, 109
Internet Assigned Numbers Authority (IANA), 109, 358, 654
Internet Control Message Protocol. ***See*** **ICMP (Internet Control Message Protocol)**
Internet Corporation for Assigned Names and Numbers (ICANN), 16, 109
Internet Engineering Task Force (IETF), 16, 98, 109, 141, 209
internet layer, 102–103, 114
Internet Message Access Protocol (IMAP), 101, 479, 510, 521, 581, 654
Internet of Things (IoT), 166, 399
internet queries, 655
Internet Research Task Force (IRTF), 109

internet service providers (ISPs), 9, 655
Internet Society (ISOC), 109
Internetwork Operating System. ***See*** **Cisco IOS**
intranets, 16–17, 655
intrusion detection system (IDS), 655
intrusion prevention systems (IPSs), 35, 655
IOS. ***See*** **Cisco IOS**
IoT (Internet of Things), 166, 399
IP (Internet Protocol) addresses, 91, 102, 398–401
ARP (Address Resolution Protocol)
broadcasts, 307–309
definition of, 301–302
examining with Packet Tracer, 309
maps, 303
overview of, 302–304
replies, 305
requests, 304
role in remote communications, 305–306
spoofing, 307–309
summary of, 313
tables, 306–307
automatic configuration for end devices, 76–77
characteristics of, 271
best-effort delivery, 272
connectionless, 271–272
media independence, 273–274
configuration
on Linux hosts, 599–600
on Windows hosts, 596–598
definition of, 4
destinations on remote network, 299–301
destinations on same network, 298–299
encapsulation, 270–271
IP addressing services, 521–530
DHCP (Dynamic Host Configuration Protocol), 527–529
DNS (Domain Name System), 522–525
nslookup command, 526–527
summary of, 535
IPv4. *See* IPv4 (Internet Protocol version 4) addressing
IPv6. *See* IPv6 (Internet Protocol version 6) addressing
loopback, pinging, 450
manual configuration for end devices, 75–76
overview of, 122–123
small business networks, 574–576
structure of, 71–73
summary of, 80, 313
switch virtual interface configuration, 77–78
troubleshooting
on end devices, 619
on IOS devices, 618
verification of, 77
VoIP (voice over IP), 469, 582
ip address command, 77, 323, 413, 600
ip default-gateway command, 77, 333
ip default-gateway ip-address command, 335–336
ip domain name command, 561
IP telephony, 582
ipconfig /all command, 622
ipconfig command, 77, 78, 423–426, 596–598, 620
ipconfig /displaydns command, 525
IPSs (intrusion prevention systems), 35, 655
IPv4 (Internet Protocol version 4) addressing, 72, 102
address conservation, 381–383
address structure, 342–349
broadcast addresses, 349
host addresses, 348
host portion, 342
logical AND, discovering addresses with, 345–346
network addresses, 347–348, 657
network portion, 342
prefix length, 344–345
subnet mask, 343–344
summary of, 390
assignment of, 358–359
binary number systems, 176–178
broadcast, 350–352, 390
coexistence with IPv6, 399+0095
dual stack addressing, 399–400
translation, 400–401
tunneling, 400
definition of, 655
destination addresses, 299
directed broadcast, 351–352, 651
DMZ (demilitarized zone), 354–355
limitations of, 398–401, 436
multicast, 352–353, 390
network segmentation, 359–362

broadcast domains and, 359–362
reasons for, 362
summary of, 391
number systems, 193–194
overview of, 342
packets, 274–276
fragmenting, 274
header fields, 274–276
headers, 274
limitations of, 277
summary of, 292
passing/blocking, 356
routing tables, 290–291
routing to Internet, 354
for small business networks, 574–576
source addresses, 299
structured design, 387–389, 392
device address assignment, 389
IPv4 network address planning, 388
with Packet Tracer, 389, 392–393
subnetting, 364–381. *See also* VLSM (variable-length subnet masking)
/8 networks, 372–373, 391
/16 networks, 367–370, 391
corporate example of, 378–380
DMZ (demilitarized zone), 377
efficiency of, 377–380
maximizing, 377–378
on an octet boundary, 364–366
within an octet boundary, 366–367
with Packet Tracer, 367, 381
private versus public address space, 374–377
summary of, 391–392
unused host IPv4 addresses, minimizing, 377–378
types of
legacy classful, 357–358, 648
link-local, 357
loopback, 356
private, 353–354
public, 353–354
summary of, 390
unicast, 349–350, 390
VLSM (variable-length subnet masking), 381–387
address conservation, 381–383
network address assignments in, 386–387
overview of, 381
subnetting schemes in, 383–385
summary of, 392
IPv6 (Internet Protocol version 6) addressing, 73, 102, 408
address formats, 401–406, 436
double colon (::), 404–405
leading zeros, 403–404
preferred format, 402
anycast, 406, 436–437
coexistence with IPv4, 399–401
dual stack addressing, 399–400
translation, 400–401
tunneling, 400
GUAs (global unicast addresses)
definition of, 408
dynamic addressing for, 417–425, 437
static configuration of, 413–416
structure of, 408–411
summary of, 437
LLAs (link-local addresses)
definition of, 408
dynamic addressing for, 425–430, 437–438
static configuration of, 413–416
structure of, 411–412
summary of, 437
multicast
characteristics of, 93, 406, 430–432, 436–437
solicited-node, 432
summary of, 438
well-known, 430–431
ND (Neighbor Discovery), 309–312, 314
address resolution, 311
examining with Packet Tracer, 312
messages, 309–310
summary of, 314
need for, 398–401, 436
number systems, 194–196
packets, 277–281
headers, 278–281
overview of, 277–278
prefix length, 406–407
subnetting, 432–435
example of, 433–434
with Packet Tracer, 438
router configuration, 435

subnet allocation, 434–435
subnet IDs, 432–433
summary of, 438
unicast, 406, 407–408, 436–437
verifying configuration of, 427–430
ipv6 address command, 323, 413–414
ipv6 address link-local command, 415–416
ipv6 unicast-routing command, 418, 431
IRFT (Internet Research Task Force), 109
ISD (intrusion detection system), 655
ISDN (Integrated Services Digital Network), 654
ISN (initial sequence number), 487, 654
ISO (International Organization for Standardization), 98, 141, 209, 654
ISOC (Internet Society), 109
ISPs (internet service providers), 9, 655
IT professionals, 35–36, 40
CCNA certification for, 35–36
networking jobs for, 36
ITU (International Telecommunication Union), 98, 111, 141, 209, 654

J

jackets, 655
Japanese Standards Association (JSA/JIS), 141
JPG (Joint Photographic Experts Group), 509
JSA/JIS (Japanese Standards Association), 141
jumbo frames, 238, 655

K

kbps (kilobits per second), 145
kernel, 47, 655
keyboard shortcuts, 58–60
kilobits per second (kbps), 145

L

LACNIC (Regional Latin-American and Caribbean IP Address Registry), 359
LANs (local area network), 12–14. *See also* network communications; networks; router configuration
definition of, 655
IEEE 802 LAN/MAN sublayers, 206–207
LAN frames, 225–226
topologies, 213–214
latency, 146, 655
Layer 2 addresses, 223–225
Layer 3 logical addresses, 122–123
layered security, 553
layers, OSI model. *See* OSI (Open System Interconnection) model
layers, TCP/IP model. *See* TCP/IP (Transmission Control Protocol/Internet Protocol) model
LC (Lucent Connector) connectors, 162
LDAP (Lightweight Directory Access Protocol), 655
leading zeros
double colon (::), 404–405
in IPv6 addresses, 403–404
learning, switch, 248–249
lease periods, 527–528
leased lines, 18, 19
legacy classful addressing, 357–358, 648
legacy LAN topologies, 214
Length field (UDP headers), 474
Lightweight Directory Access Protocol (LDAP), 655
limited broadcast, 655
line console 0 command, 63
line of sight wireless, 655
line vty 0 15 command, 64
Link Layer Discovery Protocol (LLDP), 247
link-local addresses. *See* LLAs (link-local addresses)
Linux hosts, IP (Internet Protocol) configuration on, 599–600
LLAs (link-local addresses), 357
definition of, 408, 655
dynamic addressing for, 425–430, 437–438
dynamic LLA creation, 425
dynamic LLA on Cisco routers, 426–427
dynamic LLA on Windows, 425–426
IPv6 address configuration, verification of, 427–430
with Packet Tracer, 430
static configuration of, 413–416
structure of, 411–412
summary of, 437
LLC (Logical Link Control), 206, 235, 656
LLDP (Link Layer Discovery Protocol), 247
local area networks. *See* LANs (local area network)
AND, logical, 645

logical addresses. ***See*** **IP (Internet Protocol) addresses**
logical AND, 345–346, 645
Logical Link Control (LLC), 206, 235, 656
logical NOT, 345
logical OR, 345
logical topologies, 10–11, 209–211
logical topology diagrams, 656
login block-for command, 560
login command, 63, 64
login local command, 562
long-haul networks, 160
loopback adapters, 656
loopback addresses, 356, 450, 656
loopback interfaces, 656
loopback interfaces, pinging, 356
LTE, 656
Lucent Connector (LC) connectors, 162

M

MAC (media access control) addresses, 124, 206–207, 239–248
address structure, 241–243
address table, 248–254
on connected switches, 252
definition of, 656
frame filtering, 252–253
summary of, 261
switch fundamentals, 248–249
switch learning and forwarding, 250–251
viewing, 254
ARP (Address Resolution Protocol)
broadcasts, 307–309
definition of, 301–302
examining with Packet Tracer, 309
overview of, 302–304
replies, 305
requests, 304
role in remote communications, 305–306
spoofing, 307–309
summary of, 313
tables, 306–307
broadcast, 246–247
definition of, 656
destinations on remote network, 299–301
destinations on same network, 298–299
frame processing, 243–244
hexadecimal number system, 240–241
multicast, 247–248
summary of, 261, 313
unicast, 244–245
MAC (media access control) sublayer, 236–237. ***See also*** **MAC (media access control) addresses**
data encapsulation, 236
media access, 237
MacOS hosts, IP configuration on, 596–601
maintenance threats, 545
malware, 546–547
Trojan horses, 33, 547, 665
viruses, 546
worms, 547, 668
Manchester encoding, 142–143
man-in-the-middle attack, 549
MANs (metropolitan-area networks), 656
maps (ARP), 303
Matroska Video (MKV), 509
maximizing subnets, 377–378
maximum segment size (MSS), 491–492
maximum transmission unit (MTU), 492, 656
Mbps (megabits per second), 145
mdix auto command, 259
media, network, 7–8
media access
data link layer functions, 207–208
MAC (media access control) sublayer, 237
media access control. ***See*** **MAC (media access control) addresses**
media independence, 273–274, 656
megabits per second (Mbps), 145
memory buffering, 257, 647
mesh topologies, 212
messages. ***See also*** **data encapsulation**
banner, 65–66
decoding, 89
delivery options for, 92–93
destinations, 87
DHCP (Dynamic Host Configuration Protocol), 528–529
DNS (Domain Name System), 524–525
encapsulating, 90–91
encoding, 88–89, 142–143

formatting, 90–91
ICMP (Internet Control Message Protocol), 444–448
Destination Unreachable, 445–446
Echo Reply, 444–445
Echo Request, 444–445
Neighbor Advertisement (NA), 446–448
Neighbor Solicitation (NS), 446–448
Router Advertisement (RA), 446–448
Router Solicitation (RS), 446–448
summary of, 454
Time Exceeded, 446
ND (Neighbor Discovery), 309–310
segmenting, 116–117
size of, 91–92
sources, 87
timing, 92–93
Metro Ethernet, 18, 20
metropolitan-area networks (MANs), 656
mismatch issues, troubleshooting, 617
mitigation techniques, 552–558
AAA (authentication, authorization, and accounting), 555
backups, 553–554
defense-in-depth approach, 553
endpoint security, 558
firewalls, 555–557
summary of, 565
updates and patches, 554
MKV (Matroska Video), 509
MMF (multimode fiber), 160, 657
models. *See* OSI (Open System Interconnection) model; TCP/IP (Transmission Control Protocol/ Internet Protocol) model
modems, 656
Motion Picture Experts Group (MPG), 509
MOV (QuickTime Video), 509
MPG (Motion Picture Experts Group), 509
MSS (maximum segment size), 491–492
MTU (maximum transmission unit), 492, 656
multiaccess networks, 216
multicast IPv4 addresses, 352–353, 390
multicast IPv6 addresses
assigned multicast, 646
characteristics of, 93, 406, 430–432, 436–437
solicited-node, 432
summary of, 438
well-known, 430–431, 667
multicast MAC (media access control) addresses, 247–248
multicast transmission, 656–657
multimeters, 657
multimode fiber (MMF), 160, 657
multiplexing, 117–118, 132, 657
MX records, 524

N

NA (Neighbor Advertisement) message, 309, 446–448, 657
names, Cisco IOS device, 61–62
NAS (network attached storage), 657
NAT (Network Address Translation), 354, 398, 657
NAT64 (Network Address Translation 64), 400–401
navigation, Cisco IOS, 52–56
configuration mode, 53–54
moving between modes, 54–55
Packet Tracer, 60
primary command modes, 52–53
subconfiguration mode, 53–54
summary of, 79
Syntax Checker, 55–56
Tera Term, 60
ND (Neighbor Discovery), 245, 309–312, 446
address resolution, 311
definition of, 657
examining with Packet Tracer, 312
messages, 309–310
summary of, 314
Neighbor Advertisement (NA) messages, 309, 446–448, 657
Neighbor Discovery. *See* ND (Neighbor Discovery)
Neighbor Solicitation (NS) messages, 309, 446–448, 657
netsh interface ip delete arpcache command, 602
netstat command, 479–480
netstat -r command, 283–284, 293
NetWare, 99
network access layer, 103, 114
Network Address Translation 64 (NAT64), 400–401
Network Address Translation (NAT), 354, 398, 657
network addresses, 347–348, 657
network applications, 578

network architecture, definition of, 657
network attached storage (NAS), 657
network baselines, 593–596
network communications. ***See also*** **OSI (Open System Interconnection) model; TCP/IP (Transmission Control Protocol/Internet Protocol) model**
communications standards, 111
data access, 121–129
data link addresses, 124, 126–129
devices on same network, 123
Layer 3 logical addresses, 122–123
network layer addresses, 125
overview of, 121
summary of, 132
data encapsulation, 116–121
de-encapsulation, 120–121, 132
example of, 120
message segmenting, 116–117
PDUs (protocol data units), 118–120, 132
sequencing, 96, 118–119
summary of, 132
definition of, 648
messages
decoding, 89
delivery options for, 92–93
destination, 87
encapsulating, 90–91
encoding, 88–90, 142–143
formatting, 90–91
segmenting, 96, 118–119
size of, 91–92
sources, 87
timing, 92–93
overview of, 86–87, 88
protocol suites, 97–107. *See also* TCP/IP (Transmission Control Protocol/Internet Protocol) model
evolution of, 98–99
overview of, 97–98
summary of, 130
protocols. *See also* specific protocols
definition of, 87–88
functions of, 95–96
interaction between, 96
requirements of, 88–89
summary of, 130
types of, 94–95
rule establishment for, 88, 130
standards organizations, 108–111
communications standards, 111
electronic standards, 111
internet standards, 109
open standards, 108–109
summary of, 131
network infrastructure, definition of, 657
network interface cards (NICs), 9, 139, 168, 657
network layer. ***See also*** **IP (Internet Protocol) addresses**
basic operations of, 268–269
characteristics of, 268–274, 292
hops, 269
host communication, 281–284
default gateways, 282–283
host forwarding decisions, 281–282
routing tables, 283–284
routing, 285–291
dynamic, 288–290
IP router routing tables, 286–287
IPv4 routing tables, 290–291
router packet forwarding decisions, 285–286
static, 287–288
networking jobs, 36
networks. ***See also*** **addresses; internet; network communications; router configuration; small business network management**
architecture of, 23
BYOD (bring your own device), 28
clients, 4
cloud computing, 29–30
collaboration, 28–29, 648
connectivity, testing
with Packet Tracer, 455
with ping tests, 455
with traceroute, 455
converged, 20–21, 649
data flow through, 6
end devices, 6
extranets, 16–17, 652
host roles, 4–5
impact on daily life, 3–4, 37
intermediary devices, 6–7
intranets, 16–17

LAN (local area network) design, 12–14. *See also* router configuration
IEEE 802 LAN/MAN sublayers, 206–207
LAN frames, 225–226
topologies, 213–214
media, 7–8
peer-to-peer, 5, 658
powerline networking, 31–32
prefixes, 345
reliability of, 23–27
fault tolerance, 24
QoS (quality of service), 25–26
scalability, 24–25
security design, 26–27
summary of, 38
remote, 661
representations of, 8–10, 37
role of IT professionals in, 35–36, 40
security, 33–35, 542–543
attack mitigation, 552–558
attacks, 546–552
design for, 26–27
device, 558–564, 566
mitigation techniques, 34–35
physical, 545–546
summary of, 39
threats, 33–34, 565
vulnerabilities, 543–544
segmentation of, 359–362
broadcast domains and, 359–362
definition of, 662
reasons for, 362
summary of, 391
servers
common software for, 4–5
definition of, 4
sizes of, 11–12
smart homes, 31
SOHO (small office and home office) networks, 12
topology diagrams for, 8–11
definition of, 10
logical, 10–11
network symbols for, 8–10
physical, 10
trends in, 27–32, 38–39
types of, 37
video communications tools for, 29
WANs (wide area networks), 14–15
wireless, 32
networksetup -getinfo command, 601
networksetup -listallnetworkservices command, 601
Next Header field (IPv6 packets), 280
next hop, 657
nibble boundary, 657
NICs (network interface cards), 9, 139, 168, 657
no hostname command, 62
no ip directed-broadcasts command, 352
no ip http server command, 563
no shutdown command, 77, 323–324, 335
node icon, 94
noise, 658
nonreturn to zero (NRZ), 658
Non-Volatile Memory Express (NVMe), 658
nonvolatile random-access memory (NVRAM), 67, 658
notation, positional. ***See*** **positional notation**
Novell NetWare, 99
NRZ (nonreturn to zero), 658
NS (Neighbor Solicitation) message, 309, 446–448, 657
NS records, 524
nslookup command, 526–527, 530, 547, 622–623, 658
number systems
binary, 176–194
binary positional notation, 178–180
binary to decimal conversion, 180–181
decimal to binary conversion, 182–193
IPv4 addresses, 176–178
summary of, 198
hexadecimal, 194–197
decimal to hexadecimal conversion, 196
hexadecimal to decimal conversion, 196–197
IPv6 addresses, 194–196
summary of, 198
653, 653
overview of, 176
numbers, port
definition of, 465
destination, 650
groups of, 478
multiple separation communications with, 476

netstat command, 479–480
socket pairs, 477–478
well-known, 479
NVMe (Non-Volatile Memory Express), 658
NVRAM (nonvolatile random-access memory), 67, 658

O

octet boundary, 658
subnetting on, 364–366
subnetting within, 366–367
octets, 658
Open Samples command (Packet Tracer), 22
Open Shortest Path First (OSPF), 103
open standards, 108–109
Open System Interconnection model. *See* OSI (Open System Interconnection) model
OpenDNS, 622
operating systems (OSs), 46–47, 48–49
optical fiber cabling. *See* fiber-optic cabling
OR, logical, 345
.org domain, 525
organizationally unique identifiers (OUIs), 242, 422, 658
OSI (Open System Interconnection) model, 508. *See also* TCP/IP (Transmission Control Protocol/Internet Protocol) model
application layer
client-server model, 511–512
definition of, 508
email protocols, 518–521
file sharing services, 530–533
IP addressing services, 521–530
peer-to-peer applications, 513–515
peer-to-peer networks, 512–513
protocols, 508–511
purpose of, 508
summary of, 534
web protocols, 515–518
benefits of using, 112
data link layer
data link frame, 221–226, 229
IEEE 802 LAN/MAN sublayers, 206–207
media access in, 207–208
purpose of, 204–206, 228
standards, 209
topologies, 209–220, 228
definition of, 98
network layer. *See also* IP (Internet Protocol) addresses
basic operations of, 268–269
characteristics of, 268–274, 292
hops, 269
host communication, 268–269
routing, 285–291
overview of, 112–114
Packet Tracer simulation, 116
physical layer. *See also* copper cabling; fiber-optic cabling
characteristics of, 141–146, 168
fiber-optic cabling, 158–164
purpose of, 138–140
summary of, 168
wireless media, 164–167, 169–170
summary of, 131
TCP/IP model compared to, 115–116
OSPF (Open Shortest Path First), 103
OSs (operating systems), 46–47, 48–49
OUIs (organizationally unique identifiers), 242, 422, 658
out-of-band management, 49
overhead, 658

P

P2P (peer-to-peer) applications, 513–515
P2P (peer-to-peer) networks, 5, 512–513, 534, 658
P2PRG (Peer-to-Peer Research Group), 109
packet filtering, 557
packet forwarding. *See* forwarding
packet switched. *See* switches
Packet Tracer
ARP table examination with, 309
Cisco IOS navigation with, 60
connecting routers with, 334
device configuration with, 71, 336
features of, 22–23
installation of, 21–22
IPv6 addressing configuration with, 430
IPv6 ND examination with, 312
IPv6 subnetting with, 438

physical layer connections with, 167
reference model simulations, 116
router configuration with, 323
subnetting with, 367, 381
testing network connectivity with, 455
VLSM design and implementation, 389, 392–393
packets
fragmenting, 274, 652
IPv4, 274–276
header fields, 274–276
headers, 274
limitations of, 277
summary of, 292
IPv6, 277–281
headers, 278–281
IPv6 packets, 277–278
router forwarding decisions, 285–286
PANs (personal-area networks), 658
parallel ports, 658
passing IPv4 addresses, 356
passphrases, 560
password attacks, 548
password command, 63, 64, 320
passwords
Cisco IOS devices
configuration, 63–64
encryption, 64–65
guidelines for, 62–63
configuration of, 559–561
enable, 651
SSH (Secure Shell), 561–562
patches, 554
Payload Length field (IPv6 packets), 280
PDUs (protocol data units), 118–120, 132, 660
peers, 512
peer-to-peer applications, 513–515
peer-to-peer networks, 5, 512–513, 534, 658
Peer-to-Peer Research Group (P2PRG), 109
personal-area network (PAN), 658
physical addresses. *See* MAC (media access control) addresses
physical layer
characteristics of, 141–146
bandwidth, 145–146
components, 142
encoding, 142–143
signaling, 143–144
standards organizations, 141
summary of, 168
copper cabling, 146–152
characteristics of, 147–148
coaxial cable, 151–152, 648
fiber-optic cabling versus, 163–164
rollover cables, 157
STP (shielded twisted pair), 150–151
summary of, 168–169
UTP (unshielded twisted pair), 148–150, 152–158, 169
definition of, 114
fiber-optic cabling, 158–164
copper cabling versus, 163–164
fiber patch cords, 162–163
fiber-optic connectors, 161–162
industry applications of, 160
multimode fiber, 160
properties of, 158–159
single-mode fiber, 159
summary of, 169
purpose of, 138–140
summary of, 168
wireless media, 164–167
properties of, 164–165
summary of, 169–170
types of, 165–166
wireless LANs (WLANs), 166–167
physical ports. *See* ports
physical security, 545–546
physical topologies, 10, 209–211, 659
physical topology diagrams, 659
ping command
default gateway testing with, 450–451
definition of, 659
device connectivity verification with, 78
IOS command syntax, 57
IPv6 verification with, 429
lab exercises for, 455
loopback interface testing with, 356, 450
network baseline assessment with, 593–596
overview of, 449–452
ping sweeps, 547, 659
remote host testing with, 451–452

small business network verification with, 586–590
summary of, 454–455
PNG (Portable Network Graphics), 509
PoE (Power over Ethernet), 659
Point-to-Point Protocol (PPP), 225
point-to-point topologies, 211, 213
policy vulnerabilities, 544
pools, DHCP (Dynamic Host Configuration Protocol), 527
POP (Post Office Protocol), 479, 520, 659
POP3 (Post Office Protocol), 101, 510, 659
Portable Network Graphics (PNG), 509
ports, 9
Cisco IOS, 73–74
definition of, 659
port numbers
definition of, 465, 659
destination, 650
groups of, 478
multiple separation communications with, 476
netstat command, 479–480
socket pairs, 477–478
table of, 510–511
well-known, 479
redirection, 549
registry, 479
scans of, 548, 659
selection of, 573
positional notation
binary, 178–180, 182–186
decimal, 178–179
definition of, 178
POST (power-on self-test), 659
Post Office Protocol (POP3), 101, 479, 510, 520, 659
POST requests, 517
Power over Ethernet (PoE), 659
powerline networking, 31–32, 659
power-on self-test (POST), 659
PPP (Point-to-Point Protocol), 225
Preamble field (Ethernet frames), 238
preferred format, IPv6, 402–406, 659
prefixes, 345, 659
IPv4, 344–345
IPv6, 406–407
presentation layer, 534
definition of, 113
functions of, 508–510
private cloud, 30, 659
private IPv4 addresses, 353–354, 374–377, 659
privileged EXEC mode, 53, 64, 659
protocol analyzers, 660
protocol data units (PDUs), 118–120, 132, 660
Protocol field (IPv4 packets), 276
protocol suites, 97–107. ***See also*** **TCP/IP (Transmission Control Protocol/Internet Protocol) model**
definition of, 660
evolution of, 98–99
overview of, 97–98
protocols. ***See also*** **specific protocols**
definition of, 87–88, 660
functions of, 95–96
interaction between, 96
requirements of, 88–89
types of, 94–95
proxy servers, 660
PSH flag, 486
public cloud, 30, 660
public IPv4 addresses, 353–354, 374–377, 660
PUT requests, 517
PuTTY, 50, 68–70

Q

qBittorrent, 514
QoS (quality of service), 25–26, 582, 660
quality-of-service (QoS), 660
queries, internet, 655
queuing, 660
QuickTime Video (MOV), 509

R

RA (Router Advertisement) messages, 310, 417–418, 446–448, 661
radio frequency interference (RFI), 147, 660
RADIUS (Remote Authentication Dial-in User Service), 495
RAM (random-access memory), 67, 660
random-access memory (RAM), 660
randomly generated interface IDs, 424–425

read-only memory (ROM), 243, 660
real-time traffic, 660
Real-Time Transport Control Protocol (RTCP), 582
Real-Time Transport Protocol (RTP), 582
reconnaissance attacks, 547–548, 660
Redirect message, 310
redundancy, 576–577, 660
reference models. ***See*** **OSI (Open System Interconnection) model; TCP/IP (Transmission Control Protocol/Internet Protocol) model**
Regional Internet Registries (RIRs), 358–359
regional Internet registry (RIR), 661
Regional Latin-American and Caribbean IP Address Registry (LACNIC), 359
reliability, 38
IP (Internet Protocol), 273–274
network, 23–27
of protocols, 96
TCP (Transmission Control Protocol), 486–490, 500–501
UDP (User Datagram Protocol), 494
reload command, 68
Remote Authentication Dial-in User Service (RADIUS), 495
remote communications, ARP (Address Resolution Protocol) in, 305–306
remote hosts
definition of, 282
pinging, 451–452
remote networks, 661
repeaters, 661
replies (ARP), 305
REPLY messages, 529
Representational State Transfer (REST), 102
representations, network, 8–10, 37
requests
ARP (Address Resolution Protocol), 304
TCP (Transmission Control Protocol), 481–482
UDP (User Datagram Protocol), 495–497
requests for comments (RFCs), 209, 661
Réseaux IP Européens Network Coordination Centre (RIPE NCC), 359
Reserved field (TCP headers), 472
resolution, 613
response timeout, 661
responses
TCP (Transmission Control Protocol), 482–483
timeout, 92
UDP (User Datagram Protocol), 497–498
REST (Representational State Transfer), 102
RFCs (requests for comments), 209, 661
RFI (radio frequency interference), 147, 660
ring topology, 214, 661
RIPE NCC (Réseaux IP Européens Network Coordination Centre), 359
RIR (regional Internet registry), 661
RIRs (Regional Internet Registries), 358–359
RJ-11 connectors, 661
RJ-45 connectors, 154, 661
rollover cables, 157
ROM (read-only memory), 243, 660
round-trip time (RTT), 661
route entries, 285, 293
route print command, 283–284
Router Advertisement (RA) messages, 310, 417–418, 446–448, 661
router configuration, 336–337
ARP tables, displaying, 306–307
basic configuration example, 321–323
banner warnings, 322
device name, 321
initial router settings, 323
running configuration, saving, 322
secure access, 322
basic configuration steps, 320–321, 335
default gateways, 330–334
configuration, 330–334
summary of, 335–336
troubleshooting, 334
dynamic LLAs (link-local addresses) on, 426–427
host/router communications, 223–225
interfaces, 323–330
basic configuration, 323–324
dual stack addressing, 324–325
summary of, 335
verification commands, 325–330
Router Solicitation (RS) messages, 310, 417–418, 446–448, 661
routers, 661
routing, 285–291. ***See also*** **router configuration**
definition of, 661

dynamic, 288–290
host communication, 281–284
default gateways, 282–283
host forwarding decisions, 281–282
routing tables, 283–284
IPv4 routing tables, 290–291
router packet forwarding decisions, 285–286
routing tables, 286–287, 290–291
static, 287–288
RS (Router Solicitation) messages, 310, 417–418, 446–448, 661
RST flag, 486
RTCP (Real-Time Transport Control Protocol), 582
RTP (Real-Time Transport Protocol), 582
RTT (round-trip time), 661
running configuration, altering, 68
running-config file, 67
runt frames, 238, 661

S

SACK (selective Acknowledgement), 489
SACK (selective acknowledgment), 662
satellite internet access, 19, 661
SC (subscriber connector) connectors, 161
scalability, small network, 24–25, 583–586, 624
definition of, 661–662
employee network utilization, 584–586
protocol analysis, 583–584
small network growth, 583
SDSL (symmetric DSL), 20
Secure FTP (SFTP), 101, 581, 663
Secure Shell (SSH), 50, 479, 561–562, 580, 662
SecureCRT, 50
security, 33–35
attack mitigation, 552–558
AAA (authentication, authorization, and accounting), 555
backups, 553–554
defense-in-depth approach, 553
endpoint security, 558
firewalls, 555–557
updates and patches, 554
attacks, 546–552
access, 548–549
attack mitigation, 565
malware, 546–547
reconnaissance, 547–548
summary of, 565
design for, 26–27
device, 558–564
Cisco AutoSecure, 558–559
passwords, 559–561
SSH (Secure Shell), 561–562
summary of, 566
unused services, disabling, 563–564
mitigation techniques, 34–35
physical, 545–546
summary of, 39
threats, 33–34
summary of, 565
types of, 542–543
vulnerabilities, 543–544
security passwords min-length command, 560
segmentation, network, 359–362
broadcast domains and, 359–362
definition of, 662
reasons for, 362
summary of, 391
segments, 116–117, 463, 468
ACK (Acknowledgement), 472, 484–485, 486, 488
definition of, 662
MSS (maximum segment size), 491–492
selective Acknowledgement (SACK), 489
selective acknowledgment (SACK), 662
SEQ (sequence) number, 488
Sequence Number field (TCP headers), 472
sequence numbers, 662
sequencing, 96, 118–119
Server Message Block (SMB), 531–533, 662, 663
servers
common software for, 4–5
definition of, 4
TCP (Transmission Control Protocol)
connection establishment, 483–484
server processes, 480–483
session termination, 484–485
three-way handshake, 485–486
types of, 580–581
UDP (User Datagram Protocol), 495
service password-encryption command, 64, 560

services
application layer, 579
disabling, 563–564
file sharing, 530–533
FTP (File Transfer Protocol), 530
SMB (Server Message Block), 531–533
summary of, 535–536
IP addressing, 521–530
DHCP (Dynamic Host Configuration Protocol), 527–529
DNS (Domain Name System), 522–525
nslookup command, 526–527
summary of, 535
session layer, 534
definition of, 113
functions of, 508–510
sessions, 662
SFP (small form-factor pluggable) devices, 161
SFTP (Secure FTP), 101, 581, 663
sharing services. ***See*** **file sharing services**
shell, 47
shells, 662
shielded twisted pair (STP) cable, 150–151, 662
show arp command, 603, 606
show cdp neighbors command, 609–610
show control-plane host open-ports command, 563
show interfaces command, 328, 335, 603, 604–605
show ip arp command, 306–307
show ip interface brief command, 325–326, 335, 610–611, 618
show ip interface command, 329, 335, 603, 605–606, 618
show ip ports all command, 563
show ip route command, 290–291, 293, 327, 335, 603, 606–607, 620
show ipv6 interface brief command, 325–327, 335, 427–428
show ipv6 interface command, 330, 335
show ipv6 route command, 327–328, 335, 428–429
show protocols command, 603, 607
show running-config command, 65, 67–68, 70, 333, 603–604
show startup-config command, 70
show version command, 603, 608, 611
signal attenuation, 147
signaling, 143–144
Simple Mail Transfer Protocol (SMTP), 101, 479, 510, 519–520, 581, 662, 663
simplex LC (Lucent Connector) connectors, 162
single-mode fiber (SMF), 159, 662
size
of messages, 91–92
of networks, 11–12
of windows, 472, 490–491, 667
SLAAC (stateless address autoconfiguration), 101
definition of, 662, 663
EUI-64 process, 422–424
randomly generated interface IDs, 424–425
stateful DHCPv6, 420–421
stateless DHCPv6, 419–420
slash notation, 662
sliding window protocol, 491
small business network management
applications
common applications, 578–579
summary of, 624
voice/video applications, 582
device selection, 573–574, 624
expandability, 573
host and IOS commands for, 596–611
arp, 601–602
ifconfig, 596–601
IP configuration on Linux hosts, 599–600
IP configuration on MacOS hosts, 596–601
IP configuration on Windows hosts, 596–598
ipconfig, 596–598
show arp, 603, 606
show cdp neighbors, 609–610
show interfaces, 603, 604–605
show ip interface, 603, 605–606
show ip interface brief, 610–611
show ip route, 603, 606–607
show protocols, 603, 607
show running-config, 603–604
show version, 603, 608, 611
summary of, 625–626
internet access technologies for, 19–20
IP addressing, 574–576
protocols, 579–581
protocol analysis, 583–584
summary of, 624

redundancy, 576–577, 660
scalability, 624
scaling, 583–586
definition of, 661–662
employee network utilization, 584–586
protocol analysis, 583–584
small network growth, 583
topologies, 572–573
traffic management, 577–578
troubleshooting methodologies, 611–616
basic approach, 612–613
debug command, 613–615, 616
resolution versus escalation in, 613
summary of, 626
terminal monitor command, 615–616
troubleshooting scenarios, 616–623
default gateway issues, 619–620
duplex operation, 617
IP addressing on end devices, 619
IP addressing on IOS devices, 618
mismatch issues, 617
summary of, 626–627
verifying connectivity of, 586–596
network baselines, 593–596
ping command, 586–590
summary of, 625
traceroute command, 590–594
tracert command, 590–593
small office and home office (SOHO) networks, 12, 17–19, 662
smart homes, 31, 662
SMB (Server Message Block), 531–533, 662, 663
SMF (single-mode fiber), 159, 662
SMTP (Simple Mail Transfer Protocol), 479, 510, 519–520, 581, 662
SNMP (Simple Network Management Protocol), 663
socket pairs, 477–478, 663
sockets, 663
SOHO (small office and home office) networks, 12, 17–19, 662
SOLICIT messages, 529
Solicitation messages. ***See*** **RS (Router Solicitation) messages**
solicited-node IPv6 multicast addresses, 432, 663
Source IPv4 Address field, 276
source IPv4 addresses, 122, 123, 125, 299, 663
Source IPv6 Address field, 280
Source MAC Address field, 238
source MAC addresses, 124, 126, 243, 299, 301, 305
Source Port field
TCP headers, 472
UDP headers, 474
sources, 87
Spanning Tree Protocol (STP), 247
speed settings, 257–259, 262
SPI (stateful packet inspection), 557, 663
spoofing, 663
spoofing (ARP), 307–309
spyware, 33
SSH (Secure Shell), 50, 479, 561–562, 580, 662
ST (straight-tip) connectors, 161
standards, 108–111
communications, 111
data link layer, 209
electronic, 111
internet, 109
open, 108–109
physical layer, 141
UTP (unshielded twisted pair) cable, 153–156
star topology, 213–214, 663
Start Frame Delimiter field (Ethernet frames), 238
startup-config file, 67
stateful DHCPv6, 420–421, 663
stateful packet inspection (SPI), 557, 663
stateful protocols, 471. ***See also*** **TCP (Transmission Control Protocol)**
stateless address autoconfiguration. ***See*** **SLAAC (stateless address autoconfiguration)**
stateless DHCPv6, 418–420, 663
stateless protocols, 468
static addressing, 527
static configuration
GUAs (global unicast addresses), 413–416
LLAs (link-local addresses), 413–416
static route propagation, 663
static routing, 287–288
store-and-forward switching, 254–255, 664
STP (shielded twisted pair), 150–151, 662
STP (Spanning Tree Protocol), 247
straight-through UTP cables, 157
straight-tip (ST) connectors, 161

strong passwords, 560
structured design, IPv4, 387–389, 392
device address assignment, 389
IPv4 network address planning, 388
with Packet Tracer, 389, 392–393
subconfiguration mode, 53–54
sublayers, IEEE 802 LAN/MAN, 206–207
submarine cable networks, 160
subnet IDs, 410, 432–433, 664
subnetting, 364–381
definition of, 664
IPv4
/8 networks, 372–373, 391
/16 networks, 367–370, 391
corporate example of, 378–380
DMZ (demilitarized zone), 377
efficiency of, 377–380
maximizing subnets, 377–378
on an octet boundary, 364–366
within an octet boundary, 366–367
with Packet Tracer, 367, 381
private versus public address space, 374–377
summary of, 391–392
unused host IPv4 addresses, minimizing, 377–378
VLSM (variable-length subnet masking), 381–387
IPv6, 432–435
example of, 433–434
with Packet Tracer, 438
router configuration, 435
subnet allocation, 433–434
subnet IDs, 432–433
summary of, 438
subnet IDs, 410, 432–433
subnet masks, 72, 343–344
VLSM (variable-length subnet masking), 381–387
address conservation, 381–383
network address assignments in, 386–387
overview of, 381
subnetting schemes in, 383–385
summary of, 392
subscriber connector (SC) connectors, 161
SVI (switch virtual interface), 664
SVIs (switch virtual interfaces), 74
swarms, 514
switch fabric, 664
switch virtual interfaces (SVIs), 74
Switch(config)# prompt, 53–54
switched virtual interface (SVI), 664
switches
asymmetric switching, 646
Cisco IOS. *See* Cisco IOS
default gateway configuration on, 332–334
definition of, 664
Ethernet
Auto-MDIX, 259–260
cut-through switching, 255–256, 649
duplex settings, 257–259
fast-forward switching, 256, 652
fragment-free switching, 256, 652–653
memory buffering on, 257
speed settings, 257–259, 262
store-and-forward switching, 254–255, 664
frame filtering, 252–253
frame forwarding methods on, 254–255, 262
learning and forwarding, 248–249
MAC addressing for. *See* MAC (media access control) addresses
overview of, 248–249
switch virtual interfaces, 77–78
symmetric DSL (SDSL), 20
SYN flag, 486
Syntax Checker
Cisco IOS device configuration with, 66
Cisco IOS navigation with, 55–56
default gateway configuration with, 334
nslookup command, 527
router configuration with, 323
syslog, 664
system speakers, 664

T

T568A/T68B standards, 157–158
tables
ARP (Address Resolution Protocol)
displaying, 306–307
removing entries from, 306–307
binary positional value, 182–186
CAM (content addressable memory), 649
MAC (media access control) address, 248–254
on connected switches, 252

definition of, 656
frame filtering, 252–253
switch fundamentals, 248–249
switch learning and forwarding, 248–249
viewing, 254
routing, 283–284, 286–287, 290–291
TCP (Transmission Control Protocol), 102
applications using, 472–473
congestion avoidance, 493
connection establishment, 483–484
data loss and retransmission, 486–487
definition of, 665
features of, 470–471
flow control, 471, 490–494
headers, 471–472
MSS (maximum segment size), 491–492
packet delivery, 486–487
reliability of, 467–468, 486–490, 500–501
server processes, 480–483
session termination, 484–485
summary of, 499
three-way handshake, 485–486
UDP (User Datagram Protocol) compared to, 469–470
window size, 490–491
TCP/IP (Transmission Control Protocol/Internet Protocol) model
application layer
client-server model, 511–512
definition of, 508
email protocols, 518–521
file sharing services, 530–533
IP addressing services, 521–530
overview of, 101–102
peer-to-peer applications, 513–515
peer-to-peer networks, 512–513
protocols, 508–511
purpose of, 508
summary of, 534
web protocols, 515–518
benefits of using, 112
communication process in, 103–107
definition of, 98, 664
internet layer, 102–103
network access layer, 103
network layer. *See also* IP (Internet Protocol) addresses
basic operations of, 268–269
characteristics of, 268–274, 292
hops, 269
host communication, 281–284
routing, 285–291
OSI model compared to, 115–116
overview of, 114
Packet Tracer simulation, 116
physical layer. *See also* copper cabling; fiber-optic cabling
characteristics of, 141–146, 168
fiber-optic cabling, 158–164
purpose of, 138–140
summary of, 168
wireless media, 164–167, 169–170
presentation layer, 508–510
session layer, 508–510
summary of, 131
transport layer, 102
technological vulnerabilities, 543
Telecommunications Industry Association (TIA), 111, 664
Telecommunications Industry Association/Electronic Industries Association (TIA/EIA), 141
Telnet, 50, 479, 580, 664
Tera Term, 50, 60
terabits per second, 145
terminal emulation programs, 50–52, 664
terminal monitor command, 615–616
test-net addresses, 665
text files, capturing configuration to, 68–71
TFTP (Trivial File Transfer Protocol), 101, 479, 511, 665
threat actors, 33, 542
threats, 33–34, 542–543, 565
three-way handshake, 665
three-way handshake (TCP), 485–486
throughput, 146, 665
TIA (Telecommunications Industry Association), 111, 141, 664
Time Exceeded messages, 446
timeout, response, 92
Time-to-Live (TTL) field, 275, 446, 453, 665

timing messages, 92–93
Token Ring LAN technologies, 214, 217
top-level domains, 525
topologies
data link layer, 209–220
access control methods, 216–217
contention-based access, 216–220
controlled access, 217
data link frame, 229
full-duplex communication, 215–216, 653
half-duplex communication, 215, 653
LAN (local area network), 213–214
physical/logical, 209–211
summary of, 228
WAN (wide area network), 211–213
definition of, 665
small business networks, 572–573. *See also* small business network management
topology diagrams, 8–11
definition of, 10
logical, 10–11
network symbols for, 8–10
physical, 10
ToS (Type of Service) field, 275
traceroute command
definition of, 665
IOS command syntax, 57
small business network verification with, 590–594
summary of, 454–455
testing network connectivity with, 452–453, 455
tracert command, 590–593
Traffic Class field (IPv6 packets), 280
traffic management, 577–578
traffice prioritization, 665
translation, 400–401
Transmission Control Protocol. *See* TCP (Transmission Control Protocol)
transport input command, 320, 562
transport input ssh command, 563
transport layer
definition of, 113, 114, 462
overview of, 102
port numbers
definition of, 465
groups of, 478
multiple separation communications with, 476
netstat command, 479–480
socket pairs, 477–478
well-known, 479
protocols, 467
responsibilities of, 463–466
role of, 462
segments in, 463, 468
TCP (Transmission Control Protocol)
applications using, 472–473
congestion avoidance, 493
connection establishment, 483–484
data loss and retransmission, 489
features of, 470–471
flow control, 471, 490–494
headers, 471–472
MSS (maximum segment size), 491–492
packet delivery, 486–487
reliability of, 467–468, 486–490, 500–501
server processes, 480–483
session termination, 484–485
summary of, 499
three-way handshake, 485–486
UDP (User Datagram Protocol) compared to, 469–471
window size, 490–491
UDP (User Datagram Protocol)
applications using, 475–476
client processes, 495–498
datagram reassembly, 494
features of, 473–474
headers, 474
overview of, 473
reliability of, 468–470, 494
server processes, 495
summary of, 499, 501
TCP (Transmission Control Protocol) compared to, 469–470
Trivial File Transfer Protocol (TFTP), 101, 479, 511, 665
Trojan horses, 33, 547, 665
troubleshooting
default gateways, 334
definition of, 665
small business networks, 611–623
basic approach, 612–613
debug command, 613–615, 616

default gateway issues, 619–620
DNS issues, 621–623
duplex operation, 617
IP addressing on end devices, 619
IP addressing on IOS devices, 618
mismatch issues, 617
resolution versus escalation in, 613
summary of, 626–627
terminal monitor command, 615–616
trust exploitation, 548–549
TTL (Time-to-Live) field, 275, 446, 453, 665
tunneling, 400, 665
twisted-pair. *See* STP (shielded twisted pair); UTP (unshielded twisted pair)
Type of Service (ToS) field (IPv4 packets), 275
Type/Length field (Ethernet frames), 239

U

UDP (User Datagram Protocol)
applications using, 475–476
client processes, 495–498
datagram reassembly, 494
definition of, 102, 666
features of, 473–474
headers, 474
overview of, 473
reliability of, 468–470, 494
server processes, 495
summary of, 499, 501
TCP (Transmission Control Protocol) compared to, 469–470
undebug command, 614
unicast, 93
IPv4, 349–350, 390
IPv6, 406, 407–408, 436–437
MAC addresses, 244–245
unknown, 250
unicast transmission
definition of, 665
unknown, 666
uniform resource locators (URLs), 515, 557
unique local addresses, 408, 665–666
unknown unicast, 250, 666
unshielded twisted pair. *See* UTP (unshielded twisted pair) cable
unspecified addresses, 666
unused host IPv4 addresses, minimizing, 377–378
unused services, disabling, 563–564
updates, security, 554
uploads, 512
URG flag, 486
Urgent field (TCP headers), 472
URLs (uniform resource locators), 515, 557
User Datagram Protocol. *See* UDP (User Datagram Protocol)
user executive mode, 53, 666
user passwords. *See* passwords
username command, 562
uTorrent, 514
UTP (unshielded twisted pair), 152–158
connectors, 153–156
crossover, 157
definition of, 148–150, 666
properties of, 152–153
standards, 153–156
straight-through, 157
summary of, 169
T568A/T68B standards, 157–158

V

variable-length subnet masking. *See* VLSM (variable-length subnet masking)
verification. *See also* configuration
of device connectivity, 78, 80
of IP (Internet Protocol) configuration, 77
of IPv6 addressing, 427–430
of router interfaces, 325–330
show interfaces command, 328
show ip interface brief command, 326
show ip interface command, 329
show ip route command, 327
show ipv6 interface brief command, 326–327
show ipv6 interface command, 330
show ipv6 route command, 327–328
of small business network connectivity, 586–596
network baselines, 593–596
ping command, 586–590
summary of, 624
traceroute command, 590–594
tracert command, 590–593

Version field
IPv4 packets, 275
IPv6 packets, 280
video, file formats for, 509
video applications, 29, 582
virtual circuits, 666
virtual classrooms, 666
virtual private networks (VPNs), 35
virtual terminal (vty), 64
virtualization, 666
viruses, 33, 546, 666
VLANs (virtual local area networks), 666
VLSM (variable-length subnet masking), 381–387
address conservation, 381–383, 385
definition of, 666
network address assignments in, 386–387
overview of, 381
summary of, 392
voice applications, 582
voice over IP (VoIP), 666–667
VoIP (voice over IP), 469, 582, 666–667
volatile memory, 667
VPNs (virtual private networks), 35
vty (virtual terminal), 64, 666
vulnerabilities, 543–544

W

WANs (wide area networks), 14–15
definition of, 14–15, 667
topologies, 211–213
hub-and-spoke, 211–212
mesh, 212
point-to-point, 211, 213
WAN frames, 225–226
WAPs (wireless access points), 138, 166, 667
weak passwords, 559
web browsers, 515–517
web pages, opening, 515–517
web protocols, 515–518
HTTP (Hypertext Transfer Protocol), 516–518
HTTPS (HTTP Secure), 515–518
summary of, 534
web servers, 5, 580
well-known IPv6 multicast addresses, 430–431, 667
well-known port number, 479
whois command, 547
wide area networks. ***See*** **WANs (wide area networks)**
Wi-Fi, 165–166, 169–170, 667
Wi-Fi Alliance, 165–166, 169–170
Wi-Fi analyzer, 667
WiMAX, 166, 169–170, 667
window size, 472, 490–491, 667
Window Size field (TCP headers), 472
Windows computers
ARP tables, displaying, 307
Data Usage tool, 585
dynamic LLAs (link-local addresses) on, 425–426
IP (Internet Protocol) configuration on, 596–598
wireless access points, 138, 166, 667
wireless internet service providers (WISPs), 32, 668
wireless LANs (WLANs), 103, 166–167, 234, 668
wireless media, 164–167
properties of, 164–165
types of, 165–166
wireless LANs (WLANs), 166–167
wireless mesh network, 668
wireless network interface card (NIC), 668
wireless networks, 32
wireless routers, 668
Wireshark, 129, 280, 583–584
WISPs (wireless internet service providers), 32, 668
WLANs (wireless LANs), 103, 166–167, 234, 668
WMN (wireless mesh network), 668
Worldwide Interoperability for Microware Access (WiMAX), 667
Worldwide Interoperability for Microwave Access (WiMAX), 166
worms, 33, 547, 668

X-Y-Z

X.25, 225
zero-day attacks, 33
Zigbee, 166, 169–170, 668